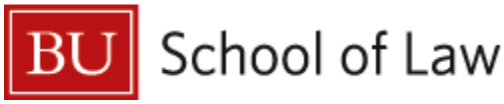
6-2020

A New Compact for Sexual Privacy

Danielle K. Citron



A New Compact for Sexual Privacy

Boston University School of Law
Public Law & Legal Theory Paper No. 20-20

June 2020

Danielle Keats Citron
Boston University School of Law

Forthcoming in William & Mary Law Review

A New Compact for Sexual Privacy

WILLIAM & MARY L. REV. (forthcoming)

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 can be done to curtail it. What is big business for firms is a big risk for individuals. The handling of intimate data undermines the values that sexual privacy secures—autonomy, dignity, intimacy, and equality. It can imperil people's job, housing, insurance, and other crucial opportunities. More often, women and minorities shoulder a disproportionate amount of the burden.

Privacy law is failing us. Our consumer protection approach offers little protection. Not only is the private-sector's handling of intimate information largely unrestrained, but it is treated as normative. This Article offers a new compact for the protection of sexual privacy. Civil rights and liberties, along with consumer protection, is at stake when firms amass intimate data. The new compact seeks to stem the tidal wave of collection, restrict certain uses of intimate data, and expand the suite of remedies available to courts. It draws upon the lessons of civil rights law in moving beyond procedural protections and in authorizing injunctive relief, including orders to stop processing intimate data.

A New Compact for Sexual Privacy

Danielle Keats Citron*

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 porn sites. Sex toys monitor the frequency and intensity of their owners' use.[2] Digital assistants record, transcribe, and store conversations in bedrooms and bathrooms.[3]

In some contexts, people enter into relationships with the firms tracking their intimate lives.[4] This is true when individuals subscribe to dating apps or purchase digital assistants. In other contexts, people have no connection with the firms handling their intimate data. Data brokers, cyber stalking

* Professor of Law, Boston University 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 Wyeth Lecture, to faculty and students for their thoughtful comments, and to the law review for superb edits. Woodrow Hartzog, Mary Anne Franks, Neil Richards, Alan Butler, Sara Cable, Cameron Kerry, Kris Collins, Jennifer Daskal, John Davisson, Hany Farid, Ahmed Ghappour, Rebecca Green, Debbie Hellman, Laura Heymann, Ryan Kriger, Gary Lawson, Karen Levy, Tiffany Li, Linda McClain, Mike Meuer, Luis Alberto Montezuma, Jeanine Morris-Rush, Nancy Moore, Nate Oman, David Rossman, David Seipp, Kate Silbaugh, Jessica Silbey, Noah Stein, Peter Swire, Ari Waldman, and David Webber shaped the piece with their astute advice. *Boston University Journal of Science & Technology Law* kindly asked me to present this paper as the keynote of the 2019 data privacy symposium. Matt Atha, Rebecca Gutterman, Caroline Hopland, and Julia Schur provided extraordinary research assistance. Boston University School of Law, especially Dean Angela Onwuachi-Willig, Associate Dean Stacey Dogan, and Associate Dean David Webber. The MacArthur Foundation graciously supported this work.

[1] Privacy International, *No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data* (Sept. 9, 2019) https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruation-apps-are-sharing-your-data.

[2] 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/.

[3] 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.

[4] For instance, people subscribe to dating apps that record their sexual preferences and favorite positions, interest in threesomes, HIV status, and hookups. They use online services that facilitate testing for sexually transmitted infections and share the results with prospective partners. Kimberly Aquilina, *STD testing? Yeah, There is an app for that*, METRO (June 6, 2017), https://www.metro.us/body-and-mind/health/std-testing-syphilis-Biem-app.

apps, and sites devoted to nonconsensual pornography and deep fake sex videos come to mind.[5]

Whether anticipated and desired 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 "data collection imperative."[6] For instance, analysts predict that within five years, the "femtech market"—menstruation, fertility, and sexual wellness apps—will be a $50 billion industry.[7]

The coin of the realm for digital services is personal data.[8] At some level, people understand that online services are not actually free.[9] 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 (well, beyond not using the service). Firms have every incentive to reinforce the status quo from which they earn considerable profits.[10]

The surveillance of intimate life garners significant returns with little risk for businesses.[11] The opposite is true for individuals.[12] The private sector's collection, use, storage, and disclosure of intimate information undermines what I have elsewhere called sexual privacy—the ways people

---

[5] Kashmir Hill, *Data Brokers were selling lists of Rape Sufferers*, FORBES (December 19, 2013), https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/#6aec189e1d53; Lorenzo Franceschi-Biccheirai & Joseph Cox, *Inside the Stalkerware Surveillance Market, Where Ordinary People Tap Each Other's Phones*, MOTHERBOARD (April 18, 2017), https://www.vice.com/en_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x; Danielle Keats Citron, *Spying Inc.*, 72 WASHINGTON & LEE L. REV. 1243 (2015).

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

[7] Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data With Your Boss?*, WASHINGTON POST (April 10, 2019).

[8] Chris Hoofnagle & Jan Whittington, *Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606 (2017).

[9] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM (2019); JULIE COHEN, BETWEEN TRUTH AND POWER (2019).

[10] Neil Richards & Woodrow Hartzog, *The Duty of Loyalty* (on file with author).

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

[12] *Id.; see generally* STIGLER COMMITTEE ON DIGITAL PLATFORMS 11 (2019) (explaining that firms collecting and processing 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 customers.").

manage the boundaries around intimate life.[13] Sexual privacy concerns the body, particularly the parts of the body associated with sex, gender, sexuality, and reproduction. It concerns any and all information about people's sex, gender, sexuality, and sexual and reproductive health. This includes on- and offline activities, interactions, communications, thoughts, searches. It concerns the decisions that people make about their intimate lives. This Article tackles the collection, use, storage, and disclosure of information implicating sexual privacy, a crucial subset of sexual privacy that I will refer to as intimate information or intimate data.[14]

Sexual privacy is foundational for our personhood and essential for our ability to flourish as human beings.[15] It enables sexual and gender experimentation and identity development.[16] It frees us to express ourselves and to form intimate relationships and associations.[17] It secures human dignity and equal opportunity.[18]

Private-sector surveillance of intimate information strips individuals of their ability to decide who learns about their miscarriages, breakups, HIV infections, sexual assaults, and nude images. It undermines people's self-esteem as they see themselves as intimate parts and not as whole selves. When companies categorize and rank people as rape sufferers or escort users and nothing more, they give those individuals fractured identities. People's self-expression is chilled. Fearful of unwanted surveillance, people stop using dating apps, fertility trackers, or digital assistants. They refrain from browsing sites devoted to gender experimentation, sexuality, and reproductive health.

The harm can be profound. Intimate data reveals people's physical and emotional vulnerabilities, which firms exploit to their advantage.[19] When intimate data is leaked or disclosed to hackers and criminals, individuals face reputational ruin, blackmail, and extortion.[20] When commercial hiring

---

[13] Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1871 (2019).

[14] I will use the terms "intimate information" and "intimate data" interchangeably to refer to any and all information implicating sexual privacy.

[15] *Id.*

[16] *Id.* Sexual privacy protects the ability of people to be sexual on their own terms, including being asexual.

[17] *Id. See generally* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 192-195 (2014).

[18] Citron, *Sexual Privacy*, supra note, at.

[19] See *infra* notes and accompanying text.

[20] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 739-45 (2018); Kate Fazzini, *Ashley Madison Cyber-Breach, 5 Years Later, Users are Being Targeted with Sextortion Scams*, CNBC (January 31, 2020),

intelligence companies use intimate data to mine, rank, and rate, people may unfairly fail to obtain job interviews.[21] People's insurance rates may rise because algorithms predict their need for expensive fertility treatments or gender reassignment surgeries.[22]

These risks are not evenly distributed across society. Women and marginalized communities disproportionately bear the burden of private-sector surveillance of intimate life. For instance, the fem-tech market will have a disproportionate impact on women in healthcare and insurance market.[23] The majority of people appearing on sites devoted to revenge porn and deep fake sex videos are women and sexual minorities. For people with intersecting marginalized identities, the harm is compounded.[24] 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.[25]

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 concerning those practices. For the most part, the collection, use, storage, and sharing of intimate data is enabled by this approach rather than restricted by it. Tracking intimate data is not just permissible, it is viewed as normative.[26]

This Article offers a new compact for the protection of intimate information. As a start, we need to revise our understanding of the privacy

---

https://www.cnbc.com/2020/01/31/ashley-madison-breach-from-2015-being-used-in-sextortion-scams.html.

[21] Ifeoma Ajunwa & Daniel Greene, *Platforms at Work: Automated Hiring Platforms and Other New Intermediaries in the Organization of Work*, *in* WORK AND LABOR IN THE DIGITAL AGE, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248675; Mar Hicks, *Hacking the Cis-tem*, IEEE ANNALS OF THE HISTORY OF COMPUTING, vol. 41, 20 (Jan.-Mar 2019). https://ieeexplore.ieee.org/document/8634814. *See generally* SAFIYA NOBLE, ALGORITHMS OF OPPRESSION (2018).

[22] *See* Jaden Urbi, "Some Transgender Drivers Are Being Kicked Off Uber's App," CNBC, August 8, 2018, https://www.cnbc.com/2018/08/08/transgender-uber-driver-suspended-tech-oversight-facial-recognition.html; S.M. West, M. Whittaker & K. Crawford, DISCRIMINATING SYSTEMS: GENDER, RACE, AND POWER IN AI (April 2019), *available at* https://ainowinstitute.org/discriminatingsystems.pdf.

[23] As discussed above, this is the explicit goal of fem-tech companies.

[24] Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," in Proceedings of the 1st Conference on Fairness, Accountability and Transparency (New York, 2018), 77–91, http://proceedings.mlr.press/v81/buolamwini18a.html; *see also* Citron, *Sexual Privacy*, *supra* note; Mary Anne Franks, *Democratic Surveillance*, HARV. J. L. & TECH (2015).

[25] Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009).

[26] Richards & Hartzog, *supra* note, at.

afforded 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 civil rights and civil liberties hang in the balance.

All personal data needs protection, but even more so for intimate information.[27] This approach aligns with the well-accepted approach to sensitive data that should apply to secure sexual privacy.[28] Intimate information should not be collected or processed without meaningful consent—knowing, voluntary, and express consent. Firms should not use personal data to infer intimate information, nor should they use intimate information to manipulate people to act against their interests. Firms should have obligations of loyalty to the intimate data that they handle. Available remedies should include injunctive relief ordering firms to stop processing intimate data until legal commitments are satisfied. Repeated violations can and should face the *data death penalty*—forbidding a firm's handling of personal data now and in the future.[29]

This Article has three parts. Part I provides a snapshot into the corporate surveillance of intimate life. It categorizes such surveillance into first-party data collection and third-party data collection. Part II highlights the damage

---

[27] There is plenty of terrific scholarship on the contours of strong baseline privacy protections. *See* Neil Richards & Woodrow Hartzog, *The Pathologies of Consent*, 96 WASH. U. L. REV. (2019); Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952 (2017); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously*, 19 STAN. TECH. L. REV. (2016); Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROTECTION REV. 423 (2018); Richards & Hartzog, supra note. 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 Institute (February 10, 2020), https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/; Cameron F. Kerry, https://www.lawfareblog.com/data-collection-standards-privacy-legislation-proposed-language; Cameron F. Kerry, A Federal Privacy Law Could Do Better than California's, L.A. Times (April 25, 2019), https://www.latimes.com/opinion/op-ed/la-oe-kerry-ccpa-data-privacy-laws-20190425-story.html; https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/;

[28] Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1128 (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 (2007).

[29] Thanks to Woodrow Hartzog for suggesting the concept of the data death penalty to describe stop processing orders.

corporate intimate surveillance causes to the values sexual privacy secures and the harm to human well-being 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 situates privacy as a matter of civil rights and not just consumer protection. It provides guideposts for regulating the private sector's surveillance of intimate information. It suggests affirmative obligations for firms in the collection, use, and storage of intimate data and the addition of injunctive relief.

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.[30] First, it describes scenarios of first-party collection—by which I mean instances where people have direct relationships with businesses collecting their intimate information. Then, it gives examples of third-party collection—by which I mean instances where people lack a direct relationship with private entities handling their intimate information. I use the concepts of first-party and third-party data collection to organize the varied commercial scenarios in which intimate information is collected, processed, used, and shared.

A. Cataloging First-Party Collection

[30] Karen Levy has an important 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 helpfully breaks down intimate surveillance into three categories: dating, tracking intimate and romantic partners, and fertility monitoring. In this article, I explore the collection, use, sharing, and storage of information about 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* 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 (2006); Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009); Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014); Danielle Keats Citron, *The Right to Sexual Privacy in* VISIONS OF PRIVACY IN THE MODERN AGE (Marc Rotenberg et al. eds 2015); Danielle Keats Citron, *Spying Inc.*, 72 WASH. & LEE L. REV. 1243 (2015); Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019); Danielle Keats Citron, *Why Sexual Privacy Matters for Trust*, 96 WASH. U. L. REV. 1189 (2019); Danielle Keats Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753 (2019). I am using first-party and third-party data collection as a way to understand the broad array of firms involved in collecting, using, sharing, and storing intimate information.

Businesses routinely gather intimate information directly from individuals. First-party collection includes sites related to sexual and reproductive health, porn sites, dating apps, and personal devices.

1. Sexual and Reproductive Health

Countless apps are devoted to the collection of information about sexual and reproductive health. Sites and apps let people track their sex lives, including when they had sex, with whom, whether they used protection, and when they masturbated.[31] Some host community forums where subscribers can connect with each other to discuss their sex lives.[32] Health apps increasingly let users track their sexual activity.[33]

There are male-oriented health companies focusing on sexual issues.[34] For instance, the startup Ro sends erectile dysfunction drugs directly to consumers. Hims provides treatments for male hair and sexual issues. Those two firms alone raised more than 80 million each in financing.[35]

The term "femtech" describes apps and services that collect information about women's period cycles, fertility, pregnancies, menopause, and sexual and reproductive histories.[36] Nearly one third of women in the United States use period-tracking apps.[37] Menstrual tracking apps are the fourth most popular health app among adults and the second most popular among girls.[38] The startup Gennev provides a "free" online menopause

---

[31] Emma McGowan, *Tracking Your Sex Life With Apps Makes It Super Easy*, Bustle (January 9, 2020), https://www.bustle.com/p/tracking-your-sex-life-with-apps-makes-it-super-easy-19779217.

[32] *Id.*

[33] Lux Alptraum, *Apple's Health App Now Tracks Sexual Activity, and That's a Big Opportunity*, MOTHERBOARD (October 23, 2016, 1:00 p.m.).

[34] https://pitchbook.com/news/articles/this-year-is-setting-records-for-femtech-funding.

[35] *Id.*

[36] Harwell, *supra* note, at.

[37] Donna Rosatto, What Your Period Tracker App Knows About You, Consumer Reports (January 22, 2020), https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you/. There are also fertility apps that track women's menstrual cycles and pregnancy apps that monitor women's habits, mood, fetal movements, and more. *Quantifying Fertility and Reproduction Through Mobile APPs: A Critical Overview*, Arrow for Change, vol. 22, at 13-14 (2016). Some apps like Glow cover all aspects of fertility, including tracking women's cycles, fertility, pregnancy, and a baby's development in the first year. *Id.*

[38] Michelle L. Moglia et al., *Evaluation of Smartphone Menstrual Cycle Tracking Applications Using an Adapted APPLICATIONS Scoring System*, OBSTETRICS & GYNECOLOGY, volume 127 (June 2016).

health assessment that "collects 72 data points—and nearly 35,000 women took it in 2019."[39] Menopause startups have raised $254 million in the past ten years while femtech startups as a whole raised more than $498 million in 2019 alone.[40]

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.[41] Apple's Health app syncs with period and fertility tracking apps and allows subscribers to track their sexual activity.[42] The Flo app provides extra features such as period predictions and health reports that can be shared with doctors.[43] Some services let subscribers obtain discounts on products like tampons.[44]

Consider the Eve Glow app. Subscribers must record their sex drive status with the following choices: "DO ME NOW, I'm down, or MIA."[45] To complete their health log, subscribers must input whether they orgasmed during sex.[46] The app's screen enables subscribers to answer "YASSS, No,

---

[39] Eliza Haverstrock, Narrative change: VCs are finally ready to talk about menopause, PitchBook (May 28, 2020), available at https://pitchbook.com/news/articles/vc-menopause-femtech

[40] https://pitchbook.com/news/articles/vc-menopause-femtech.

[41] Privacy International, *No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data* (Sept. 9, 2019) https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruation-apps-are-sharing-your-data. For instance, the app Clue goes further and asks subscribers to track not just the dates and details of their menstrual cycles but also their discharge of cervical fluids, medication, sex life, injections, illnesses, and cervical position. Sadaf Khan, *Data Bleeding Everywhere: A Story of Period Trackers*, MEDIUM (June 7, 2019), https://deepdives.in/data-bleeding-everywhere-a-story-of-period-trackers-8766dc6a1e00. The Ovia app lets users indicate the consistency of their cervical discharge, from egg whites and water to a bottle of school glue. *Id.* As Karen Levy has noted, period-tracking apps are also marketed to people's partners so that they can manage their relationships around menstrual cycles. Karen Levy, *Intimate Surveillance*, 51 IDAHO L. REV. 679, 685-86 (2015) (discussing apps like PMSTracker and iAmAMan, which enables subscribers to track multiple women's cycles and uses multiple passwords to allow users to conceal their tracking activity).

[42] Lux Alptraum, *Apple's Health App Now Tracks Sexual Activity, and That's a Big Opportunity*, MOTHERBOARD (October 23, 2016). Some apps are exclusively designed to track people's sexual activity. On Bedpost's app, subscribers track the names of sexual partners, dates of sexual experiences, and rank the sexual experience. http://www.bedposted.com/

[43] *Id.*

[44] Rosatto, *supra* note, at.

[45] MIA presumably means "Missing In Action."

[46] Sadaf Khan, *Data Bleeding Everywhere: A Story of Period Trackers*, MEDIUM (June 7, 2019), https://deepdives.in/data-bleeding-everywhere-a-story-of-period-trackers-8766dc6a1e00.

or Faked It."[47] They are asked to indicate whether they are experiencing cramps, tender breasts, or bloating.[48]

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. 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.[49] The apps track and store those communications.

Three million people use Glow's suite of apps, which include Eve Glow, Glow, Glow Nurture, and Glow Baby.[50] The company is part of HVF Labs whose objective is to "take advantage of potential low-cost sensors, the gradual increase in access to broadband, and the *high storage capacity to collect and explore 'data as a commodity*.'"[51] 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. Only some of the user data shared is "made anonymous."[52]

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.[53] Trackle links a vaginal thermometer with an app measuring women's inner temperature.[54]

Reproductive health apps market themselves as providing expert advice. Yet many are riddled with misinformation. According to researchers, free menstrual cycle tracking apps are riddled with inaccurate information.[55] Most the apps were "inaccurate, contain misleading health information, or do not function." Only 20 percent of the period-tracking

---

[47] *Id.*

[48] Khan, *supra* note, at.

[49] *Id.*

[50] Natasha Felizi & Joana Varon, *Menstruapps – How to Tur Your Period Into Money (For Others)*, CHUPADOS (CODING RIGHTS) (emphasis added).

[51] *Id.*

[52] *Id.*

[53] https://www.kickstarter.com/projects/700989404/looncup-the-worlds-first-smart-menstrual-cup. Looncup is now available for pre-order. http://www.looncup.com/.

[54] *Quantifying Fertility and Reproduction Through Mobile APPs: A Critical Overview*, ARROW FOR CHANGE, vol. 22, at 13-14 (2016).

[55] Moglia, *supra* note, at 1157.

apps predicted periods accurately and even those apps contained erroneous medical information.[56]

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.[57] Flo was caught sending Facebook subscribers' information including when they were trying to conceive and having their periods.[58]

2. Porn Sites

Pornography sites collect and store a wealth of information about people's sexual interests, desires, and sexual practices. They derive intimate information from people's search queries, the time and frequency of their visits, and private chats. The most popular free porn site PornHub reports that the most searched terms on the site include lesbian, "milf," stepmom, and teen.[59] The very nature of some porn sites reveals people's sexual interests like bestiality or incest sites.

Some specialty sites require members to provide email addresses, passwords, and credit card information.[60] A zoophilia forum accumulated personal information for about 71,000 individuals, including usernames, birth dates, and IP addresses.[61] Rosebuttboard.com, a forum dedicated to

---

[56] *Id.*

[57] Jerry Beilinson, *Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds*, CONSUMER REPORTS (July 28, 2016), https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/

[58] https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636?mod=e2tw

[59] *The 2019 Year in Review*, PORNHUB INSIGHTS (Dec. 11, 2019), https://www.pornhub.com/insights/2019-year-in-review#searches; https://www.psychologytoday.com/us/blog/all-about-sex/201803/surprising-new-data-the-world-s-most-popular-porn-site.

[60] Joseph Cox, *Thousands of Bestiality Website Users Exposed in Hack*, MOTHERBOARD (March 29, 2018), available at https://www.vice.com/en_us/article/evqvpz/bestiality-website-hacked-troy-hunt-have-i-been-pwned (explaining that hack of bestiality site revealed more than 3,000 users' full names, password hashes, birthdates, IP addresses, and a "few hundred private messages between users").

[61] Have I Been Pwned (@haveibeenpwned), TWITTER (Oct. 19, 2019, 5:25 PM), https://twitter.com/haveibeenpwned/status/1185668262538838016. Hackers exposed the personal details of the users of the bestiality site online. Ahmed Waqas, *Animal abuse website hacked; thousands of users exposed*, HACKREAD (March 30, 2018), https://www.hackread.com/animal-abuse-website-hacked-users-exposed/.

"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.[62]

Porn sites are some of the most popular sites online. They garner more visitors a month than Amazon, Netflix, and Twitter combined.[63] In 2018, PornHub had 33.5 billion visits.[64] It had an average of 63,000 visitors per minute.[65] In 2019, that number grew to 80,000 visitors per minute.[66]

3. Dating Apps

Dating apps and services collect broad swaths of people's intimate (paired with personally identifying) information, including name, photograph, occupation, location, relationship status, romantic or sexual interests, sexual orientation, interest in extramarital affairs, or sexually transmitted infections.[67] Adults are not the only ones on dating apps; many teenagers also subscribe to Tinder, MeetMe, Hot or Not, MyLOL, and Kik.[68]

---

[62] Joseph Cox, *Another Day, Another Hack: Is Your Fisting Site Updating Its Forum Software?*, VICE (May 10, 2016, 9:54 AM), https://www.vice.com/en_us/article/qkjj4p/rosebuttboard-ip-board; Jonathan Keane, *Hack shows government and military employees used their email addresses on hardcore fetish site*, DIGITAL TRENDS (May 13, 2016, 12:11 PM), https://www.digitaltrends.com/computing/rosebutt-hack/; Troy Hunt (@troyhunt), TWITTER (May 10, 2016, 10:06 AM), https://twitter.com/troyhunt/status/730036184651431937.

[63] Elena Maris, Timothy Libert & Jennifer Henrichsen, *Tracking Sex: The Implications of Widespread Sexual Data Leakage and Tracking on Porn Websites*, NEW MEDIA & SOCIETY (July 2019).

[64] *Digital Fingerprints: How the Porn You Watch May Be Watching You* (Feb. 13, 2019).

[65] https://fightthenewdrug.org/pornhub-visitors-in-2018-and-review-of-top-searches/.

[66] *The 2019 Year in Review*, PORNHUB INSIGHTS (Dec. 11, 2019), https://www.pornhub.com/insights/2019-year-in-review.

[67] *See* Thomas Germain, *How Private is Your Online Dating Data?*, CONSUMER REPORTS (Sept. 21, 2019), https://www.consumerreports.org/privacy/how-private-is-your-online-dating-data/ ("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/. It is worth noting the rise of dating intelligence apps like Lulu that allow women to anonymously review and rate men. Lulu raised $6 million in venture funding and was acquired by Badoo in 2016. https://pitchbook.com/newsletter/dating-intelligence-app-lulu-acquired-by-badoo.

[68] Christina Elgersma, *Tinder and 7 More Dating Apps Teens Are Using*, COMMON SENSE MEDIA BLOG (February 12, 2019), *avalaible at*

Such sites are commonly used by LGBTQ youth who lack supportive networks at school to use dating apps to connect with others.[69]

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.[70] Journalist Judith Duportail discovered just how extensive her disclosures to Tinder were when her GPDR request to the company returned 800 pages of detailed information.[71] A review of the 1,700 messages Duportail sent through the app revealed her "hopes, fears, sexual preferences and deepest secrets."[72]

All of this intimate information is ripe for exploitation and disclosure.[73] In some cases, this data may appear in the profiles of potential matches.[74] As explored below, it may be shared with advertisers and other firms. It may be inadequately secured and stolen by thieves. Hackers have targeted individual accounts and dating services to steal intimate information in order to blackmail and extort subscribers.[75] In 2015, a data breach resulted

---

https://www.commonsensemedia.org/blog/tinder-and-7-more-dating-apps-teens-are-using. Teenagers can access some of these apps via Facebook. *Id.*

[69] *Id.*

[70] Germain, *supra* note.

[71] 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. 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. Facebook started a dating app in 2019. https://www.nytimes.com/2019/09/05/opinion/facebook-dating-app.html; https://newsroom.fb.com/news/2019/09/facebook-dating/.

[72] Duportail, *supra* note.

[73] "Tinder's privacy policy clearly states: 'you should not expect that your personal information, chats, or other communications will always remain secure.'" Duportail, *supra* note; *see also Privacy Policy*, TINDER, https://www.gotinder.com/privacy (last updated May 2, 2018) ("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.").

[74] 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. 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.*

[75] 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-

in hackers publishing online the personal details of subscribers to Ashley Madison, a site for people seeking extra-marital affairs.[76] Millions of subscribers' names, emails, sexual preferences, and sexual desires were posted online in a searchable format. To this day, criminals have been using the intimate information shared with Ashley Madison in extortion schemes.[77]

With respect to particular sites, membership or browsing on the site may reveal someone's sexual preferences and indiscretions.[78] In October 2016, hackers obtained 412 million account records from Friend Finder Networks.[79] The information exposed included "email addresses, 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.[80]

---

apps-hacks-breaches-security/. "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." *Id.*

[76] Zak Doffman, *Ashley Madison Hack Returns To 'Haunt' Its Victims; 32 Million Users Now Watch and Wait*, MEDIUM (Feb. 1, 2020) (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), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/. The data released by hackers included names, passwords, addresses, 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." *Id.* Nor do they realize how easy it is to re-identify such information.

[77] Zak Doffman, *Ashley Madison Hack Returns To 'Haunt' Its Victims; 32 Million Users Now Watch and Wait*, MEDIUM (Feb. 1, 2020) (explaining that victims of Ashley Madison hack are receiving emails with embarrassing details from the breach, such as that a victim shared that they received "'chemical help' for a good time or private messages sent to other site members, and with demands for bitcoin ransom to be paid in a limited amount of time).

[78] *See, e.g.*, Cox, *supra* note; Broder Van Dyke, *infra* note.

[79] "Among the leaked account details were 78,301 US military email addresses, 5,650 US government email addresses and over 96[million] Hotmail accounts. . . . [A]lso included the details of what appear to be almost 16[million] deleted accounts." 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.

[80] "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

Three years later, a hacker obtained 250,000 "email addresses, usernames, IP addresses, and hashed passwords" from Dutch sex-work forum Hookers.nl where "clients discuss[ed] their experiences with sex workers."[81]

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. The app let partners to communicate with each other via text or video chat.[82] The Lioness vibrator similarly enables subscribers to live stream "what is going on in the moment" and permits partners to remotely control the device.[83] Companies sell wi-fi enabled butt plugs, vibrating masturbators for men, and devices for the penis that track thrusting.[84] Like many consumer goods, internet-connected sex toys are not developed with privacy and security in mind.[85]

---

details, emails, dates of birth, post codes, sexual preferences and whether they were seeking extramarital affairs." Gibbs, *supra* note. 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.

[81] Samantha Cole & Joseph Cox, *A Hacker Stole 250k User Account Details from a Dutch Sex Work Site*, VICE (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 ("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/("Dutch broadcaster NOS, which broke the story. . . viewed some of the data and said it could determine some real names of users")

[82] 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/.

[83] https://blog.lioness.io/now-you-can-see-your-orgasm-in-real-time-359afbdfa6d0. 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 Complaint, N.P & P.S. v. Standard Innovation Corp., Case No. 16-CV-08655 (N.D. Ill. Filed February 27, 2017).

[84] Emily Dreyfuss, Don't Get Your Valentine an Internet-Connected Sex Toy, WIRED (February 14, 2019); https://jezebel.com/how-fit-is-your-dick-exactly-the-sexfit-ring-knows-al-1618065007.

[85] Internet of Dongs, Goals, available at https://internetofdon.gs/about/. Security researchers involved in "The Internet of Dongs Project" report on security vulnerabilities and work with companies interested in fixing problems. 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. https://internetofdon.gs/vendor-resources/.

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.[86] Amazon's Echo and other Alexa-enabled devices are marketed as in-home hubs for managing day-to-day tasks. They record people's communications, storing them as voice recordings and text transcripts in the cloud.[87] Amazon retains text transcripts even after subscribers choose to delete the saved audio files of their voice interactions with the device.[88]

According to researchers, voice-activated assistants like Alexa and Echo do not only wake and record when subscribers say the wake word. The systems are error-prone and have recorded intimate conversations.[89] Apple's Siri has captured recordings of sexual encounters.[90] Computer science researchers at Northeastern University conducted a study of smart speakers by exposing devices to three audiobooks and nine episodes of the television show The Gilmore Girls.[91] There were 63 false positives in 21 hours.[92]

Amazon employs thousands of people worldwide to analyze and transcribe voice clips to improve Alexa's accuracy.[93] Some employees have watched people's home camera footage.[94] One German Amazon customer inadvertently received hundreds of Alexa recordings and transcripts from

---

[86] Alex Hern, *Apple contractors 'regularly hear confidential details' on Siri recordings*, GUARDIAN (July 2019, 2019 12:34 PM), https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings.

[87] Makena Kelly & Nick Statt, *Amazon confirms it holds on to Alexa data even if you delete audio files*, VERGE (July 3, 2019, 4:14 p.m. EDT), https://www.theverge.com/2019/7/3/20681423/amazon-alexa-echo-chris-coons-data-transcripts-recording-privacy.

[88] *Id.*

[89] Allen St. John, *Smart Speakers that Listen When They Shouldn't* (August 29, 2019); Alex Hern, *Apple contractors 'regularly hear confidential details' on Siri recordings*, GUARDIAN (July 2019, 2019 12:34 PM), https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings.

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] Matt Day, Giles Turner & Natalia Drozdiak, *Amazon Workers Are Listening to What You Tell Alexa*, BLOOMBERG (April 10, 2019, 6:34 PM EDT), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

[94] Natalia Drozdiak et al., *Amazon Workers May Be Watching Your Cloud Cam Home Footage*, BLOOMBERG (Oct. 10, 2019 5:00 AM), https://www.bloomberg.com/news/articles/2019-10-10/is-amazon-watching-you-cloud-cam-footage-reviewed-by-humans.

another user in response to a GDPR request in August 2018.[95] The person could be heard in multiple locations, including the shower, as could a frequent female guest.[96] 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."[97] In July 2019, Google admitted to a similar breach after a contractor shared with a news site more than 1,000 sound recordings of customer conversations made by Google Assistant.[98] Included in the recordings were people talking about medical conditions.[99]

Amazon plans to expand Alexa's reach, with one executive telling *The New York Times*, "there is no reason not to put them everywhere in your house."[100] Amazon has released a tiny version of the device, Echo Flex, meant for bathrooms, which plugs into wall outlets.[101] Customized, location-specific versions of Alexa are being sold and deployed in hotel rooms around the country.[102]

B. Surveying Third-Party Collection

---

[95] 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. 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.*

[96] Brown, *supra* note.

[97] Brown, *supra* note.

[98] Todd Hasleton, *Google admits partners leaked more than 1,000 private conversations with Google Assistant*, CNBC (July 11, 2019), https://www.cnbc.com/2019/07/11/google-admits-leaked-private-voice-conversations.html.

[99] Hasleton, *supra* note.

[100] Weise, *supra* note, at. 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://www.slashgear.com/kohler-put-alexa-in-your-showerhead-and-gave-your-toilet-an-app-03605166/.

[101] Karen Weise, *Amazon Wants Alexa to Move (With You) Far Beyond the Living Room*, NEW YORK TIMES (September 25, 2019).

[102] 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. 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.

First-party collection is often tied to third-party collection. Sometimes, companies purchase intimate data from first-party collectors. At other times, they obtain intimate information from someone who lack authority to share, disclose, or sell it. This section provides illustrations.

1. The Data Hand-Off: Advertising and Analytics

First-party data collectors often allow advertising firms to collect subscribers' intimate information for a fee. Period-tracking apps share user data with online advertisers who may further resell the information.[103] For instance, Maya and MIA Fem share data about subscribers' contraception and sexual encounters with Facebook's advertising system (even if those individuals do not have Facebook accounts themselves).[104] Although the apps are marketed to consumers as "free," their price is people's most intimate information.[105]

First-party data collectors allow analytics firms to place trackers on their sites. For instance, Grindr shared subscribers' HIV status (noted as positive, positive on HIV treatment, negative, or negative on PrEP) with two companies hired to optimize the app.[106] It also disclosed to advertisers

[103] At least 11 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. 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

[104] 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/. For instance, users tried to block tracking by using anonymizing browsers.

[105] Hoofnagle & Whittington, *supra* note, at.

[106] 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. 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. Localytics, The Stages of Personalization, *available at* https://ebooks.localytics.com/the-stages-of-personalization#the-stages-of-personalization-1. Profile data, the company explains, can originate from many sources. 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

subscribers' "tribe" (meaning what gay subculture they identify with), precise geolocation, sexuality, relationship status, and phone ID.[107] Some of the information shared with advertisers appeared in plain text.[108]

Third-party trackers are pervasive on porn sites. Researchers found that 93 percent of 22,484 porn sites analyzed allowed third parties to collect information about people's browsing habits, even where viewers took steps to hide them.[109] On average, porn sties had seven companies tracking viewers' information. Google trackers appeared on 50 percent of the sites studied, Oracle on 24 percent, and Facebook on ten percent.[110] Porn-specific trackers included ExoClick, JuicyAds, and EroAdvertising.[111] Another 2019 study found that more half of the top 100 most popular porn sites host third-party trackers that use a technique allowing cookies to be synchronized across sites.[112] Microsoft's Elena Maris noted that, "The fact that the mechanism for adult site tracking is so similar to, say, online retail should be a huge red flag."[113]

Third-party trackers collected people's IP addresses, phone's advertising identification number, and information suggesting their sexual desires.[114] Forty-five percent of porn site URLs include words or phrases

---

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.

[107] Ghorayshi & Ray, *supra* note. In late 2019, Norwegian researchers found that Grindr uses various advertising networks and some received information about the type of relationship the user is looking for. Norwegian Consumer Council, Out of Control—A Review of Data Sharing By Popular Mobile Apps 30, available at https://fil.forbrukerradet.no/wp-content/uploads/2020/01/mnemonic-security-test-report-v1.0.pdf

[108] *Id.* Grindr's privacy policy states that if subscribers "choose to include information in your profile, and make your profile public, that information will also become public." *Id.*

[109] Elena Maris, Timothy Libert & Jennifer Henrichsen, *Tracking Sex: The Implications of Widespread Sexual Data Leakage and Tracking on Porn Websites* (July 2019).

[110] *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*, THE VERGE (July 18, 2019). The company also claimed that tags for ad services are never allowed to transmit personally identifiable information. *Id.*

[111] *Id.* at 5.

[112] Pelayo Vallina et al., *Tales from the Porn: A Comprehensive Privacy Analysis of the Web Porn Ecosystem*, *available at* http://www1.icsi.berkeley.edu/~narseo/papers/pornweb2019_preprint.pdf.

[113] https://www.nytimes.com/2019/07/17/opinion/google-facebook-sex-websites.html

[114] *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

suggesting a particular sexual preference or interest, such as "boyfuckmomtube." Adult advertising networks collect IP addresses, browsers, locations, basic PC details, and other information including how much time people spend on certain videos and what categories of porn they select.[115]

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. They detail people's sexual preferences, porn consumption, sex toy purchases, escort service usage, and reproductive choices.[116] People are tagged as rape victims, Erectile Dysfunction sufferers, sex toy purchasers, AIDS/HIV infected, and gay air force personnel.[117]

Data brokers sell lists of gay and lesbian adults, rape victims, people with sexual addictions, individuals with sexually transmitted diseases, purchasers of adult material and sex toys.[118] Some data brokers specialize in dating profiles. For instance, USDate sells dating profiles that include people's photographs, usernames, email addresses, nationality, gender, and sexual orientation.[119] Exact Data sells customer lists of adult dating service subscribers, dating and escort services, and "Suddenly single."[120]

YouPorn and RedTube, did not allow third parties to access users' activity on the sites or their web histories. Tracy Clark-Flory, *Who's Tracking Your Porn*, SALON (December 12, 2013). Pornhub now has trackers, including adult advertising networks.

[115] Dylan Curran, *Browsing Porn in Incognito Mode Isn't Nearly as Private as You Think*, THE GUARDIAN (May 27, 2018).

[116] *Id.*

[117] Jeff Roberts, *With data brokers selling lists of alcoholics to big business, the feds have some thinking to do*, Gigaom (March 13, 2004), https://gigaom.com/2014/03/13/with-data-brokers-selling-lists-of-alcoholics-to-big-business-the-feds-have-some-thinking-to-do/.

[118] Jeff Roberts, *With data brokers selling lists of alcoholics to big business, the feds have some thinking to do*, GIGAOM (March 13, 2004), https://gigaom.com/2014/03/13/with-data-brokers-selling-lists-of-alcoholics-to-big-business-the-feds-have-some-thinking-to-do/

[119] https://datadating.tacticaltech.org/viz; https://www.vice.com/en_us/article/59vbp5/shady-data-brokers-are-selling-online-dating-profiles-by-the-millions; Charlie Warzel, *Facebook and Google Trackers Are Showing Up on Porn Sites*, N.Y. TIMES (July 17, 2019), *available at* https://www.nytimes.com/2019/07/17/opinion/google-facebook-sex-websites.html.

[120] https://www.exactdata.com/mailing-lists.html?keyword=dating (last visited Jan. 31, 2020).

The data-broker industry generates 200 billion dollars annually.[121] People's personal information is harvested from a vast array of sources, including government records, advertisers, and analytics firms, largely without individuals' knowledge.[122] Thousands of data brokers operate in the United States.[123] Data brokers have personal information on 95 percent of the U.S. population.[124]

Data brokers say that their dossiers enhance online advertising and email marketing campaigns.[125] They offer their services as "people search sites" to anyone interested in finding out about specific individuals.[126] They also sell risk mitigation products described as helping clients prevent fraud that can adversely impact people's ability to obtain certain benefits.[127] Clients include alternative payment providers, educational institutions, insurance companies, lenders, political campaigns, pharmaceutical companies, technology firms, and real estate services.[128] Customers also include government agencies and law enforcement.[129] As Chris Hoofnagle put it years ago, data brokers serve as "Big Brother's Little Helpers."[130]

---

[121] https://clearcode.cc/blog/what-is-data-broker/.

[122] Federal Trade Commission, *Report on Data Brokers*, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[123] https://clearcode.cc/blog/what-is-data-broker/.

[124] 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

[125] Yael Grauer, *What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?*, Motherboard (March 27, 2018), https://www.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection

[126] *Id.*

[127] Federal Trade Commission, *Report on Data Brokers*, at viii, 32-33, 48 https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[128] Federal Trade Commission, *Report on Data Brokers*, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[129] David Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. FORUM 262 (2013).

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

3. Cyber Stalking Apps

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. Cyber stalking apps enable continuous real-time monitoring of everything phone owners do and say with their devices.[131] 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. Targeted phones can be turned into bugging devices, recording conversations within a fifteen-foot radius.[132]

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.[133] The goal is the stealth surveillance of intimates or ex-intimates.[134] Firms are trying 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.[135] The Electronic Frontier Foundation's Eva Galperin has been watching the industry closely and she explains that the "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."[136]

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. Sites solicit users to post people's nude photos and contact information.[137] Some are devoted to gay men and others to

---

[131] Citron, *supra* note, at 1247.

[132] *Id.*

[133] *Id.* at 1246.

[134] *Id.* at 1247.

[135] Laura Hautala, *Stalkerware sees all, and US laws haven't stopped its spread*, C/NET (June 5, 2020), https://www.cnet.com/news/stalkerware-sees-all-and-us-laws-havent-stopped-its-spread/.

[136] Andy Greenberg, *Hacker Eva Galperin Has a Plan to Eradicate Stalkerware*, WIRED (April 3, 2019), https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/.

[137] Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014); Danielle Citron & Woodrow Hartzog, *The Decision that Could Finally Kill the Revenge Porn Business*, ATLANTIC (February 3, 2015),

women.[138] Sites earn revenue from online advertising, profiting directly from their trade in human misery.[139]

Online hubs hosting nonconsensual pornography are plentiful.[140] More than 3,000 porn sites feature revenge porn as a genre.[141] Sites have emerged soliciting users to post deep-fake sex videos.[142] Much like revenge porn sites, the business model of these sites is also 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.[143] Instead of considering victims' requests to remove their nude images, the most popular sites move the images behind a paywall.[144]

In a variation on this theme, software developers are selling apps that allow subscribers to upload photographs of women and see them nude. The app bills itself as artificial intelligence that "undresses photos of women and produce[s] a realistic nude image."[145] Services charge a flat fee for

---

https://www.theatlantic.com/technology/archive/2015/02/the-decision-that-could-finally-kill-the-revenge-porn-business/385113/.

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

[139] Carolyn A. Uhl et al., *An Examination of Nonconsensual Pornography Websites*, SAGE (February 8, 2018).

[140] I will refrain from pointing out the major sites devoted to posting nonconsensual pornography to avoid drawing further attention to them.

[141] https://www.mcolaw.com/white-papers-research/action-sheet-on-revenge-porn. A notorious revenge porn site reappeared in February 2020 after being shuttered by Danish authorities in 2018. Joe Uchill, *Someone is Trying to Revive the Infamous Revenge Porn Site Anon-IB*, MOTHERBOARD (February 14, 2020, 8:39 am). 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. Within three weeks of the site's reopening, over 1,500 posters had uploaded or commented on nude images.

[142] Bobby Chesney & Daniel Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 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 6 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.").

[143] *Id.*

[144] *Id.*

[145] https://www.theverge.com/2019/6/27/18760896/deepfake-nude-ai-app-women-deepnude-non-consensual-pornography. There are services specializing in photoshopping "cum shots" on women's faces and creating fake nudes. Some services say that they may use the photos and post them online unless the person paying for them requests otherwise.

premium version. One start-up claims to have what it calls porn-social media matching software, which uses facial recognition software to cross references faces in pornography videos and people's social media profiles. The business' stated goal is to "help others check whether their girlfriends ever acted in those films."

II. ASSESSING THE DAMAGE AND LAW'S RESPONSE

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

A. Undermining the Values Secured by Sexual Privacy

Sexual privacy allows people to manage the boundaries around their intimate lives. [146] With sexual privacy, people enjoy the freedom to go "backstage" to experiment with their bodies, sexuality, and gender.[147] They decide who learns about their innermost fantasies, sexual history, and sexual and reproductive health.

The private sector's handling of intimate data undermines the values that sexual privacy secures. Firms have jeopardized the autonomy that sexual privacy enables. The dating app Jack'd endangered individuals' choice to keep their nude photos private by making it easy for strangers to find them online. Grindr negated subscribers' choice to share intimate information only with potential partners by giving it to advertisers and analytics. There is every reason to believe that subscribers were distressed (to say the least) by the denial of their autonomy.

Private-sector surveillance of intimate information also imperils self-expression and the ability of people to explore new information and ideas.[148] The social conformity theory of chilling effects helps explain

---

[146] *Id.* at 1886. My prior work explores the value of sexual privacy in great detail. *See* Citron, *supra* note, at 1882-93; Danielle Keats Citron, *Why Sexual Privacy Matters for Trust*, 96 WASH. U. L. REV. 1189, 1193-1203 (2019) (exploring the importance of sexual privacy for trust in intimate relationships).

[147] Citron, *Sexual Privacy*, *supra* note, at.

[148] Jerry Kang, *Information Privacy in Cyberspace*, 50 STAN. L. REV. 1193, 1260 (1998). For a masterful exploration of the importance of intellectual privacy, see NEIL M. RICHARDS, INTELLECTUAL PRIVACY (2015). Sexual privacy and intellectual privacy are both foundational privacy rights that often intersect.

why.[149] People may refrain from searching, browsing, and expressing themselves if they perceive their expression and exploration as falling outside the mainstream.[150] For fear that intimate information will be collected and shared in unwanted ways, people will stop visiting sites devoted to gender, sexuality, or sexual health. They will not use period-tracking apps that might help them manage anxiety, pain, and uncertainty.[151] They will stop visiting adult sites that enable "vicarious expression and satisfaction of minority interests that are difficult, embarrassing, and occasionally illegal to indulge in reality."[152] They might avoid communicating about intimate matters for fear of unwanted exposure.[153] The self-censorship can be more subtle though no less significant. As Jonathon Penney explains, chilling can be more subtle—we may see people change engagement and expression to more socially conforming, mainstream ones rather than experimental, nonmainstream ones.[154]

Public health officials feared this kind of chilling effect after news broke that Grindr had shared its customers' HIV status with analytics firms.[155] A Grindr subscriber told Vox that he removed his HIV status from his profile after learning about the disclosure. He explained that, "Some 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."[156] This example is consistent with

---

[149] Jonathan W. Penney, *Chilling Effects: Understanding Them and Their Harms* (on file with author); Jonathon W. Penney, *Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study*, 6 INT. POLICY REV. 1 (2017) https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling- effects-online-comparative-case; Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior*, in CAMBRIDGE UNIVERSITY HANDBOOK ON SURVEILLANCE LAW (David Gray et al. eds., 2017); Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMM. 296 (2016).

[150] Penney, supra note, at 58-62.

[151] Khan, *supra* note, at.

[152] S. Mowlabocus, *Porn 2.0? Technology, Social Practice, and the New Online Porn Industry*, in PORN.COM: MAKING SENSE OF ONLINE PORNOGRAPHY (F. Attwood, ed. 2010); Maris et al., *supra* note, at 2.

[153] Maris et al, *supra* note, at 2; Matthews & Tucker.

[154] Penney, *supra* note, at 66.

[155] 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. 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 "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.*

[156] Ghorayshi & Ray, *supra* note.

studies showing that victims of nonconsensual pornography tend to withdraw from online engagement and expression.[157]

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."[158] 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."[159] 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.[160]

When people's nude photos are posted online without consent, they see themselves as just their genitals or breasts and fear that others will see them that way. For example, in 2018, a young lawyer stayed in a hotel for work.[161] Without her knowledge or permission, a hotel employee placed a camera in the bathroom and recorded her as she showered.[162] The employee posted the video and her personal details on various porn sites.[163] 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.[164]

Private-sector handling of intimate information can jeopardize the trust that is essential for the development of intimate relationships. As Charles

---

[157] Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117, 125–26 (2016); *see also* Jonathon W. Penney, *Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study*, 6 INTERNET POL'Y REV., May 26, 2017, at 1, 3. *See generally* CITRON, HATE CRIMES IN CYBERSPACE, *supra* note, at; Danielle Keats Citron, *Civil Rights In Our Information Age*, in THE OFFENSIVE INTERNET (Saul Levmore & Martha C. Nussbaum, eds. 2010); Jonathon W. Penney & Danielle Keats Citron, *When Law Frees us to Speak*, FORDHAM L. REV. (2018). 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, at 385; Citron, *Cyber Civil Rights*, *supra* note.

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

[159] ANITA ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 15 (2011).

[160] Citron, *supra* note, at 1882-83.

[161] Phone Interview with Gina Doe (October 15, 2018) (notes on file with author); Interview with Gina Doe (May 3, 2019) (notes on file with author). I will explore the invasion of Gina Doe's sexual privacy in greater detail in my book project.

[162] October 15, 2018 Interview.

[163] *Id.* The perpetrator sent a video of her showering to her LinkedIn contacts. *Id.*

[164] *Id.*

Fried argued years ago, privacy is the oxygen for intimacy.[165] Intimacy develops as partners share vulnerable aspects of themselves.[166] 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 will stop using their services, to the detriment of the project of intimacy. The loss of trust is profound when sites disclose people's nude images without consent. People stop dating for fear that future partners will frequent revenge porn sites and porn sites to post their nude photos in violation of their trust and confidence.[167]

Equal opportunity is on the line as well. The surveillance of intimate life is particularly costly to women and marginalized people. 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.[168] Nonconsensual porn impacts women and girls far more frequently than men and boys. Individuals who identify as sexual minorities are more likely than heterosexual individuals to experience threats of, or actual, nonconsensual pornography.[169] 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.[170] The damage stems from prevailing stereotypes and the social construction of sexuality. When heterosexual men appear in videos having sex, they are socially empowered by the performance whereas women and sexual minorities are demeaned, disempowered, and viewed as stigmatized.[171]

---

[165] CHARLES FRIED, AN ANATOMY OF VALUES (1970).

[166] *Id.* at; Citron, *Why Sexual Privacy Matters for Trust*, *supra* note, at.

[167] Citron, *Why Sexual Privacy Matters for Trust*, *supra* note, at. When domestic violence victims learn that that they were being tracked on their cellphones, they fear purchasing new phones lest abusers install cyber stalking app again.

[168] Asia A. Eaton et al., 2017 *Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration*, CYBER C.R. INITIATIVE 12 (June 2017). For other studies confirming this finding, see Citron, *Sexual Privacy*, supra note, at 1919 n. 307.

[169] *See* Citron, *Sexual Privacy*, *supra* note, at 1920 (discussing various studies confirming this finding); Ari Waldman, Law, Privacy, and Online Dating: 'Revenge Porn' in Gay Online Communities, 44 Law & Social Inquiry 987 (2019) (discussing studies showing that 15 percent of lesbian, gay, and bisexual internet users report that someone has threatened to share their explicit images and 7 percent say that someone has actually done it).

[170] Waldman, *supra* note, at.

[171] Citron, Hate Crimes in Cyberspace, supra note, at; Citron, Sexual Privacy, supra note, at.

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 15,000 deep fake videos online are deep fake sex videos and 99 percent of those videos involve inserting women's faces into porn without consent.[172] In the past year, the number of deep fake sex videos have grown exponentially as have deep fake sex videos featuring women without consent.[173]

Consider the fem-tech market's potential disproportionate impact on women.[174] According to media reports, some employers and health insurers have access to employees' period- and fertility-tracking apps. Women's intimate information could be used to raise the cost of employer-provided health insurance, adjust wages, or scale back employment benefits.[175] It could impact the ability to obtain life insurance, keep jobs, and get promotions. Medical researcher Paula Castano explains that the information tracked by fertility apps raise concerns because they offer little insight as a medical clinical matter and "focus on variables that affect time out of work and insurance utilization."[176]

If intimate information is shared with data brokers, it could be used in the scoring of individuals, to their detriment. As the Federal Trade Commission explains, data brokers' scoring processes are not transparent, which means that "individuals cannot take actions to mitigate the impact of negative scores, such as being limited to ads for subprime credit or receiving different levels of service from companies."[177] "An insurance company could use scoring products to infer that individuals to classify

---

[172] Deeptrace Labs, *The State of Deepfakes: Landscape, Threats, and Impact* 6 (September 2019), *available at* https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf. 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). These sites generate income from advertising. Indeed, as the first comprehensive study of deepfake video and audio explains, "deepfake pornography represents a growing business opportunity, with all of these websites featuring some form of advertising." *Id.*; *see generally* Chesney & Citron, *supra* note, at.

[173] Zoom Interview with Henry Adjer (June 10, 2020) (notes on file with author).

[174] As discussed above, this is the explicit goal of fem-tech companies.

[175] Drew Harwell, *Is Your Period App Sharing Your Intimate Data with Your Boss?*, WASHINGTON POST (April 10, 2019). 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.*

[176] Harwell, supra note, at.

[177] Federal Trade Commission, *supra* note, at 48.

individuals as higher risk."[178] Scoring products could negatively impact the interest rates charged on loans.[179] News about the disproportionately higher creditworthiness of men as compared to women for Apple's new credit card demonstrates the point.

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.[180] As more intimate information is collected, used, and shared, the more it will 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.[181] A wealth of scholarship and research explores the discriminatory impacts of algorithmic discrimination in the commercial sector.[182] A prevailing concern is that algorithmic tools "replicate historical hierarchies by rendering people along a continuum of least to most valuable."[183]

---

[178] *Id.*

[179] Rosato, *supra* note, at.

[180] Petition for Rulemaking Concerning Use of Artificial Intelligence in Commerce, https://epic.org/privacy/ftc/ai/EPIC-FTC-AI-Petition.pdf. *See generally* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 19 (2014).

[181] See, e.g., Complaint and Request for Investigation filed by Electronic Privacy Information Center, In the Matter of Airbnb, Inc. (filed with FTC on February 26, 2020). EPIC raised concerns about Airbnb's deployment of "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. 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" among other information. *Id.* at 5. Airbnb's algorithm claims to identify "negative traits" including whether a person is "involved in pornography . . . or sex work" or "has interests that indicate negative personality or behavior traits." *Id.*

[182] 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 (April 2018), https://medium. com/s/story/data-violence-and-how-bad-engineering-choices-can-damage-society-39e44150e1d4; I. Raji & Joy Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, Conference on Artificial Intelligence, Ethics, and Society (2019), available at https://www.media.mit.edu/projects/actionable-auditingcoordinated-bias-disclosure-study/publications/.

[183] West, Whittacker & Crawford, supra note, at 10. See also Jevan Hutson et al., *Debiasing Desire: Addressing Bias & Discrimination on Intimate Platforms*, https://arxiv.org/pdf/1809.01563.pdf; Sasha Costanza-Chock, *Design Justice, A.I. and*

The opacity of commercial algorithms makes identifying and challenging discrimination difficult.[184] 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 all-women's colleges along with any resume that included the word "women's."[185] Amazon abandoned the tool when it could not ensure that it was not free of bias against women.

B. Surveying the Harm

The wide-spread collection, storage, use, and disclosure of intimate information risks emotional, physical, and reputational harm. It makes people vulnerable to manipulation, blackmail, and extortion.[186] 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 just one of many exposed in the hack. He committed suicide days after the public learned about the hack. Gibson's wife explained that her husband's suicide note described his deep shame about having his name on the site. She explained her husband was mourning the loss of his job. As his daughter explained, Gibson resigned—or was urged to resign—after the church learned about the

---

Escape from the Matrix of Domination, JOURNAL OF DESIGN AND SCIENCE (July 2018), https://jods.mitpress.mit.edu/pub/costanza-chock; Kate Crawford, *Artificial Intelligence's White Guy Problem*, N.Y. Times (June 26, 2016), https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html.

[184] https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf (arguing that HireVue's hiring algorithms "are likely to be biased by default" and keeps secret the "training data, factors, logic, or techniques used to generate each algorithmic assessment"). Indeed, career staff in the offices of state attorney generals 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.

[185] J. Dastin, *Amazon scraps secret AI recruiting tool that showed bias against women*, REUTERS, *available at* https://www.reuters.com/ article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/.

[186] 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).

site.[187] "We all have things 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," she noted.[188] Gibson's son spoke at his memorial service, noting that shame killed his father.[189] Gibson's fear about losing his job was well-founded. Victims of sexual-privacy invasions have been fired or encountered great difficulty obtaining work.[190]

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. For seven months in 2018, victims lost 332,000 dollars to these scams. More than 89,000 people were targeted, and on average they paid 540 dollars. Increasingly, criminals are targeting high-earning victims, including company executives, doctors, and lawyers.[191]

The national security implications of this kind of activity are also significant. The concentration of sensitive information on dating sites presents an inviting target for governments seeking leverage over political activists, dissidents, or foreign agents.[192] National security experts raised these concerns after the Chinese government bought the gay dating app

---

[187] Jon Robson, *Episode 5: The Yes Ladder*, BUTTERFLY EFFECT PODCAST (aired November 3, 2017), https://www.stitcher.com/podcast/the-butterfly-effect-with-jon-ronson/e/52105431?autoplay=true.

[188] https://www.buzzfeednews.com/article/mbvd/pastor-exposed-by-ashley-madison-hack-commits-suicide.

[189] Jon Robson, *Episode 5: The Yes Ladder*, BUTTERFLY EFFECT PODCAST (aired November 3, 2017), https://www.stitcher.com/podcast/the-butterfly-effect-with-jon-ronson/e/52105431?autoplay=true. Gibson was not the only suicide related to the hack of Ashley Madison. Two Canadian citizens killed themselves in the wake of the leak. Chris Baraniuk, *Ashley Madison: Suicides over website hack*, BBC (Aug. 24, 2015).

[190] DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014); see, e.g., Complaint, FTC et al. v. EMP Media, No. 18 CV 00035, at ¶ 47 (D. Nev. Jan. 9, 2018) (victims of nonconsensual pornography attest to fear of losing jobs).

[191] Isobel Asher Hamilton, *Criminal Groups Are Offering $360,000 Salaries to Accomplices who can Help them Scam CEOs about their Porn Watching Habits*, BUSINESS INSIDER (Feb. 24, 2019).

[192] "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. 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.*

Grindr.[193] 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."[194]

Criminals and hostile states are not the only ones who exploit intimate information in ways that undermine people's well-being. When companies use people's acute emotional fragility or membership in a protected class to override their wishes, their actions can be viewed as a "dark pattern."[195] "The Spinner" exemplifies the troubling nature of dark patterns. It promises to bend the will of people's intimate partners with its advertising services. The online service sends innocent-looking links to people via text that, when clicked, creates cookies that send targeted advertisements.[196] The company claims to have swayed people to get back together, to initiate sex, and to settle their divorces. The company's most requested service is its "initiating sex campaign," which sends ads trumpeting reasons why people should initiate sex.

Another illustration of troubling manipulation is period-tracking app FEMM, which uses subscribers' intimate information to dissuade them from terminating their pregnancies. An anti-abortion group runs the app, but it does not tell that to subscribers.[197] The app's marketing materials

---

[193] Steven Blum, *What Does a Chinese Company Want with Gay Hookup App Grindr?*, LOS ANGELES MAG. (Nov. 4, 2019), https://www.lamag.com/citythinkblog/grindr-china-fbi/.

[194] Josh Rogan, *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/.

[195] STIGLER COMMITTEE ON DIGITAL PLATFORMS 240-41(2019). 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 sensitive data is used to 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. Such systems might not be understood as deceptive under traditional understanding of consumer protection laws. *Id.* at 249.

[196] Parmy Olson, *For $29, This Man Will Help Manipulate Your Loved Ones With Targeted Facebook and Browser Links*, FORBES (January 15, 2019, 7:20 a.m.); Fiona Tapp, *New Service Promises to Manipulate Your Wife Into Having Sex With You*, ROLLING STONE (August 18, 2018, 11:38 am EST).

[197] Jessica Glenza, *Revealed: Women's Fertility App Run By Anti-Abortion Campaigners*, THE GUARDIAN (May 30, 2019),

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 a network of doctors and nurses to provide you the best health care. We're a new revolution in women's health!"[198] The app provides materials claiming that birth control is unsafe and highlighting information that promotes pregnancy. The app misleads subscribers about its motives and propagates misinformation.

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 the provision of health care.[199] It generally presumes the propriety of commercial collection of personal data.[200] As William McGeveran explains in his influential privacy casebook, American law treats the processing of personal data as both inevitable and pro-social.[201]

1. Privacy Legislation

American privacy law generally does not curtail data collection.[202] Instead, it focuses on procedural protections, such as ensuring the transparency of corporate data practices (referred to as notice) and securing certain rights over personal data (referred to as choice).[203] Even its more

---

https://www.theguardian.com/world/2019/may/30/revealed-womens-fertility-app-is-funded-by-anti-abortion-campaigners.

[198] https://play.google.com/store/apps/details?id=org.femmhealth.femm&hl=en_US

[199] The Children's Online Privacy Protection Act of 1998 is the rare exception. It limits the collection of children's online information to instances where parents have explicitly provided consent. Similarly, in the EU, the GDPR protects information pertaining to individuals' "sex life" as sensitive information, precluding its collection except upon explicit consent.

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

[201] WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 382-83 (2016); 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 (2007).

[202] Citron, *Privacy Policymaking of State Attorneys General*, *supra* note, at 771. Some states limit commercial contexts in which Social Security numbers and zip codes can be collected.

[203] *See, e.g.*, CAL. BUS. & PROF. CODE § 22575 (West 2016); CAL. CIV. CODE § 1798.100 (West 2018). State attorneys general played an important role in getting legislation passed to require privacy policies. Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 764-65 (2016).

reform-oriented elements sometimes continue this trend. The California Consumer Privacy Act (CPPA), enacted in 2018, for example, gives consumers the right to know what personal information has been collected and to opt-out of its sale.[204]

So long as companies post privacy policies and offer opt-out rights under state law, they can largely collect, use, and sell intimate information without limitation.[205] It should therefore not be a surprise that Grindr's privacy policy warns that its advertising partners "may be collecting information from you."[206] The fem-tech market is doing the same. A recent study showed that ten popular fem-tech apps including Clue sold subscribers' personal information to at least 135 companies.[207] Individuals should not be reassured if companies pledge to de-identify intimate information before selling it. Intimate information can be easily re-identified when combined with other information.[208]

Under federal and state law, companies must store intimate information in a reasonably secure manner. Legal obligations stem from data security,[209] data disposal,[210] encryption,[211] breach notification,[212] and

---

[204] CAL. CIV. CODE § 1798.100, 1798.105, 1798.110, 1798.120 (West 2018). Under the California Online Privacy Protection Act, websites must detail the categories of personal information that they collect and the categories of third parties with whom that information may be shared. On the CCPA generally and its comparison to GDPR, see Anupam Chander, Margot Kaminski, and William McGeveran, *Catalyzing Privacy Law*, MINN. L. REV. (forthcoming 2020).

[205] CAL. CIV. CODE § 1798.100, 1798.105, 1798.110, 1798.120 (West 2018). Of course, compliance with notice requirements isn't 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, at. Many consumers will not invoke their opt-out rights due to the stickiness of defaults and the sheer number of companies that would 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).

[206] Thomas Germain, *Popular Apps Share Intimate Details About You With Dozens of Companies*, CONSUMER REPORTS (January 14, 2020), https://www.consumerreports.org/privacy/popular-apps-share-intimate-details-about-you/

[207] Rosato, *supra* note, at.

[208] Daniel Kondor et al., *Towards Matching User Mobility Traces in Large-Scale Datasets*, IEEE, https://ieeexplore.ieee.org/document/8470173.

[209] *See, e.g.*, CAL. CIV. CODE 1798.81.5(b) (West 2016); Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 Mass. Code Regs. 17.00 (2010).

[210] *See, e.g.*, CONN. GEN. STAT. 42-471 (2015); MASS GEN. LAWS ch. 931 2.

[211] *See, e.g.*, CAL. CIV. CODE 1798.85(a)(3).

[212] *See, e.g.*, CAL. CIV. CODE 1798.82.

unfair and deceptive acts and practice (UDAP) laws.[213] Companies may have a duty to adopt certain data security practices, such as having a comprehensive data-security program addressing potential risks to consumers.[214] As explored below, companies have faced suit for inadequately securing intimate information.

One might assume think 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), 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. It covers particular healthcare providers (known as covered entities), such as medical practices, hospitals, and health insurance companies.[215] HIPAA, for instance, requires that covered entities obtain consent before using or disclosing individually identifiable "protected health information." That provision does not apply to the broad array of non-covered entities, including fem-tech apps, search engines, medical information sites, or dating sites.[216] When a dating app collects information about individuals' HIV status or when a femtech app stores the dates of abortions and miscarriages, it is not constrained by HIPAA's privacy rules.

2. Privacy Policymaking of Law Enforcers

In the rare case, the Federal Trade Commission (FTC) and state Attorneys General (AG) have set norms around the collection and storage of intimate information.[217] Federal and state UDAP laws provide support

---

[213] *See, e.g.*, CONN. GEN. STAT. 42-11-a-110q.

[214] William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1140, 1175-1180 (2018).

[215] In passing HIPAA in 1996, Congress delegated authority to the Department of Health and Human Services to enact national data privacy or confidentiality and data security standards. Allen, supra note, at 113-14. DHHS issued its Standards for Privacy of Individually Identifiable Health Information known as the HIPAA Privacy Rule. 45 CFR 164.524. The HIPAA Privacy Rule, enacted in 2000, 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. *Id.*

[216] Period-tracking apps 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, at.

[217] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016). The Consumer Financial Protection Bureau also has the authority to regulate abusive conduct, at least within the banking and financial services sector. Under 12 U.S.C. 5531, an abusive practice is one that materially interferes with the ability of consumers to understand a term or condition of a "consumer financial product or

for this activity.[218] The following examples provide precedent 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. 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.[219] 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, doctor's offices that perform abortions."[220] 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."[221] Once an individual's device had been tagged, then that person would continue to see pro-life ads for the next thirty days.[222]

The Massachusetts AG's office viewed the company's collection of location data to infer women's reproductive health as constituting an unfair and deceptive business practice.[223] For the Massachusetts AG, the

---

service" or takes unreasonable advantage of their understanding of such a service or product's material risks or of their inability to protect their interests.

[218] 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. *Id.* In the late 1960s and early 1970s, state lawmakers followed the federal government's lead in adopting so-called baby Section 5 acts, that is, UDAP laws. With this authority, state attorneys general have served as crucial privacy norm entrepreneurs using their authority under state UDAP laws. *Id.* I had the great fortune of witnessing creative state AG privacy policymaking in advising then-California AG Kamala Harris from 2014 to 2016. *Id.*

[219] *In the Matter of Copley Advertising & John F. Flynn*, Assurance of Discontinuance (dated April 4, 2017), https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2017/04/nDP.pdfhttps://www.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts.

[220] *Id.*¶ 7.

[221] *Id.* ¶ 10.

[222] *Id.* ¶ 11.

[223] *Id.* 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 https://www.ftc.gov/news-events/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app. For a discussion of the norms around collection of geolocation data, *see* Danielle Citron, *BEWARE: The Perils of Location Data*, FORBES, (December 24, 2014), https://www.forbes.com/sites/daniellecitron/2014/12/24/beware-the-dangers-of-location-data/#6037ba1543cb. The U.S. Supreme Court has held that obtaining cell-site location data from third parties implicates a search under the Fourth Amendment. *United States v. Carpenter* (finding that location data "holds for many Americans the 'privacies of

advertising firm intruded upon a "consumer's private health or medical affairs or status" resulting in the "*gathering* or dissemination of private health or medical facts about the consumer without his or her consent."[224]

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.[225] 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.[226]

In another effort to curtail the collection of intimate data, the FTC sued mobile spyware company Retina-X under its UDAP authority in Section 5 of the Federal Trade Commission Act.[227] The complaint alleged that defendant's spyware injured consumers by enabling stalkers to monitor people's physical movements, sensitive information, and online activities without consent.[228] The unwanted collection of cellphone activity risked exposing victims to emotional distress, financial losses, and physical harm, including death.[229] The FTC charged that 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.[230] In 2019, 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.[231]

---

life'" and that a government with access to historic location data "achieves near perfect surveillance"); see also *United States v. Jones*. I have been advising federal lawmakers on efforts to provide stronger regulatory 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, at.

[224] *In the Matter of Copley Advertising*, ¶ 15 (emphasis added).

[225] *Id.* ¶ 20.

[226] See Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. (2011).

[227] Section 5 of the Federal Trade Commission Act prohibits unfair and deceptive acts and practices. It served as the template for state UDAP laws, which are often referred to as mini-FTC Acts.

[228] Complaint, In the Matter of Retina-X Studios, LLC, at ¶ 11-12 (U.S. Fed. Tr. Comm'n).

[229] *Id.*

[230] *Id.* ¶ 32.

[231] Agreement Containing Consent Order, In the Matter of Retina-X et al. (U.S. Fed. Tr. Comm'n); Decision and Order, In the Matter of Retina-X Studios (U.S. Fed. Tr. Comm'n).

Regrettably, the defendant was not required to refrain from selling monitoring products in the future, a result that shows another of the limits 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.[232] 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. Bollaert was convicted of 27 felony counts and sentenced to eight years of imprisonment and ten years of mandatory supervision.[233]

The FTC sued another revenge porn operator under Section 5 of the FTC Act for exploiting nude images shared in confidence for commercial gain.[234] The operator agreed to shutter the site and delete the images.[235] The FTC joined forces with the Nevada 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.[236] 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.[237]

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

---

[232] Citron, *Privacy Policymaking of State Attorneys General*, *supra* note, at 775.

[233] https://www.sandiegouniontribune.com/sdut-kevin-bollaert-revenge-porn-case-resentencing-2015sep21-story.html

[234] Complaint, In the Matter of Craig Brittain, No. C-4564 (January 29, 2015), https://www.ftc.gov/system/files/documents/cases/150129craigbrittaincmpt.pdf.

[235] Press Release, FTC, *Website Operator Banned from the 'Revenge Porn' Business After FTC Charges He Unfairly Posted Nude Photos* (Jan. 29, 2016); see generally Danielle Citron & Woodrow Hartzog, *The Decision That Could Finally Kill the Revenge-Porn Business*, ATLANTIC (Feb. 3, 2015). CCRI joined together with Without My Consent to file comment to the consent decree in that case. Comments of the Cyber Civil Rights Initiative and Without My Consent to the Federal Trade Commission (filed February 23, 2015), *available at* https://www.ftc.gov/system/files/documents/public_comments/2015/02/00007-93359.pdf.

[236] Complaint, FTC et al. v. EMP Media, No. 18 CV 00035, at ¶ 45 (D. Nev. Jan. 9, 2018); Press Release, FTC, *FTC, Nevada Obtain Order Permanently Shutting Down Revenge Porn Site MyEx* (June 22, 2018). The Nevada Attorney General argued that the site violated state UDAP law by intimidating people into paying for the removal of their photos. *Id.*

[237] FTC et al. v. EMP Media Inc., No. 18 CV 0035 (D. Nev. June 15, 2018).

"reasonable security."[238] State attorneys general, adhering to this approach, often serve as "first responders" to data breaches, at times in coordination with the FTC.[239]

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. The Vermont AG's complaint highlighted the site's failure to maintain information security policy and to use multi-factor authentication.[240] The complaint alleged that the site's inadequate security amounted to an unfair business practice that risked "significant harm to consumers' reputation, relationships, and personal life" and raised people's risk of identity theft. The case resulted in a consent decree with the FTC and settlements with state Attorneys General.

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.[241] The dating app allegedly deceived customers by breaking its promise to ensure the confidentiality of photos marked "private." Although the site had been warned about the security vulnerability more than a year earlier, it had failed to take remedial action.

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 "absolutely no sensitive data (pictures, video, chat logs) pass through (or are held) on our servers."[242] The complaint alleged that the defendant intruded on the plaintiffs' privacy by recording their communications and activities without consent in violation of the federal

[238] Citron, *Privacy Policymaking of State Attorneys General*, *supra* note, at.

[239] *Id.*

[240] Complaint, Vermont v. Ruby Corp., Civ. No. 730-12-16 (dated December 14, 2016).

[241] Press Release, N.Y. Attorney General's Office, *N.Y. State Attorney 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.

[242] First Amended Complaint, S.D. et al. v. Lovense, No. 18-CV-00688, at 33 (N.D. Cal. Aug. 24, 2018).

and state wiretap laws and state privacy tort law.[243] Subscribers brought similar claims against We-Vibe for recording information about their use of the defendant's vibrators.[244] The case settled for 3.75 million dollars.

By contrast, individuals have been unable to hold platforms accountable for hosting their nude images without consent.[245] Section 230 of the federal Communications Decency Act (CDA) has barred their efforts.[246] 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 and hateful expression. Under Section 230, providers or users of interactive computer services are shielded from liability for under- or over-filtering user-generated content.[247] Section 230(c)(1) says that providers or users of interactive computer services will not be "treated as publishers or speakers" for information provided by another information content provider.[248]

Lower federal and state courts have dismissed victims' civil claims even though site operators solicited, chose to republish, or failed to remove nonconsensual pornography.[249] Section 230 did not bar the state AG and FTC suits discussed above because they concerned site operators' own extortion schemes, not their publication of user-generated content.[250]

---

[243] *Id.* at 65. The case proceeded to discovery after the court rejected the defendant's motion to dismiss. Order Granting in Part and Denying in Part Defendant's Motion to Dismiss, S.D. v. Hytto Ltd., D/B/A Lovense, No. 18-CV-00688 (N.D. Cal. May 14, 2019).

[244] Amended Complaint, N.P & P.S. v. Standard Innovation Corp., Case No. 16-CV-08655 (N.D. Ill. Filed February 27, 2017).

[245] Danielle Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, 86 FORDHAM L. REV. 401 (2017); Danielle Keats Citron, *Cyber Mobs, Disinformation, and Death Videos: The Internet As It Is (And As It Should Be)*, 118 MICH. L. REV. (2020).

[246] Citron & Wittes, supra note, at; Written Testimony of Danielle Keats Citron, House Energy and Commerce Committee Hearing on Fostering a Healthier Internet (October 17, 2019). For an enlightening history of Section 230's adoption and judicial interpretation, see JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019).

[247] 42 U.S.C. 230(c); Citron & Wittes, *supra* note, at.

[248] 42 U.S.C. 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. 42 U.S.C. 230(c)(2).

[249] MARY ANNE FRANKS, THE CULT OF THE CONSTITUTION (2019); CITRON, HATE CRIMES IN CYBERSPACE, *supra* note, at; Danielle Citron & Mary Anne Franks, *The Internet As a Speech Machine and Other Myths Confounding Section 230 Speech Reform*, U. CHI. L. FORUM (forthcoming 2020), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532691; Citron & Wittes, supra note, at; Mary Anne Franks, *Sexual Harassment 2.0*, 71 MD. L. REV. 655, 695 (2012).

[250] CITRON, HATE CRIMES IN CYBERSPACE, *supra* note.

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 plaintiffs' lack of standing or cognizable harm under state law.[251] Those lawsuits have a greater likelihood of surviving motions to dismiss if plaintiffs have suffered financial harm like identity theft, as opposed to the increased risk of such harm.[252]

One might think anti-discrimination 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. Hiring AI systems may be mining intimate information in ways that have a disparate impact on individuals from protected groups but it has been impossible to detect and thus private suits are hard to pursue.[253]

4. Criminal Law

Only a narrow set of commercial practices—spyware and cyberstalking 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.[254] Congress passed that provision, 18 U.S.C. 2512, to "dry up" the source of equipment that is highly useful for private nonconsensual surveillance.[255]

Section 2512 makes it a crime to intentionally manufacture, sell, or advertise a device knowing or having reason to know that its design renders it "primarily useful" for the surreptitious interception of wire, oral, or electronic communications.[256] Defendants face fines of up to $10,000, up to five years imprisonment, or both. Section 2512 covers a "narrow category of devices whose principal use is likely to be for wiretapping or

---

[251] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 739-45 (2018).

[252] *Id.*

[253] https://ainowinstitute.org/discriminatingsystems.pdf (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 commercial sector); AI Now 2017 Report, https://ainowinstitute.org/AI_Now_2017_Report.pdf.

[254] Citron, *Spying Inc.*, *supra* note, at 1264.

[255] S. REP. NO. 90-1097, at 2183 (1968).

[256] 18 U.S.C. 2512(1)(b) (2012).

eavesdropping."[257] Twenty-five states and the District of Columbia have similar statutes.[258]

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. In September 2014, federal prosecutors brought Section 2512 charges against StealthGenie's CEO Hammad Akbar.[259] StealthGenie's spyware app secretly intercepted communications to and from mobile phones.[260] 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."[261] A federal judge issued a temporary restraining order authorizing the FBI to disable the site hosting StealthGenie.[262] The defendant pleaded guilty to the charges and was ordered to pay $500,000 in fines.[263] There have been no subsequent reported federal criminal cases against spyware purveyors since the StealGenie case. At the state level, prosecutions have been virtually nonexistent.[264]

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.[265] As privacy advocate James Dempsey argued and as prosecutors have confirmed, the small number of prosecutions under Section 2512 is attributable to the fact that it is hard to demonstrate that equipment is primarily designed for stealth interception of communications.[266]

Individual sexual-privacy invaders are a different matter, as my prior scholarship has explored.[267] Consider nonconsensual pornography. Today,

---

[257] United States v. Shriver, 989 F.2d 898, 906 (7th Cir. 1992).

[258] Citron, *Spying Inc.*, *supra* note, at 1265 n. 132 (collecting statutes).

[259] *Id.* at 1267.

[260] *Id.*

[261] *Id.*; Hautala, *supra* note, at (noting federal prosecutor's frustration that the primarily useful requirement makes it difficult to bring Section 2512 cases).

[262] *Id.*

[263] Department of Justice, Man Pleads Guilty to Selling Spyware and Ordered to Pay $500,000 Fine (November 25, 2014), available at https://www.justice.gov/opa/pr/man-pleads-guilty-selling-stealthgenie-spyware-app-and-ordered-pay-500000-fine.

[264] *Id.*

[265] *Id.*

[266] James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65 (1997).

[267] Citron, *Sexual Privacy*, *supra* note, at; Citron & Franks, *supra* note, at.

46 states, D.C., and Guam criminalize the posting of nude photos without consent.[268] Law enforcement has been slowly but surely pursuing cases under those laws.

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 four-fold: to situate data privacy as a matter of civil rights; 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.

A. Reframing the Conversation

In the United States, information privacy is viewed through a consumer protection lens.[269] The central theme is notice and choice.[270] So long as businesses provide notice of their data practices, then consumers are treated as having elected to trade their data for commercial services.[271] The U.S. approach has been described as "privacy self-management" and "privacy work."[272]

The consumer protection model—as it is currently constructed—is both descriptively and conceptually flawed.[273] Firms provide "notice" in privacy policies while "consent" is inferred from people's decision to visit sites, download apps, and purchase goods.[274] Both are fictions. As currently

---

[268] In 2014, before Dr. Mary Anne Franks and the Cyber Civil Rights Initiative began working with lawmakers, three states criminalized the practice. See Citron, *supra* note, at (discussing the development of so-called revenge porn laws); Mary Anne Franks, *Reform From the Front Lines*, FLA. L. REV. (2018).

[269] Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952 (2017); Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROTECTION REV. 423 (2018); Neil Richards & Woodrow Hartzog, *The Pathologies of Consent*, 96 WASH. U. L. REV. (2019).

[270] The California Online Privacy Protection Act requires that entities notify California residents about their data collection practices. Most companies follow CalOPPA because of the significant likelihood of any service collecting information from California residents.

[271] JULIE COHEN, CONFIGURING THE NETWORKED SELF (2015).

[272] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013); Daniel J. Solove, *The Myth of the Privacy Paradox*, GEO. WASH. L. REV. (forthcoming). Alice Marwick invokes the concept of privacy work, drawing on a feminist framework that aptly captures uncompensated work that is disproportionately shouldered by women and marginalized communities. See ALICE MARWICK, HIDDEN: NETWORKED PRIVACY AND THOSE LEFT OUT (forthcoming).

[273] Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1658 (1999).

[274] Richards & Hartzog, *The Pathologies of Consent*, supra note, at.

constructed, notice rarely provides individuals with relevant information that they can understand and use. It rarely, if ever, provides details about third-party marketing. It does not seek express, written consent in a form designed to inform people about a firm's practices, and it does not give them an option of declining the collection of their personal information if they use the service.

Even when firms make an effort at directly notifying individuals about their practices, the consent provided is hardly meaningful. Lived experience casts doubt on the proposition that people have really consented to the trade of their personal data for services.[275] When a pop up appears online, people tend to click "I Agree" because it is less onerous than reading dense privacy policies provided.[276] Evan Selinger and Brett Frischmann talk about this as a form of manufactured consent and rightly so.[277] Individuals have difficulty appreciating low-probability harms that nonetheless happen to a significant percentage of people.

Further complicating the ability to secure meaningful consent is the fact that companies have every incentive, in the words of Woodrow Hartzog, to "hide the risks in their data practices though manipulative design, vague abstractions, and complex words."[278] Firms' website interfaces and default settings are designed to maximize data collection. As Hartzog explains further, businesses "engineer . . . [interactions] to expedite the transfer of rights and relinquishment of protections."[279]

A consumer protection approach not only fails to satisfy its goal of notice and choice, it insufficiently captures the stakes.[280] To be sure, a firm's collection of intimate data might constitute deception if its privacy policy says one thing and does another. But, in addition, it might undermine the

---

[275] Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 953 (2017).

[276] WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 130 (2018).

[277] BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY 209-210 (2018) (explaining that people feel compelled to agree, undermining any desire to object, and thus informed consent is really manufactured or manipulated consent). Shoshana Zuboff talks about the notice and consent regime as a kind of psychic numbing. ZUBOFF, supra note, at.

[278] Testimony of Woodrow Hartzog, "Policy Principles for Federal Data Privacy Framework," Senate Committee on Science, Technology, and Commerce (February 17, 2019), *available at* https://www.commerce.senate.gov/services/files/8B9ADFCC-89E6-4DF3-9471-5FD287051B53.

[279] *Id.*

[280] *See* Danielle Keats Citron & Mary Anne Franks, *The Internet as Speech Conversion Machine and Other Myths Confounding Section 230 Reform*, U. CHI. LEGAL F. (forthcoming); Citron, *Sexual Privacy*, *supra* note; Citron, *Cyber Civil Rights*, *supra* note.

crucial values that sexual privacy protects and impede a fair chance to work, obtain housing, afford insurance, and express oneself.[281] The consumer protection model lacks the capacity and even the vocabulary with which to protect these interests.[282]

In certain contexts, law protects crucial life opportunities and social goods as civil rights.[283] Federal and state civil rights laws secure the ability to work, attend school, use the telephone, secure housing, and vote on equal terms.[284] I am not suggesting that civil rights laws apply to the private sector surveillance of intimate data, which they mostly do not.[285] Nonetheless, a civil rights framing brings into focus that far more than consumer choices are in jeopardy when firms amass intimate information.[286] The ability to engage in life's crucial activities hangs in the balance, especially for women, sexual minorities, and racial minorities and often on an intersectional basis.

Situating sexual privacy in the civil rights conversation is important.[287] Law plays a crucial expressive role.[288] It teaches us why certain interests matter and why they warrant law's protection.[289] A civil rights framing would attest to the close relationship between reservoirs of intimate data and opportunities essential for human flourishing. I am not suggesting that civil rights laws cover all freedoms and social goods in need of protection

---

[281] Julie Cohen, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY LIFE (2012).

[282] NEIL M. RICHARDS, WHY PRIVACY MATTERS (forthcoming) (on file with author).

[283] Title VII; FMLA; Title IX; Americans with Disabilities Act.

[284] Danielle Citron & Mary Anne Franks, *Cyber Civil Rights in an Age of COVID*, HARV. L. REV. BLOG (May 14, 2020), https://blog.harvardlawreview.org/cyber-civil-rights-in-the-time-of-covid-19/.

[285] Of course, Title VII might be understood to ban discriminatory hiring practices that involve relying on intimate information, as I have suggested in previous work. See Citron, Hate Crimes in Cyberspace, supra note, at. There is also the Genetic Information Nondiscrimination Act, which bans employers from using genetic information in employment decisions.

[286] As scholars have explored, antidiscrimination laws like Title VII are ill-suited to address the use of discriminatory algorithms in employment matters. See Deborah Hellman, *Measuring Algorithmic Fairness*, 106 VA. L. REV. 811 (2020); Pauline Kim, *Data Discrimination at Work*, 58 WILLIAM & MARY L. REV. 857 (2018); Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016).

[287] I will be further exploring this argument in later work. Danielle Keats Citron & Courtney Hinkle, *Privacy, a Matter of Civil Rights* (in progress).

[288] CITRON, HATE CRIMES IN CYBERSPACE, supra note, at; Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373 (2009).

[289] Citron, *Law's Expressive Value*, *supra* note, at.

(they do not).[290] Their reach is further limited by the state action doctrine.[291] These limitations curtail the expressive power of those laws.[292] Nonetheless, situating private sector surveillance of intimate life as a matter of civil rights and not just consumer choices helps begin the conversation about what those freedoms *should* be in the context of privacy law specifically and civil rights law more generally.

Some legislators and law enforcers have underscored the connection between privacy and civil rights. New York AG Letitia James attributed her investigation of the gay dating app Jack'd to the special importance of privacy to the LGBTQ community. As she noted, "[a]pproximately 80 percent of the app's users were individuals of color and had reason to fear discrimination from the exposure of their personal information or private photographs."[293]

Understanding privacy as a matter of civil rights provides inspiration for reform. Data protection laws tend to focus on process, such as notice of an entity's data practices and the ability to correct mistakes.[294] By contrast, civil rights law moves in a more substantive direction by limiting certain conduct and requiring affirmative obligations.[295] Under civil rights law, caretakers of crucial spaces must maintain them in ways that promote equal

---

[290] In her important new book, Robin West calls for a transformative understanding of civil rights that does not merely prohibit discrimination but that entails rights essential to the justice of the nation. ROBIN L. WEST, CIVIL RIGHTS: RETHINKING THEIR NATURAL FOUNDATION (2019).

[291] *Id.* (exploring the various ways that civil rights laws have failed to fulfill their potential to protect social goods themselves).

[292] As Alice Walker eloquently explained, "'Civil rights' is a term that did not evolve out of black culture, but rather out of American law. As such, it is a term of limitation. It speaks only to physical possibilities—necessary and treasured, of course—but not of the spirit. Even as it promises assurance of greater freedoms it narrows the area in which people might expect to find them." ALICE WALKER, IN SEARCH OF OUR MOTHER'S GARDENS 335 (1983).

[293] Press Release, *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#:~:text=NEW%20YORK%20%E2%80%93%20New%20York%20Attorney,%2C%20bisexual%2C%20and%20transgender%20community.

[294] Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020).

[295] Woody Hartzog and Neil Richards have laid important groundwork for a substantive turn for privacy law in their coauthored scholarship. See, e.g., *id.*; Richards & Hartzog, *The Duty of Loyalty*, supra note.

access and holds them accountable when they fail to do so.[296] School administrators, private employers, hotel proprietors, and restaurant owners have responsibilities to ensure that their spaces are free of discrimination and abuse.[297] Educational institutions and employers must craft and enforce anti-discrimination policies, and they must respond to credible complaints of sexual harassment or racial abuse. Hotels and restaurants must ensure that individuals are not denied service on the basis of protected characteristics.

Privacy law should follow this substantive turn. We see a measured move in that direction in the wake of the COVID-19 pandemic. A bill recently proposed by Senators Warner and Blumenthal frames the recognition of a "right to privacy" in "emergency health data" as a civil rights matter.[298] It requires the adoption of reasonable safeguards against unlawful discrimination based on emergency health data. It prohibits discrimination against, or otherwise making unavailable, goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation" and the right to vote on the basis of "emergency health data." The bill would have the Secretary of Health and Human Services work with the U.S. Commission on Civil Rights and the FTC to submit a report examining how the collection, use, and disclosure of COVID-19 health information impacts civil rights issues.

Recognizing privacy as a matter of civil rights may provide support for stronger privacy protections at the federal and state level. Information privacy is having a zeitgeist moment. Dozens of federal privacy bills are under consideration. At the state level, privacy laws are being proposed at a rapid clip.[299] A civil rights framing might incentivize lawmakers to adopt robust privacy protections rather than watering bills down and letting bills die in committee. If privacy bills are described as consumer protection matter, then lawmakers will be more comfortable arguing that the profitability of firms should be balanced against consumer interests. Lawmakers would be less inclined to barter away civil rights against discrimination to protect firms' profits or to reduce administrability

[296] Danielle Keats Citron & Mary Anne Franks, *Cyber Civil Rights in the Age of COVID-19*, HARV. L. REV. BLOG (May 19, 2020), https://blog.harvardlawreview.org/cyber-civil-rights-in-the-time-of-covid-19/.

[297] Title VII, Title IX.

[298] https://epic.org/privacy/covid/Public-Health-Emergency-Privacy-Act.pdf

[299] CCPA; Washington state.

costs.[300] Indeed, in some circumstances, civil rights do not allow for any bartering at all—this is certainly true voting.

In recognizing privacy's centrality to human flourishing, the U.S. would move in a direction that most of the world has already adopted. In the European Union, information privacy (better known as data protection) is a "fundamental right" essential for "dignity, personality, and informational self-determination."[301] This is not a wholesale endorsement of the EU's General Data Protection Regulation—its overall tack is overly focused on procedural commitments.[302] Instead, it is to note that most of the world views data privacy as a human right.

B. Special Protections for Intimate Information

Before turning to the special protections owed intimate information, I have to note the need for strong baseline protections for *all* personal data collected in the private sector.[303] All of the reasons why we need sexual privacy support comprehensive data protection in the United States. Technological advances may soon enable firms to turn innocuous personal data into sensitive information—including intimate information—with a high degree of accuracy.[304] Paul Ohm and Scott Peppet have memorably termed this prospect "when everything reveals everything."[305] We need to stem the tide of over-collection and to restrict downstream use, sharing, and storage of personal data in part to protect intimate information.

No matter, whether or not lawmakers move on any of the countless comprehensive data privacy bills under consideration at the federal and state level Intimate information warrants special protection right now. This

---

[300] We see some accommodation of economic interests in Title VII in its exclusion of small firms. I am grateful to Neil Richards for exploring this point with me.

[301] Paul M. Schwartz & Karl-Nikolaus Pifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115 (2017); see also Paul M. Schwartz, *Global Data Privacy Law: The EU Way*, NYU L. REV. (2018).

[302] Bert-Jaap Koops, *The Trouble with European Data Protection Law*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692.

[303] 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 NYU L. REV. 1814 (2011). Federal and state laws address what information constitutes personal information in different ways. An organizing principle is whether an individual is identified or can be reasonably identified.

[304] Paul Ohm & Scott Peppet, *What If Everything Reveals Everything?*, *in* BIG DATA IS A MONOLITH 53 (Cassidy Sugimoto et al, eds. 2016).

[305] *Id.* That possibility certainly supports the call for strong baseline rules for the handling of personal information.

section focuses on areas worthy of reform. Certain activity should be off limits, including the collection and use of intimate information in certain contexts. Additional remedies should be available to address violations, including a "stop processing" order until violations are fixed. We might also consider reserving the possibility of a data death penalty.

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 undermines the values that sexual privacy protects and risks people's well-being.

To be sure, 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. To be sure, no legal approach can guarantee this outcome. The following reforms, however, are offered with that goal in mind.

Firms should be required to obtain meaningful consent before collecting intimate information. The "gold standard of consent" combines the "knowing and voluntary" waiver standard from constitutional law and the informed consent standard from biomedical ethics.[306] Requests for consent also must be "*infrequent* [and] the risks of giving consent must be *vivid* and easy to envision."[307] Last, firms can only seek consent to collect intimate data for a legitimate business purpose.

As to the knowing requirement, requests for consent should be clear and understandable. They should explain what intimate data would be collected, how it would be used by the firm to provide its service, and how long it would be retained. Requests for consent should be conspicuous. Where possible, they should be made separately from the process of signing up for a service. They should be designed in a way that enhances the likelihood that people will understand them.[308] Lessons from design

[306] Richards & Hartzog, supra note, at 1465, 1475.

[307] *Id.* at 1492. Richards and Hartzog also argue that for consent to be meaningful, it must occur in contexts where people have the incentive to take the request seriously. For platforms collecting sensitive information like dating apps, they argue that people may be more inclined to consider the risks so long as requests do not arrive in dribs and drabs. *Id.* at 1498.

[308] On this score, see the important work of Ryan Calo. *See, e.g.*, M. Ryan Calo, *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012). Calo

psychology can be leveraged to make it more likely that people consider the question rather than simply clicking "I Agree."[309]

As for voluntariness, requests for consent must not be "take it or leave it" if a firm can provide that service without collecting intimate data. Adult sites, for instance, do not need to track people's searches to provide their services. Thus, people should be able to decline collection requests and still be able to browse adult sites. Firms also should not make it difficult for people to deny requests or engage in other activity designed to "coerce, wheedle, and manipulate people to grant it."[310]

The context of the request should signal that the person answered the request with care. Firms should not be permitted to make several requests.[311] They must limit their requests. When requests for consent are infrequent, individuals have time to consider them and likely will not feel overwhelmed. With frequent requests, individual just agree to stop being hasseled.[312] Firms also should spell out the risks in concrete and vivid terms so that individuals understand what happens if their intimate data is leaked or improperly used or shared.

Under this approach, first-party data collectors would have to obtain people's meaningful consent before amassing intimate information. They could only request consent to collect intimate data for a legitimate business reason. Sometimes, however, the collection of intimate data is necessary for the service to function at all. This is true of dating, fertility, and period-tracking apps. In such a case, requests for collection would have to make clear that the service depends upon the collection of intimate data and that it will be used only to provide that service and no other reason. In that case, firms could decline to provide services to people who reject their request.

No so for third-party data collectors. Third-party data collectors must make clear that individuals can decline their requests without consequence. 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. If

---

explores various mechanisms for delivering notice that rely on consumer experience rather than entirely words or symbols. *Id.* at 1039-47.

[309] See European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 (Adopted on May 4, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[310] Richards & Hartzog, *supra* note, at 1489.

[311] *Id.* at 1494.

[312] *Id.*

adopted, they would not only have to seek permission from individuals, but requests would have to be made so that people can easily refuse and know that their refusals will have no consequences (beyond not getting personalized ads).

Admittedly, this requirement would be a significant setback for advertisers and data brokers. Data brokers would have to seek explicit consent before collecting intimate information. So would advertisers that track intimate information on porn sites, period-tracking services, and dating apps. To be clear, meaningful consent would only apply to intimate information. The advertising and data brokerage industries would not end. Instead, the default presumption that intimate information can be collected unbeknownst to individuals and without their permission would have to end. The sky will 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 coauthor Mary Anne Franks has long argued that nude images should not be posted online without written consent. 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 before 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.[313] As we noted then, written consent would not prevent the posting of nude photos, just nude photos where the subject did not consent (or at least where 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 data brokers and advertisers. If firms want to collect intimate information, then they should obtain people's meaningful consent to do so.

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

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.[314] HIPAA's Privacy Rule permits data use necessary for the treatment, payment, or health care system operations data and requires consent for any uses beyond those purposes. Under federal law, cable providers generally may not disclose subscribers' information to anyone without subscribers' consent.[315]

An alternative approach to seeking meaningful consent would be to limit the collection of intimate information to instances where entities have a legitimate, reasonable basis for collecting intimate data and where individuals would reasonably expect it.[316] 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 that unknown shadowy actors are amassing their intimate information in digital dossiers. In my view, this approach is far less compelling than requiring meaningful consent. The data collection imperative for intimate data would continue with too little friction restraining it.

Certain collection practices should be off-limits. Law should prohibit services whose raison d'être is the nonconsensual collection of intimate data. Period the end, no exceptions. Software that "undresses" women in

---

[314] 740 Ill. Comp. Stat. 14/20(2).

[315] Cable Privacy Protection Act. The European Union's General Data Protection Regulation requires opt-in consent for the placement of tracking cookies. For sensitive information including information about individuals' sexuality, companies can only collect such information with explicit, affirmative consent.

[316] See the thoughtful proposals of Cameron F. Kerry in Proposed Standards for Data Collection in Privacy Legislation, Lawfare, https://www.lawfareblog.com/data-collection-standards-privacy-legislation-proposed-language ("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 noted, 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. . . . 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."

photographs runs afoul of this mandate; so do apps that facilitate the secret and undetectable monitoring of someone's cellphone and sites hosting nonconsensual pornography and deep fake sex videos.[317] 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, as I have long argued they should.[318]

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 are precluded from collecting information that exclusively concerns individuals' First Amendment activities. In *NAACP v. Alabama*, the Supreme Court struck down a court order requiring the civil rights group to create and produce its membership list on the ground that privacy in group associations is indispensable to preserving the freedom to associate.[319] 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.

To wrap up this discussion, 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.[320] The Fair Credit Reporting Act and the Video Privacy Protection Act similarly require the destruction of records from background checks or movie watching as soon

---

[317] Such a rule would reinforce the legal practice of pornography—the recording and sharing of nude imagery with the subject's explicit consent.

[318] 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. My prior work has explored suggestions for amending Section 230 and so I will not belabor the point here. See CITRON, HATE CRIMES IN CYBERSPACE, supra note; Danielle Keats Citron & Mary Anne Franks, *The Internet as a Speech Conversion Machine and Other Myths Confounding Section 230 Reform*, U. CHI. LEGAL F. (forthcoming); Danielle Keats Citron, *Cyber Mobs, Disinformation, and Death Videos: The Internet As It Is (And As It Should Be)*, 118 Mich. L. Rev. 1073 (2020); Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, 86 FORDHAM L. REV. 401 (2017); Citron, *Cyber Civil Rights*, *supra* note.

[319] NAACP v. Alabama, 357 U.S. 449, 466 (1958).

[320] Seda Gürses et al, *Engineering Privacy by Design Reloaded*, *available at* https://iapp.org/media/pdf/resource_center/Engineering-PbD-Reloaded.pdf.

as practicable.[321] Under the EU's General Data Protection Regulation, personal data can be kept only for as long as is necessary to fulfill the original basis for its collection and processing.[322]

2. Use Restrictions

Policymakers should restrict the uses of personal data to protect the values secured by sexual privacy and reduce the risks to well-being. Companies collect massive quantities of personal information on the expectation that someday it will generate significant returns. As Paul Ohm observes, "chasing profits, companies hoard data for future, undefined uses; redistribute it to countless third parties; and repurpose it in ways their customers never imagined."[323]

Personal data collected for a legitimate business purpose should not be repurposed to infer people's intimate information without obtaining separate consent. This mirrors the approach of the Fair Information Practice Principles (FIPPs).[324] The FIPPs are the foundation both for most privacy laws in the United States and around the world, as well as for most understandings of information ethics. Under the FIPPs, information obtained for one purpose cannot be used or made available for other purposes without the person's consent.[325] That restriction is often referred to as a "secondary use limitation."

Under this approach, a social media company could not use its subscribers' personal data to infer their sexuality, HIV status, and miscarriages without seeking meaningful consent. It could not use subscribers' intimate information to infer other intimate information without seeking meaningful consent. Subscribers' intimate information, of

---

[321] 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).

[322] Article 5, *Principles Related to the Processing of Personal Data*, General Data Protection Regulation, section 1(c) ("personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')").

[323] Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1128 (2015).

[324] The FIPPs were first articulated by privacy scholar Alan West in 1967 and popularized by the U.S. Department of Health, Education, and Welfare in 1973. See ALAN WESTIN, PRIVACY AND FREEDOM (1967); https://epic.org/privacy/consumer/code_fair_info.html.

[325] https://epic.org/privacy/consumer/code_fair_info.html; Privacy Policy Guidance Memorandum Department of Homeland Security (December 29, 2008) https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

course, could be used for the purpose for which it was collected and for which firms obtained meaningful consent. This would include allowing subscribers to message each other and to post intimate information.

We 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, law enforcers have investigated uses of personal data to target the vulnerabilities of protected groups as unfair commercial practices.[326] Such cases, however, remain rare. A ban would make clear that such practices are unlawful and would discourage enforcement actions directed at such exploitative practices.[327] 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.[328]

Strong use restrictions would protect the values that sexual privacy secures and prevent harms explored in this piece. Individuals would not have their sexual autonomy undermined by a dating app's secret sharing their HIV status, sexual fantasies, or sex toy use with advertisers. They would not suffer blows to their self-esteem due to the posting of their nude photos on revenge porn sites or the inclusion of their sexual assault in data brokers' dossiers. They would not be chilled from using reproductive-health apps for fear that their struggles with painful periods or infertility would undermine their job opportunities or raise their insurance premiums.

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.[329] Privacy debates of late have focused on the wisdom of recognizing civil actions for damages

---

[326] HARTZOG, supra note, at 131 (explaining that UDAP laws are designed to prevent the exploitation of human vulnerabilities).

[327] Jaime Luguri & Lior Strahelivitz, *Shining a Light on Dark Pattern*, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205.

[328] Richards & Hartzog, *Duty of Loyalty*, *supra* note, at; Richards & Hartzog, *Pathologies of Consent*, *supra* note, 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").

[329] The topic of privacy remedies has not attracted sustained attention with notable exceptions. For such an exception, see the important work of Lauren Henry Scholz. See, e.g., Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 1 (2019). Scholz argues for the recognition of restitution as privacy remedy.

or administrative fines.[330] Injunctive relief, however, has not been a key part of the discussion, but it should be.

Privacy legislation should recognize judicial power to order injunctive relief in cases for serial offenders. In such a case, injunctive relief should be mandatory to assure meaningful protection of sexual privacy and make clear its priority over competing interests.[331]

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.[332] Federal, state, and local anti-discrimination statutes permit injunctive relief,[333] and courts have employed equitable remedies in flexible and creative ways.[334] In workplace sexual harassment cases, courts have ordered employers to implement anti-harassment policies and procedures, provide training, retain personnel records, and install security cameras.[335]

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 several steps. Under the first step, the court would issue an order directing the party to fulfill its legal

---

[330] The debate has largely centered on private rights of action. Industry lobbyists strongly oppose privacy bills that include private rights of action. Private rights of action are essential given the limited resources available to federal and state law enforcers.

[331] Lawmakers must make clear that such injunctive relief is automatic. In the absence of clear legislative intent, courts are reluctant to order equitable remedies. Winter v. Natural Resources Defense Council, 555 U.S. 7, 24 (2008). There is an extensive scholarly debate about 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*, U. CHI. L. FORUM 177 (2014). 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. PIT. L. REV. 513, 515 (1984).

[332] 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 Michael T. Morley, *Enforcing Equality: Statutory Injunctions, Equitable Balancing under eBay, and the Civil Rights Act of 1964*, U. CHI. L. FORUM 177 (2014).

[333] See, e.g., Civil Rights Act of 1964, 204(a); 43 Pa. Stat. 962(c)(3); *Availability of Injunctive Relief under State Civil Rights Acts*, 24 U. CHI. L. REV. 174, 174, 180 (1956). In some civil rights statutes, injunctions are the only available remedy. For instance, Title III of the Americans with Disability Act only allows injunctive relief as opposed to monetary damages. Dudley v. Hannaford Brothers Co., 333 F.3d 299, 304 (1st Cir. 2003).

[334]

[335] See, e.g., United States v. Greenwood Community School Corp. (S.D. Ind.); Carey v. O'Reilly Auto. Stores, 2019 WL 3412170 (S.D. Fla. May 31, 2019).

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 second order) the firm to stop processing intimate data until compliance has been achieved as shown by an independent third-party audit.[336] For the final step, if the court is shown clear evidence that the party has failed to comply for the third time, 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 cyberstalking apps and sites devoted to nonconsensual pornography would have to halt their services.[337] An adult site would be ordered to stop collecting individuals' searches without meaningful consent. 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. Halt processing orders must be "appropriate, necessary, and proportionate" to ensure compliance with legal obligations.[338] In 2019, the Hamburg Commissioner for Data Protection and Freedom of Information (Hamburg Commissioner) started an administrative procedure to stop Google employees and contractors from listening to voice recordings of Google Home device subscribers for three months.[339] 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."[340] Google responded by pledging not transcribe voice recordings collected from its personal assistant device.[341]

---

[336] A schedule would be set to report the auditor's findings to the court.

[337] In the case of revenge porn sites and their ilk, such relief would depend upon changes to Section 230 as explored in note.

[338] Recital 129 of the GDPR.

[339] Hamburg Commissioner for Data Protection and Freedom of Information, Speech Assistant Systems Put to the Test (August 1, 2019), *available at* https://datenschutz-hamburg.de/assets/pdf/2019-08-01_press-release-Google_Assistant.pdf. 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.*

[340] *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.

[341] *Id.* Google seemingly has not altered its position.

EU data protection authorities had been issuing halt-processing orders even before the GDPR's adoption. For instance, Ireland's data protection authority ordered Loyaltybuild 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. 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.[342] It took the company seven months to fulfill those obligations.

To be sure, even temporary stop-processing orders exact significant costs. Loyaltybuild lost millions of Euros in revenue, a considerable blow to the firm.[343] 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.[344] But the grave risk to individuals and society posed by the handling intimate information warrants strong remedies.

C. 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 challenge.

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.

---

[342] https://iapp.org/news/a/cease-processing-orders-under-the-gdpr-how-the-irish-dpa-views-enforcement/

[343] *Id.* The behemoth Google halted transcriptions of conversations captured by personal devices with little impact on its bottom line.

[344] At a faculty workshop, my colleagues 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 AnonIB. See *supra* note. 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.

In some markets, third parties may have invested in them as we have seen in the sexual wellness and dating markets.[345]

Firms would look to other revenue sources if advertising fees and outside funding dropped significantly. 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.

Non-profit organizations might support efforts to provide some services free of charge. The fem tech market seems a likely possibility. Reproductive justice organizations might provide funding 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 firm's commitment to privacy engenders trust.[346] Individuals may be more inclined to use services because they believe that a firm's service is worth their price.[347]

---

[345] Dana Olsen, *The top 13 VC investors in femtech startups*, PITCHBOOK (November 2, 2016), *available at* https://pitchbook.com/news/articles/the-top-13-vc-investors-in-femtech-startups (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), *available at* https://pitchbook.com/news/articles/dating-app-raises-vc-as-facebook-enters-the-relationship-biz (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. Dana Olsen, *This year is setting records for femtech funding*, PITCHBOOK (October 31, 2018), available at https://pitchbook.com/news/articles/this-year-is-setting-records-for-femtech-funding. 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 invested in Lola, which provides subscription-based delivery of organic tampons, Flo, the period-tracking app, and Future Family, a business offering reproductive-health services. *Id.*

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

[347] *Id.*

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.[348] 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."[349] 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."[350]

Just because activity can be characterized as speech does not mean that the First Amendment protects it from government regulation.[351] 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."[352] Indeed.

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.[353] Some government regulations censor speech central to self-governance or the search for truth while others raise no such concerns. Some government regulations imperil speech crucial to self-expression while others pose no such threat.[354]

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 explicit 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

---

[348] 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, 1050-51 (2000) (arguing that government imposed fair information practice rules that restrict the ability of speakers to communicate truthful data about others is inconsistent with the basic First Amendment principles); Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 63 (2014) (arguing that "for all practical purposes, and in every context relevant to the current debates in information law, data is speech.").

[349] Leslie Kendrick, *First Amendment Expansionism*, 56 WILLIAM & MARY L. REV. 1199, 1212 (2015).

[350] *Id.*

[351] *Id.*

[352] Neil M. Richards, *Why Data Privacy Laws Is (Mostly) Constitutional*, 56 WILLIAM & MARY L. REV. 1501, 1507 (2015).

[353] Kendrick, supra *note*, at.

[354] Id.

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 truth.

Regulating the surveillance of intimate life with explicit consent requirements and narrow no-collection zones would not chill self-expression but rather secure the conditions for self-expression.[355] The nonconsensual collection of people's sex toy habits or porn site searches undermines their willingness to engage in sexual expression. People whose nude photos appear on revenge porn sites have difficulty interacting with others and often retreat from online engagement and self-expression.[356]

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 of public disclosure of private conversations might well have a chilling effect on private speech."[357] 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."[358]

With the proposed reforms, people would be less fearful of engaging in intimate expression and interaction. 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. 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

---

[355] Danielle Keats Citron & Neil M. Richards, *Four Principles for Digital Expression (You Won't Believe #3!)*, 95 WASH. U. L. REV. 1353, 1379 (2018).

[356] CITRON, HATE CRIMES IN CYBERSPACE, *supra* note, at 195.

[357] 532 U.S. 514 (2001). See Citron, Hate Crimes in Cyberspace, supra note, at 208-210 (discussing the Court's recognition in *Bartnicki v. Vopper* that privacy protections foster private speech).

[358] Carpenter v. United States, 138 S. Ct. 2206 (2018). See also David Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 77 (2013) (exploring the chilling effect of indiscriminate, continuous police collection of geolocation data).

concerns as laws restricting speech on matters of public interest.[359] As the Court explained in *Snyder v. Phelps*, speech on public matters enjoys rigorous protection "to prevent the stifling of debate essential to democratic self-governance."[360] In contrast, speech about "purely private matters" receives "less stringent" protection because the threat of liability would not risk chilling the "meaningful exchange of ideas" and "robust debate on public issues."[361] Its restriction "does not pose the risk of a reaction of self-censorship on matters of public import." To illustrate a "purely private matter," the Court pointed to an individual's credit report and videos showing someone engaged in sexual activity.[362] 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.[363] Rules governing the collection of information raise few, if any, First Amendment concerns.[364] These rules "prohibit information collection by separating the public sphere from the private."[365] Trespass laws, intrusion on seclusion tort, and video-voyeurism statutes have withstood constitutional challenge.[366] Courts have upheld laws requiring informed consent before entities can collect personal data, such as the Fair Credit Reporting Act (FCRA), federal and state wiretapping laws, and the Children's Online Privacy Protection Act (COPPA).[367] It is also worth noting that the reform proposals turn on people's explicit consent. The Court has held that "private decision making can avoid government partiality and insulate privacy measures from First Amendment

[359] 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 Kenneth S. Abraham & Edward G. White, *First Amendment Imperialism and the Constitutionalization of Tort Liability*, TEX. L. REV. (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3437289.

[360] Snyder v. Phelps, 131 S. Ct. 1207 (2011). For an extended discussion of Snyder v. Phelps, *see* CITRON, HATE CRIMES IN CYBERSPACE, *supra* note, at 215.

[361] Snyder, 131 S. Ct. at 1216 (noting that the "content of a particular person's credit report 'concerns no public issue' and was speech solely in the individual interest of the speaker and its particular business audience" and that "videos of an employee engaging in sexually explicit acts did not address a public concern" because it "did nothing to inform the public about any aspect of the [employing agency's] functioning or operation").

[362] 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.

[363] Richards, *supra* note, at.

[364] Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. Rev. 1149, 1182 (2005).

[365] Id.

[366] NEIL M. RICHARDS, INTELLECTUAL PRIVACY (2015).

[367] *Id.*

challenge."[368] Indeed, explicit consent is part and parcel of data collection laws like FCRA and COPPA.

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."[369] These rules "are of general applicability, neither discriminating against or significantly impacting the freedoms guaranteed by the First Amendment."[370] 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.[371]

Trespassers cannot avoid liability by contending that they infringed others' property rights in order to collect information.[372] Computer hackers cannot avoid criminal penalties by insisting that they were only trying to obtain information.[373] 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. 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.

Reform proposals restricting the use of intimate information without explicit 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.[374] Laws restricting secondary uses of information have not been held to violate the First Amendment.[375] In *Bartinicki v. Vopper*, the Supreme Court assessed the First Amendment implications of the Wiretap Act's prohibition on the use or disclosure of intercepted communications. The Court underscored that "the prohibition on 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.[376]

---

[368] Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2669 (citing Rowan v. Post Office, 397 U.S. 728 (1970)).

[369] Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1186 (2005).

[370] *Id.*

[371] *Id.* at 1188 (noting that in *Cohen v. Cowles*, the Supreme Court held that the press may not with impunity break and enter an office or dwelling to gather news").

[372] *Id.*

[373] *Id.*

[374] *Id.* at 1190-91.

[375] *Id.* at 1194.

[376] *Bartnicki*, 532 U.S. at 527.

Sorrell v. IMS Health,[377] decided in 2011, does not cast doubt on the likely constitutionality of the collection and use restrictions suggested here. In *Sorrell*, the Court struck down a Vermont law banning two types of activities. First, the law prohibited pharmacies, health insurers, or similar entities from disclosing doctors' prescription data for marketing purposes. Second, the law prohibited pharmaceutical companies and health data brokers from using doctors' prescription data for marketing purposes unless the medical prescriber consents.[378] Data brokers and an association of pharmaceutical companies challenged the regulations on the grounds that they violated their free-speech rights.

Justice Kennedy, writing for the majority, struck down the law on First Amendment grounds. Under First Amendment doctrine, discrimination against particular speakers or messages—known as viewpoint-based discrimination—is "virtually always invalid."[379] The Court found that the law did precisely that. It held that the law "imposes a burden based on the content of the speech and the identity of the speaker."[380] The majority underscored that the law "imposed content- and speaker-based restrictions on the availability and use of prescriber-identifying information."[381]

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.[382] Under the law, pharmacies could share prescriber information to academics and other private entities. The Court explained, "The State has burdened a form of protected expression it has 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."

The Court found viewpoint discrimination in the law's targeting of specific speakers—data brokers and pharmaceutical companies—and not others. As the majority noted, academic institutions could buy prescription data "in countering the messages of brand-name pharmaceutical manufacturers and in promotion the prescription of generic drugs," but

---

[377] 131 S. Ct. 2653 (2011).
[378] *Sorrell*, 131 S. Ct. at 2660.
[379] RICHARDS, INTELLECTUAL PRIVACY, supra note, at.
[380] *Sorrell*, 131 S. Ct. at 2665.
[381] *Id.*
[382] *Sorrell*, 131 S. Ct. at 2662.

pharmaceutical companies and detailers "were denied the "means of purchasing, acquiring, or using prescriber-identifying information."[383]

The majority rejected the state's argument that the consent provision insulated the law's use restriction from constitutional concerns.[384] 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." 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."[385]

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." 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.[386] The majority emphasized that the law "allowed prescriber data to be studied and used by all but a narrow class of disfavored speakers."

Some have suggested that *Sorrell* casts doubt on the constitutionality of data protection laws in recognizing that "a strong argument exists that prescriber-identifying information is speech for First Amendment purposes."[387] 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, seemingly affirmed the constitutionality of sectoral privacy laws like the federal health privacy law. He explained if Vermont had "advanced its asserted privacy interest by allowing information's sale or disclosure in only a few narrow and well-justified circumstances" as in HIPAA, the law would have been constitutional.[388]

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

---

[383] *Sorrell*, 131 S. Ct. at 2663.

[384] *Id.* at 2669.

[385] *Id.*

[386] *Id.*

[387] Jane Bambauer argues that if data is speech than privacy regulations always burden the production of knowledge. Bambauer, *supra* note, at 63.

[388]

policy" and imposed impermissible viewpoint restrictions.[389] 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.[390] 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 the measure was drawn to achieve that interest.[391] Crucially, as Richards explains, the Court made clear that the "law 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.[392]

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. Privacy law reform should provide 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.

---

[389] RICHARDS, INTELLECTUAL PRIVACY, supra note, at.

[390] Sorrell, 131 S. Ct. at 2668.

[391] *Id.*

[392] Richards, supra note, at 1523.