

# Digital Security and Reproductive Rights

## *Lessons for Feminist Cyberlaw*

Michela Meister and Karen Levy

Reproductive rights in the United States are under threat, and the threat is growing more serious by the day. The 2022 Supreme Court opinion in *Dobbs v. Jackson Women's Health Organization*,<sup>1</sup> overturning the fundamental right to abortion enshrined in *Roe v. Wade*,<sup>2</sup> cast into danger the lives and livelihoods of millions of people. Alongside (and quite clearly related to) the decimation of reproductive rights in courts and legislatures are an increasing number of ideologically driven attacks on abortion seekers, providers, and clinics. Clinics have been the targets of bombings, blockades, and invasions. Day to day, providers and their clients face picketers, protesters, online harassment, stalking, and doxing designed to intimidate clients into ceasing to exercise what reproductive rights they still have, and to dissuade providers from providing essential health services.

The rise of digital technologies has exacerbated these threats in multiple ways, and digital threats have a marked impact on abortion access. Abortion is a common experience in the United States—almost one in four women will have an abortion in her lifetime<sup>3</sup>—and these threats are clearly designed to chill and punish access to care for people seeking abortions. While much has been written about the impact of violence and harassment on abortion services, the relationship between these threats and digital privacy and security is only beginning to be fully appreciated.<sup>4</sup> Given the impact that digital attacks have on abortion across all levels—from the individual patient experience to providers, to clinics, and to the legality of abortion across the nation—this attention is long overdue.

Threats to reproductive rights are of paramount importance to people interested in the gendered relationship between law and technology. But they also offer a case study in what a feminist viewpoint provides to cyberlaw even beyond

abortion. In this chapter, we offer three lessons for feminist cyberlaw in the wake of *Dobbs*. We show how a feminist perspective—one that acknowledges “contexts, bodies, and legacies,” as articulated by this volume’s coeditor Meg Leta Jones<sup>5</sup>—offers a fuller view of how digital security and privacy intrusions are embedded in social ecosystems, can result in grave physical and mental harms, and are impossible to understand or prevent in isolation from broader patterns of surveillance. These lessons are applicable not only in the critical context of reproductive rights, but across many arenas in which cyberlaw operates.

### SILOES AND DEAD BODIES

*Dobbs* and its aftermath hit home a lesson that feminist security scholars have consistently highlighted: that a good deal of contemporary security research tends to understand digital security threats in relative isolation, devoid of broader context. Academic security scholarship often highlights novel, technically sophisticated digital attacks, yet sometimes neglects the social contexts in which everyday people experience insecurity, and the real, lived consequences of those threats. A new wave of feminist security research has countered this trend, calling explicit attention to the social and relational aspects of digital insecurity—and showing how even technically unsophisticated attacks (which might not traditionally garner much interest among academic security researchers) can be both immensely harmful and extremely difficult to protect against, largely because of their social complexity.

Much of this feminist security scholarship focuses particularly on the context of technology-mediated abuse, an extremely widespread phenomenon which is very likely the most frequent context in which digital insecurity is experienced by everyday people.<sup>6</sup> One in three women and one in four men in the United States experiences intimate partner violence, stalking, or rape at some point during their lives, and transgender people are about twice as likely as cisgender people to experience intimate partner violence;<sup>7</sup> digital technologies play a prominent role in abuse contexts, providing means by which attackers can control, stalk, and harass their targets.<sup>8</sup> In this context, the vectors of attack for abuse may be technically very simple and require no special technical expertise—even something as basic as looking over a partner’s shoulder or perusing search history on a shared device can be sufficient to glean intimate personal data.<sup>9</sup>

A core insight of this line of work is that digital security, while often siloed in academic analysis, is in reality inextricably linked to physical, emotional, sexual, and economic security. Analyzing digital security threats in isolation from other vectors of attack is necessarily incomplete, and often mischaracterizes or understates the potential risks and consequences of digital security breach. For example, traditional digital security research is unlikely to account for the physical proximity of an attacker and a target (which can facilitate involuntary information-sharing,

as in shoulder-surfing), the ways in which a target may be have a preexisting relationship with the attacker (giving the attacker access to resources like the answers to common security questions), or the ways in which threats to digital security can go hand-in-hand with threats to other forms of security (for example, an attacker may threaten physical violence if one takes steps to protect one's digital data from access).<sup>10</sup> Feminist thinkers describe how conventional security threat modeling that focuses on digital access in isolation can neglect broader questions about safety and justice for marginalized people.<sup>11</sup>

A similar question of focus arises in legal privacy scholarship. Privacy is sometimes described as having a “dead body problem”: many privacy violations lack harms that are readily cognizable as such, making it difficult to address and prevent them through tort law.<sup>12</sup> Targeted ads based on internet tracking, for example, may give one an uneasy feeling of being watched; shoddy privacy practices that result in disclosure of personal information may cause embarrassment or impinge on one's sense of dignity. But unease and humiliation are not concrete harms, and tend not to be readily compensable via tort law. The “dead body problem” in privacy, as it's described, is that there aren't any: the nature of harm is diffuse and abstract, making it difficult to seek legal redress for harms and to marshal the political will to address privacy problems in the policy realm.<sup>13</sup>

Yet feminist thinkers retort: if you can't find any dead bodies in privacy law, you just aren't looking very hard. Feminist legal thinkers have long highlighted in their scholarship the dire, violent, and often life-or-death consequences of privacy and security violation, particularly for women, the LGBTQ community, and communities of color.<sup>14</sup> Perhaps the most direct confrontation between feminist legal thought and “mainline” privacy scholarship arose in 2006, when Ann Bartow wrote an essay reviewing Daniel Solove's *A Taxonomy of Privacy*.<sup>15</sup> Solove's taxonomy, published that same year, has since become one of the most influential and heavily cited articles in all of privacy law; in it, Solove attempts to bring order to the notoriously slippery concept of “privacy” by categorizing privacy violations into sixteen types (aggregation, appropriation, breach of confidentiality, etc.).<sup>16</sup> In her review, Bartow asserts that Solove's taxonomy “suffers from too much doctrine, and not enough dead bodies”;<sup>17</sup> that his “dry, analytical”<sup>18</sup> approach “fail[s] to sufficiently identify and animate the compelling ways that privacy violations can negatively impact the lives of living, breathing human beings beyond simply provoking feelings of unease.”<sup>19</sup> The diminishment of reproductive rights is one of the chief examples Bartow brings to bear in her critique, noting presciently that “the prospect that women will either forgo sexual relationships or possibly even bear unwanted children as a consequence of inadequate information privacy is the sort of harm Solove's taxonomy could have taken greater notice of.”<sup>20</sup>

Solove countered Bartow's critique in a subsequent article,<sup>21</sup> responding that “most privacy problems lack dead bodies.”<sup>22</sup> He acknowledges as aberrations

(“exceptional cases”<sup>23</sup>) a few situations in which women were murdered by stalkers after the stalkers obtained the women’s physical addresses from government and commercial sources—but dismisses what he decries as “Bartow’s quest for horror stories”<sup>24</sup> as counterproductive.<sup>25</sup> In Solove’s view—one that has become as authoritative as that of any contemporary privacy scholar—highlighting the most visceral and violent privacy harms (it must be noted, those suffered in these cases by women) could serve to obscure other pervasive privacy harms that accrete more gradually and less egregiously. Solove is, of course, correct in assessing that not all privacy harms need to rise to the level of stalking, rape, murder, or forced childbirth to constitute real harms worth addressing. Yet the scholarship also has a performative effect: dismissing these harms as “sensationalistic,” as Solove does, sidelines them as distractions from apparently more pressing issues.<sup>26</sup> And it is incontrovertible that the mine run of privacy scholarship has for decades focused a great deal more energy on issues related to consumer protection than it has on issues related to bodily autonomy and physical safety. In part, deciding which harms to name and to most closely associate with the term “privacy” is a question of political strategy, with both benefits and drawbacks; but it certainly bears notice that at least one such drawback is reduced focus, from both scholars and policymakers, on centering reproductive and bodily integrity as a core privacy issue.

The aftermath of *Dobbs* illustrates the inseparability of digital and physical security, and the production of “dead bodies” as a consequence of privacy violation, with stark clarity. Digital vulnerabilities—say, location tracking of one’s visit to a reproductive health clinic, or search results demonstrating information-seeking around abortion access—are life-or-death scenarios: they bear directly on the ability to seek lifesaving medical care and to have autonomy over one’s own body and future. Digital privacy *is* physical safety in these scenarios, and to isolate it in analysis, without fully accounting for its broader context and effects, necessarily impoverishes both our research and our law. A feminist approach ameliorates this shortcoming through a focus on the inextricability of the digital and the physical, and attention to visceral and violent harm as a key outcome produced by insecurity.

#### TILES AND MOSAICS

In Fourth Amendment jurisprudence, “mosaic theory” refers to the idea that courts, in determining whether a search is constitutional, should take a collective, holistic approach—considering the aggregation of police information-gathering as a whole to evaluate whether that activity constitutes a search, rather than focusing on any discrete information-gathering action in isolation.<sup>27</sup> Mosaic theory relies on the insight that pervasive data collection is more than the sum

of its parts—that individual pieces of data, like the tiles of a mosaic, may reveal information about a person’s life that becomes clear only when the pieces are viewed in the context of one another, as a whole picture.

This insight has a corollary important in the post-*Dobbs* era, with crucial implications for privacy protection. It’s true that some insights only emerge given the arrangement of individual data points into a more coherent whole. But it’s similarly true that once a mosaic is in view—once the full picture is visible—the removal of any one tile tends not to have a substantial effect on the image’s interpretation. A mosaic of a horse still looks pretty much like a horse even if it’s missing a few tiles. In the context of privacy, this leads to an important implication: protecting any particular data point from view may not be enough to substantially reduce what can be inferred about a person given the totality of data points available.<sup>28</sup>

After the leak of the initial *Dobbs* draft (and again after the release of the full opinion), well-meaning individuals took to the internet to share advice about how to protect one’s privacy around abortion and reproductive care. A common suggestion was to delete digital period trackers, which are used by many people to track periods of fertility and menstruation—and which, it might be assumed, could be a source of critical evidence in any legal action based on termination of a pregnancy.<sup>29</sup> Another common approach was for people in states with abortion access to offer aid to abortion seekers from other states, using coded language—offering, for instance, to take out-of-state visitors “camping” as code for helping them obtain abortion services.<sup>30</sup> And immediately following the *Dobbs* ruling, some Big Tech firms altered internal policies as well: Google, for example, announced plans to automatically delete location-tracking data from trips to abortion clinics, domestic violence shelters, and addiction treatment facilities, among other places.<sup>31</sup> Each of these developments was intended to provide some degree of privacy around particularly sensitive data involving abortion-seeking.

But feminist writers—notably Cynthia Conti-Cook, Kendra Albert, Maggie Delano, Emma Weil, and Elizabeth Joh (in this volume)—offered a more realistic view that demonstrated that these efforts, though well-meaning, were ultimately misguided and of limited utility in protecting the privacy of abortion seekers.<sup>32</sup> Cynthia Conti-Cook’s clear-eyed analysis of the “digital abortion diary” demonstrates that search histories and communication logs (e.g., text messages) are much more likely to be used in prosecutions than is something like a period tracker.<sup>33</sup> Efforts to rely on coded messages among networks of untrained volunteers could expose abortion seekers to myriad risks poorly understood by those seeking to help. And Google’s deletion of location data logs, while perhaps a step in the right direction, is of limited effect in the context of amassed search query data, text messages, license plate tracking, and easily purchased data from data brokers.<sup>34</sup>

Essentially, these efforts aim to remove a tile from the mosaic of ubiquitous surveillance—but doing so doesn’t obscure the full picture from view. There’s very

little that individual abortion seekers, medical providers, or allies can do in the face of generalized surveillance from which inferences of all types (including, but not limited to, abortion-seeking behavior) can be drawn from general communications, search, and behavioral data. A targeted focus on technologies specific to reproductive tracking is a natural point of focus, but largely symbolic in the broader context.<sup>35</sup>

## ECOSYSTEMS AND ENTANGLEMENTS

Threats to reproductive rights are multiplex. They originate from many points, including statehouses, intimate partners, and religious and political ideologues. They have many vectors of attack, including both digital surveillance and physical intimidation—as well as the propagation of misinformation and other behaviors not always immediately understood as privacy threats. The targets of attack include not only abortion seekers, but clinics, individual health care providers, and allies who might aid abortion seekers in obtaining care. This complexity implies that vulnerabilities at any point, from any attacker, against any target can effectively impede reproductive care—and demands that we adopt a broad *ecosystemic* approach to reproductive privacy and security protection.

To illustrate, consider the following three threats (among many): the 2015 misinformation campaign against Planned Parenthood, online “hit lists” of abortion providers, and the digital surveillance of abortion seekers.

### *A Massive Misinformation Campaign*

In July 2015, the Center for Medical Progress, an anti-abortion group, promoted a massive misinformation campaign against Planned Parenthood which incited a wave of attacks against abortion clinics.<sup>36</sup> The campaign centered around the use of fetal tissue, a key component for a variety of areas in medical research, such as in developing vaccines and studying diseases like ALS, cancer, and HIV. Some clinics allow people having abortions to donate the fetal tissue to medical research; however, the donation is always voluntary and the tissue is never sold.<sup>37</sup> The main claim of the misinformation campaign was that Planned Parenthood sells the fetal tissue from abortions.

This campaign involved a high degree of espionage and took place over the course of two years. Members of the Center for Medical Progress set up a fake company, BioMax, which they claimed works to bring fetal tissue to research labs. Under the guise of this fake company, attackers set up meetings with Planned Parenthood officials, where they used hidden cameras to secretly record hundreds of hours of meetings. They then edited these videos to imply that Planned Parenthood sells fetal tissue.<sup>38</sup>

The implications were drastic. Millions of people viewed the manipulated videos. The doctors and staff depicted in the videos were subjected to both digital and

physical harassment and death threats. The effects were not only felt by the doctors and staff in the videos, but by abortion clinics nationwide. Threats to Planned Parenthood clinics around the country skyrocketed and have remained at higher levels ever since.<sup>39</sup>

### *Bounties and “Wanted” Lists*

Abortion providers endure daily harassment, political stigma, and at times physical violence. Online databases created by anti-abortion extremists are a serious threat to providers. These sites display photos and personal information about abortion providers. The first such website was created in the mid-1990s with the name “The Nuremberg Files,” a reference to the Nuremberg Trials through which Nazi war criminals were tried after World War II. The site, which was eventually forced off the internet by its ISP, included personal information about providers, including names, photos, home addresses, license plate numbers, information about their families, and even the addresses of churches they attend. The site also included “Wanted” posters for certain doctors and operated like a “hit list”: after a doctor was injured, their name was grayed out, and after a doctor was murdered, their name was drawn with a strike through it.<sup>40</sup>

Currently, the anti-abortion group Operation Rescue maintains a website called AbortionDocs.org. The site contains dossiers about (at the time of this writing) 1,479 individual abortion providers and hundreds of clinics, comprising tens of thousands of documents in total.<sup>41</sup> Each provider (which the site calls an “Abortionist”) has a page which often includes their photo, the clinic where they work (which the site calls the “Abortion Mill”), an inset Google map of the clinic, and any other available documents on the provider, such as their medical license, social media profiles, personal pictures, malpractice suits against them, and relevant news articles.

The policy of the site is to only post publicly available information and not to post private information, like home addresses or photos of family members.<sup>42</sup> The site specifically states that its purpose is to simply provide information; it claims to “denounce acts of violence against abortion clinics and providers in the strongest terms.”<sup>43</sup> However, given the history of the Nuremberg Files, it is clear that such a public repository of information about providers poses a significant threat by providing a centralized resource to people wishing to target abortion providers.

“Vigilante” laws like Texas’s SB8 augment the threat from anti-abortion advocates by incentivizing motivated individuals to enforce state laws privately. These laws provide a monetary “bounty” to people willing to bring private civil actions against abortion providers (as well as others who aid abortion seekers in receiving care)—up to \$10,000 under Texas’s law.<sup>44</sup> Private enforcement mechanisms not only effectively circumvent certain forms of legal challenge (since the state is not a direct actor in preventing care) but can provide motivation for individuals

ideologically opposed to abortion to both surveil and sue those suspected of providing or assisting with abortions. Websites like [prolifewhistleblower.com](http://prolifewhistleblower.com) offer means through which people can provide tips on abortion providers (though the website has had trouble maintaining consistent hosting).<sup>45</sup>

### *Threats Faced by People Seeking Abortions*

People seeking abortions (or information about abortions) face a variety of threats, including harassment, surveillance, and targeted misinformation. Some threats, of course, may come directly from the state in jurisdictions where abortion is criminalized. But many threats are closer to home. Given the immense stigma surrounding abortion, abortion seekers may wish to keep their abortions secret from family members or partners, particularly (though not exclusively) in cases of abuse. A common fear is that a family member or partner might learn of an abortion, for example, from the search history on an abortion-seeker's phone or computer, or because of the time they are away to have the procedure.<sup>46</sup>

Another set of threats comes from anti-abortion advocacy groups, who employ strategies like digital marketing campaigns to target abortion seekers at clinics via geofencing. For example, the anti-abortion marketing group Choose Life helps anti-abortion groups implement geofencing to target people sitting in abortion clinics with anti-abortion ads.<sup>47</sup> To enter an abortion clinic, clients must often walk past crowds of picketers, who may verbally harass clients, disseminate misinformation about abortions, or attempt to physically block clients from entering clinics. Anti-abortion protesters have also been known to take photos of clients entering clinics and record license plate numbers. For example, in one case in Texas, an anti-abortion group matched license plates with car registration information and sent mass emails to a local college about people they suspected were seeking abortions.<sup>48</sup>

These three threats are, of course, far from the only difficulties people and organizations face in seeking or providing abortion care; our aim here is not to provide a complete threat model of all potential vulnerabilities to reproductive privacy and security, and new threats are very likely to arise as the legal and technology landscapes continue to change over time. However, a few important analytic points arise from considering these three scenarios.

First, we see—again—the entanglement of the digital and the physical, as digital threats often have physical consequences. Misinformation campaigns and sites such as [AbortionDocs.org](http://AbortionDocs.org) both enable violence against providers. People who are unable to receive a wanted abortion, either because of misinformation they read online, or fear of harassment or stigma, are forced to undergo the life-changing process of being pregnant and bearing a child. All these threats can pose a chilling effect: simply the threat of a family member finding out about an abortion can prevent someone from seeking one. Similarly, harassment and threats to providers may dissuade doctors from providing abortion care.



Second, the role of misinformation as a component of privacy and security threat is often underappreciated. Misinformation researchers Claire Wardle and Hossein Derakhshan characterize both misinformation and “mal-information” (a category including hate speech, harassment, and disclosure of private information) as interconnected elements of a broader phenomenon, which they term *information disorder*.<sup>49</sup> Combatting misinformation about abortion is vital to helping people make informed decisions about their health—both through the prevention of highly orchestrated campaigns like the Center for Medical Progress’s expose of Planned Parenthood, and through ensuring accurate information is readily available online without risk or manipulation. (For example, lawmakers have recently urged Google to improve its search results about abortion services, which often divert abortion seekers to “crisis pregnancy centers” that dissuade them from receiving abortion care.)<sup>50</sup>

Finally, the nature of reproductive care requires that we approach privacy and security through an *ecosystemic* lens. Threats to abortion providers’ privacy *are* threats to abortion seekers’ reproductive rights. Targeted misinformation campaigns about Planned Parenthood can (and are designed to) motivate attacks against unaffiliated abortion providers and people seeking abortion care. In considering how to defend against privacy and security threats to reproductive rights, it’s not enough to focus on strengthening the defenses of a single target—be it an abortion seeker, an individual provider, or a clinic; threats to each affects the other parties. This interdependence is yet another reason why individualized solutions, like deleting a period tracker app, are insufficient for robust reproductive privacy protection.

. . .

As we’ve seen, feminist perspectives offer a clear-eyed view of the nature of threats to reproductive privacy. They illustrate that privacy threats indeed lead to physical harms and “dead bodies,” if you prioritize looking for them; they show the insufficiency of protecting discrete pieces of particularly sensitive data while continuing to collect massive amounts of other more general data; and they emphasize the entanglements and interdependence of multiple kinds of vulnerabilities, multiple kinds of attacks, and multiple kinds of targets. Recognizing these characteristics shows an appreciation for the complexity of the problem—a first step toward devising adequate solutions to protect the lives and livelihoods of abortion seekers and providers in the post-*Dobbs* era.

## NOTES

1. 597 U.S. \_\_\_\_ (2022).
2. 410 U.S. 113 (1973).

3. See Guttmacher Institute, *Abortion Is a Common Experience for U.S. Women, Despite Dramatic Declines in Rates*, <https://www.guttmacher.org/news-release/2017/abortion-common-experience-us-women-despite-dramatic-declines-rates> (Oct. 19, 2017).

4. See, e.g., Center for Reproductive Rights, *Defending Human Rights: Abortion Providers Facing Threats, Restrictions, and Harassment* (2009), [https://reproductiverights.org/sites/default/files/documents/DefendingHumanRights\\_0.pdf](https://reproductiverights.org/sites/default/files/documents/DefendingHumanRights_0.pdf).

5. Meg Leta Jones, *Cyberlaw, But Make it Feminist*, in *FEMINIST CYBERLAW* (Meg Leta Jones and Amanda Levendowski, eds., 2024) (distinguishing the feminist cyberlaw perspective from the cyberlaw canon due to its focus on these dimensions). See also Amanda Levendowski, *Defragging Feminist Cyberlaw*, 37 *BERKELEY TECH. L.J.* \_\_\_ (2023) (describing the reliance of cyberlaw on core feminist values of consent, accessibility, and safety).

6. See generally Diana Freed, et al., “A Stalker’s Paradise”: How Intimate Partner Abusers Exploit Technology, *PROC. ACM CONF. ON HUMAN FACTORS IN COMPUTING SYSTEMS (CHI)* Article 667 (2018); Diana Freed, et al., *Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders*, *PROC. ACM CONFERENCE ON HUMAN-COMPUTER INTERACTION (CSCW)* Article 46 (2017); Karen Levy & Bruce Schneier, *Privacy Threats in Intimate Relationships*, 6 *J. CYBERSECURITY* 1 (2020); Tara Matthews, et al., *Security and Privacy Experiences and Practices of Survivors of Intimate Partner Abuse*, 15 *IEEE SECURITY & PRIVACY* 76 (2017); Julia Slupska, *Safe at Home: Towards a Feminist Critique of Cybersecurity*, 15 *ST. ANTONY’S INT’L REV.* 83 (2019); Julia Slupska and Leonie Maria Tanczer, *Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things*, in *EMERALD INTERNATIONAL HANDBOOK OF TECHNOLOGY-FACILITATED VIOLENCE AND ABUSE* 663 (Jane Bailey, Asher Flynn, and Nicola Henry, eds., 2021); Emily Tseng, et al., *The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums*, 29 *PROC. USENIX SECURITY SYMPOSIUM* 1893 (2020).

7. Domestic Violence Statistics, National Domestic Violence Hotline, <https://www.thehotline.org/stakeholders/domestic-violence-statistics/>; Sarah M. Peitzmeier, et al., *Intimate Partner Violence in Transgender Populations: Systematic Review and Meta-Analysis of Prevalence and Correlates*, 110 *AM. J. PUB. HEALTH* e1, e1 (2020).

8. Freed et al., *Stalker’s Paradise*, *supra* note 6, at 1.

9. Freed et al. describe the nature of the attack in this context as often coming from a “UI-bound adversary” without specialized technical knowledge—that is, “an authenticated but adversarial user of a victim’s device or account who carries out attacks by interacting with the standard user interface [UI], rather than through the installation of malicious or sophisticated software tools.” *Id.*

10. See *id.*; Levy & Schneier, *supra* note 6.

11. See Angelika Strohmayer, Rosanna Bellini, and Julia Slupska, *Safety as a Grand Challenge in Pervasive Computing: Using Feminist Epistemologies to Shift the Paradigm from Security to Safety*, *IEEE PERVASIVE COMP.* 1 (July 14, 2022); Tactical Technology Collective, *The Holistic Security Manual*, <https://holistic-security.tacticaltech.org/index.html>.

12. See, e.g., Gideon Lewis-Kraus, *Facebook and the “Dead Body” Problem*, *NEW YORK TIMES MAGAZINE* (Apr. 24, 2018), <https://www.nytimes.com/2018/04/24/magazine/facebook-and-the-dead-body-problem.html>.

13. See, e.g., *TransUnion LLC v. Ramirez*, 594 U.S. \_\_\_ (2021) (demonstrating the difficulty of establishing concrete harm).

14. See, e.g., Anita Allen and Erin Mack, *How Privacy Got Its Gender*, 10 *N. ILL. U. L. REV.* 441 (1991); Alvaro M. Bedoya, *Privacy as Civil Right*, 50 *NEW MEXICO L. REV.* 301 (2020); KHIARA BRIDGES, *THE POVERTY OF PRIVACY RIGHTS* (2017); SIMONE BROWNE, *DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS* (2015); Danielle Keats Citron, *Sexual Privacy*, 128 *YALE L.J.* 1870 (2018); Karen Levy, *Intimate Surveillance*, 51 *IDAHO L. REV.* 679 (2015); SCOTT SKINNER-THOMPSON, *PRIVACY AT THE MARGINS* (2021); Kristen Thomasen, *Beyond Airspace Safety: A Feminist Perspective on Drone Privacy Regulation*, 16 *CANADIAN J. L. & TECH.* 307 (2018); Ari Ezra Waldman, *Law, Privacy, and Online Dating: “Revenge Porn” in Gay Online Communities*, 44 *L. & SOC. INQUIRY* 987 (2019).

15. Ann Bartow, *A Feeling of Unease About Privacy Law*, 155 U. PA. L. REV. PENNUMBRA 52 (2006).
16. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).
17. Bartow, *supra* note 15, at 52.
18. *Id.*
19. *Id.*
20. *Id.*, at 62.
21. See Daniel J. Solove, “I’ve Got Nothing to Hide” And Other Misunderstandings of Privacy, 44 SAN DIEGO L. REV. 745 (2007).
22. *Id.*, at 768.
23. *Id.*
24. *Id.*, at 769.
25. Note, however, that in later work typologizing privacy harms, Solove—writing with Danielle Keats Citron—did highlight physical violence as a salient type of harm that could result from privacy violation. See Danielle Keats Citron and Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 831–34 (2022).
26. Solove, *Nothing to Hide*, *supra* note 21, at 769.
27. See Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).
28. This point is aligned with analyses of deanonymization, which demonstrate that the removal of particularly sensitive “personally identifiable information” does little to mitigate the risk of reidentification since so much other information is available. See, e.g., Arvind Narayanan and Vitaly Shmatikov, *Myths and Fallacies of “Personally Identifiable Information,”* 53 COMM. ACM 24 (2010).
29. Kashmir Hill, *Deleting Your Period Tracker Won’t Protect You*, NEW YORK TIMES (June 30, 2022), <https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html>.
30. Kaitlyn Tiffany, *What Are Abortion Code Words Even For?*, THE ATLANTIC (July 17, 2022), <https://www.theatlantic.com/technology/archive/2022/07/abortion-code-words-social-media-activism/670521/>.
31. Jen Fitzpatrick, *Protecting People’s Privacy on Health Topics*, Google Keyword blog (July 1, 2022), <https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/>.
32. See Hill, *supra* note 29; Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 U. BALT. L. REV. 1 (2020); Kendra Albert, Maggie Delano, and Emma Weil, *Fear, Uncertainty, and Period Trackers*, MEDIUM (June 28, 2022), [https://medium.com/@Kendra\\_Serra/fear-uncertainty-and-period-trackers-340ab8fdff74](https://medium.com/@Kendra_Serra/fear-uncertainty-and-period-trackers-340ab8fdff74). Within this volume, Elizabeth Joh’s chapter also hits home this point—explaining in detail the multitude of readily available data sources that obviate the need for reliance on something like a period tracker to establish an inference that a person is seeking an abortion. Elizabeth Joh, *Dobbs Online: Digital Rights as Abortion Rights*, in *FEMINIST CYBERLAW* (Meg Leta Jones and Amanda Levenowski, eds., 2024). Joh further notes that “digital self-help” strategies are unlikely to be of much utility for poor women, who comprise the majority of abortion seekers. *Id.*
33. In corroboration of Conti-Cook’s point, a prominent case in Nebraska a few weeks after the *Dobbs* ruling demonstrated the inefficacy of narrow privacy protection for abortion-seeking. In this case, police investigated a seventeen-year-old and her mother after receiving a tip that the women had purchased medication to induce abortion and had buried the fetus. Police submitted a search warrant to Meta (Facebook’s parent company) and were able to obtain private direct messages between the teenager and her mother discussing the situation, which provided critical evidence. Both the teenager and her mother were charged with several felonies. See Jason Koebler and Anna Merlan, *This Is the Data Facebook Gave Police to Prosecute a Teenager for Abortion*, MOTHERBOARD (Aug. 9, 2022), <https://www.vice.com/en/article/n7zevd/this-is-the-data-facebook-gave-police-to-prosecute-a-teenager-for-abortion>.
34. See Abby Ohlheiser, *Anti-Abortion Activists Are Collecting the Data They’ll Need for Prosecutions Post-Roe*, MIT TECH. REV. (May 31, 2022), <https://www.technologyreview.com/2022/05/31/1052901/anti-abortion-activists-are-collecting-the-data-theyll-need-for-prosecutions-post-roe/>; Alfred Ng, *Data Brokers Resist Pressure to Stop Collecting Info on Pregnant People*, POLITICO (Aug. 1, 2022), <https://www.politico.com/news/2022/08/01/data-information-pregnant-people-00048988>.

35. This point echoes a similar issue in analyses of the privacy risks of “sex tech”: the tendency to focus on the “sexiest” and most novel examples of potential privacy breach (e.g., connected sex toys) to the exclusion of the quotidian, generalized avenues through which most intimate surveillance occurs (e.g., email, search). See Karen Levy, *The Phallus-y Fallacy: On Unsexy Intimate Tracking*, 18 AM. J. BIOETHICS 22 (2018).

36. Sharmila Devi, *Anti-Abortion Groups Target Funding of Planned Parenthood*, 386 LANCET 941 (2015).

37. Center for Medical Progress v. Planned Parenthood Federation of Am., 551 F. Supp. 3d 320, 324 (S.D.N.Y. 2021).

38. Jackie Calmes, *Planned Parenthood Videos Were Altered, Analysis Finds*, NEW YORK TIMES (Aug. 27, 2015), <https://www.nytimes.com/2015/08/28/us/abortion-planned-parenthood-videos.html>.

39. The National Abortion Federation collects detailed data about the frequency of different types of violence and disruption propagated against providers, and has done so since 1977. Its most recent available statistics show significant year-on-year increases in stalking, blockades of abortion facilities, suspicious packages, vandalism, invasions, and assault and battery. See National Abortion Federation, *2021 Violence and Disruption Statistics*, [https://prochoice.org/wp-content/uploads/2021\\_NAF\\_VD\\_Stats\\_Final.pdf](https://prochoice.org/wp-content/uploads/2021_NAF_VD_Stats_Final.pdf). In 2015, the year of the Center for Medical Progress misinformation campaign, there were marked increases in death threats and threats of harm to providers, picketing, hate mail, and other forms of disruption. See National Abortion Federation, *2015 Violence and Disruption Statistics*, <https://prochoice.org/wp-content/uploads/2015-NAF-Violence-Disruption-Stats.pdf>.

40. See Michael Vitiello, *The Nuremberg Files: Testing the Outer Limits of the First Amendment*, 61 OHIO ST. L.J. 1175 (2000); Rene Sanchez, *Abortion Foes’ Internet Site on Trial*, WASHINGTON POST (Jan. 15, 1999), <https://www.washingtonpost.com/archive/politics/1999/01/15/abortion-foes-internet-site-on-trial/a284d05f-f83b-4eae-ad57-61985b66eaae/>.

41. AbortionDocs.org, <https://abortiondocs.org/>.

42. AbortionDocs.org *Disclaimer*, <https://abortiondocs.org/disclaimer/>.

43. *Id.*

44. See Emma Bowman, *As States Ban Abortion, The Texas Bounty Law Offers a Way to Survive Legal Challenges*, NPR (July 11, 2022), <https://www.npr.org/2022/07/11/1107741175/texas-abortion-bounty-law>.

45. See Meryl Kornfield, *A Website for ‘Whistleblowers’ To Expose Texas Abortion Providers Was Taken Down—Again*, WASHINGTON POST (Sept. 6, 2021), <https://www.washingtonpost.com/nation/2021/09/06/texas-abortion-ban-website/>.

46. See Digital Defense Fund, *Keep Your Abortion Private and Secure*, <https://digitaldefensefund.org/ddf-guides/abortion-privacy>.

47. *All About Geofencing*, Choose Life Marketing, <https://www.chooselifemarketing.com/all-about-geofencing/>.

48. See Center for Reproductive Rights, *supra* note 4.

49. Claire Wardle and Hossein Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe Report No. DGI(2017)09 (Sept. 27, 2017), <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c>, at 20–22.

50. Kim Bellware, *Lawmakers Urge Google to Fix Abortion Searches Suggesting “Fake Clinics,”* WASHINGTON POST (June 18, 2022), <https://www.washingtonpost.com/health/2022/06/18/google-abortion-clinic-searches-fake/>. See also Yelena Mejova, et al., *Googling for Abortion: Search Engine Mediation of Abortion Accessibility in the United States*, 2 J. QUANTITATIVE DESCRIPTION 1 (2022) (describing the frequency of listings for crisis pregnancy centers vs. abortion clinics in response to search queries).