Business and Human Rights Journal (2023), **8,** 259–264
doi:10.1017/bhj.2023.16

Business and Human Rights Journal

DEVELOPMENTS IN THE FIELD

Protecting Reproductive Rights Post-*Roe*: Can Companies Keep Your Data Safe?

Meagan Barrera[1] and Danny Rayman Labrin[2]

[1]Independent Scholar, USA
[2]Independent Scholar, Chile
Corresponding author: Meagan Barrera; Email: Meaganmbarrera@gmail.com

Abstract

The United States Supreme Court decision in *Dobbs v Jackson Women's Health Organization* brought to the forefront the intersections between technology and reproductive rights. As the country grappled with the impact of *Dobbs* on reproductive rights, digital and human rights experts warned that the vast amounts of data collected by companies could now be used to target and punish people seeking or facilitating access to abortions. This is the most recent manifestation of the negative impact technology can have on women, girls and persons of diverse sexual orientations and gender identities, and represents a global challenge for companies that collect, store, share and process user data. To fulfill their responsibility to respect human rights, companies should take steps to prevent the risks associated with collecting, storing, sharing and processing user data, and adapt these steps to respond to emerging risks, such as those now posed by the *Dobbs* decision.

Keywords: Data; gender; reproductive rights; right to privacy; technology

I. Introduction

In June 2022, the United States Supreme Court decision in *Dobbs v Jackson Women's Health Organization* (*Dobbs*) rolled back reproductive rights and access to abortion across the country. With the *Dobbs* decision, historic abortion bans previously deemed unconstitutional by the 1973 *Roe v Wade* decision took effect, as did restrictive abortion laws passed since 1973.[1] In some of the most restrictive states, this has put pregnant people's lives at risk,[2] and may lead to the criminalization of individuals for facilitating access to abortions.[3]

The ruling in *Dobbs* has broad-reaching impacts not only on reproductive healthcare and health rights, but also in the context of technology and human rights. Digital and human rights experts have long cautioned that companies' collection of vast amounts of user data

[1] Center for Reproductive Rights, 'Roe v. Wade', https://reproductiverights.org/roe-v-wade/ (accessed 18 February 2023).

[2] Rachel Treisman, 'States with the Toughest Abortion Laws have the Weakest Maternal Supports, Data Shows', *NPR* (18 August 2022), https://www.npr.org/2022/08/18/1111344810/abortion-ban-states-social-safety-net-health-outcomes (accessed 18 February 2023); Center for Reproductive Rights, 'The Disproportionate Harm of Abortion Bans: Spotlight on Dobbs v. Jackson Women's Health' (29 August 2021), https://reproductiverights.org/supreme-court-case-mississippi-abortion-ban-disproportionate-harm/ (accessed 18 February 2023).

[3] Center for Reproductive Rights, 'After Roe Fell: Abortion Laws by State', https://reproductiverights.org/maps/abortion-laws-by-state/ (accessed 18 February 2023).

© The Author(s), 2023. Published by Cambridge University Press.

https://doi.org/10.1017/bhj.2023.16 Published online by Cambridge University Press

poses significant risks to people's right to privacy as well as other fundamental rights and freedoms.[4] This situation is not unique to the United States. As long-established rights are stripped away in countries around the world, companies that collect, store, share and process user data may increasingly face situations where that data are used to infringe upon their users' rights.

Since the *Dobbs* decision, civil society has called on companies to protect user data, limit data collection, and provide reassurance that users will not be put at risk of punishment for exercising their reproductive rights.[5] Companies must adapt their policies and practices to new threats to human rights, and the *Dobbs* decision requires that they double up on their efforts to prevent and mitigate the increased risks to reproductive rights. This piece outlines the risks to reproductive rights of collecting, storing, sharing and processing user data in general, and in light of the *Dobbs* decision in particular, and shares how companies can address these risks.

II. Technology, Privacy and Reproductive Rights

Technology dominates our daily lives and companies have amassed a broad range of user data, including health data and data that can be used to infer sensitive health-related information about individuals. Experts note that such data collection has disproportionate impacts on the privacy and security of women, girls and persons of diverse sexual orientations and gender identities.[6] Technology, and data collected by companies, has regularly been used to target, harass and surveil women and girls, including for their sexual and reproductive health choices.[7] Following the decision in *Dobbs,* the risks to women and girls have increased significantly, and companies are again confronted with how their collection of user data could be used to violate reproductive rights and associated fundamental rights.

Right to Privacy Online

In the digital age, ensuring privacy protections for online data is critical to protecting many human rights, including access to abortion and reproductive rights, and to preventing the persecution of those who have accessed those rights.

[4] American Civil Liberties Union, *Informational Privacy in the Digital Age* (New York: American Civil Liberties Union, 2015), https://www.aclu.org/other/human-right-privacy-digital-age (accessed 18 February 2023); Human Rights Council (HRC), 'The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights', A/HRC/39/29 (3 August 2018).

[5] Privacy International, 'Privacy and Sexual and Reproductive Health in the Post-Roe World' (22 July 2022), https://privacyinternational.org/long-read/4937/privacy-and-sexual-and-reproductive-health-post-roe-world (accessed 27 March 2023); Jake Laperruque et al, 'Following the Overturning of Roe v Wade, Action is Needed to Protect Health Data', Center for Democracy and Technology (24 June 2022), https://cdt.org/insights/following-the-overturning-of-roe-v-wade-action-is-needed-to-protect-health-data/ (accessed 27 March 2023); Corynne McSherry and Katharine Trendacosta, 'What Companies Can Do Now to Protect Digital Rights in a Post-Roe World', *Electronic Frontier Foundation* (10 May 2022), https://www.eff.org/deeplinks/2022/05/what-companies-can-do-now-protect-digital-rights-post-roe-world (accessed 27 March 2023).

[6] Association for Progressive Communications, 'Gender Perspectives on Privacy: Submission to the United Nations Special Rapporteur on the Right to Privacy' (October 2018), https://www.apc.org/sites/default/files/APC_submission_Gender_Perspectives_on_Privacy_Oct_2018.pdf (accessed 18 February 2023).

[7] Ibid, 13–15; Cat Zakrzewski et al, 'Texts, Web Searches About Abortion Have Been Used to Prosecute Women', *The Washington Post* (3 July 2022), https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/ (accessed 27 March 2023); Jason Koebler and Anna Merlan, 'This is the Data Facebook Gave Police to Prosecute a Teenager for Abortion' *Vice* (9 August 2022), https://www.vice.com/en/article/n7zevd/this-is-the-data-facebook-gave-police-to-prosecute-a-teenager-for-abortion (accessed 27 March 2023).

https://doi.org/10.1017/bhj.2023.16 Published online by Cambridge University Press

In 2019, the United Nations Human Rights Council (HRC) clarified that the right to privacy applies online, and acknowledged the potential negative impacts that emerging technologies can have on privacy.[8] The HRC further noted the particular impacts technology may have on women and members of vulnerable and marginalized groups,[9] and encouraged businesses that collect, store, share and process data to meet their responsibility to respect human rights, including the right to privacy, in accordance with the United Nations Guiding Principles on Business and Human Rights (UNGPs).[10]

The failure to protect online privacy can have far-reaching implications for a broad spectrum of human rights, and as highlighted by the HRC, businesses must take steps to put in place adequate policies and safeguards to protect these rights.

Third Party Access to User Data

Companies that collect, sell, share or aggregate user data must consider how that data can be used by third parties to infringe upon human rights, including reproductive rights.[11] For example, investigations into reproductive health apps revealed that these apps shared detailed and sensitive data with social media platforms, raising concerns about the companies' privacy practices and user consent.[12] Data brokers that collect or purchase user data are still largely unregulated in the United States, and companies may not even be aware of how the data they collect, sell or share is used, including whether it ends up in the hands of law enforcement and other state bodies.[13] Recent research found that data brokers sold the location data of people who visited abortion clinics in the United States, revealing the risks such data pose to the exercise of reproductive rights.[14]

Data shared with third parties could also be used to target specific populations to sell products and services or promote disinformation with the aim of restricting sexual and reproductive health decisions, contributing to gender-based discrimination.[15] In one example, anti-abortion groups used data-driven surveillance to target women contemplating abortion for the purpose of sending them anti-abortion advertisements.[16] Experts have warned that these groups could go further, using that data to target people that have facilitated access to abortions post-*Roe*.[17]

[8] HRC, 'The Right to Privacy in the Digital Age: Resolution', A/HRC/RES/42/15 (26 September 2019).

[9] Ibid.

[10] Ibid.

[11] Stefanie Felsberger, 'Cycles of Control: Private Companies and the Surveillance of Reproductive Health', *Tactical Tech* (21 February 2023), https://tacticaltech.org/news/cycles-of-control/ (accessed 23 February 2023).

[12] Privacy International, 'No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data' (9 September 2019), https://www.privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data (accessed 23 February 2023).

[13] Center for Democracy and Technology, *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers* (Washington DC: Center for Democracy and Technology, 2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf (accessed 18 February 2023).

[14] Joseph Cox, 'Data Broker is Selling Location Data of People Who Visit Abortion Clinics', *Vice* (3 May 2022), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood (accessed 18 February 2023).

[15] Felsberger, note 11; Association for Progressive Communications, note 6, 18.

[16] Sharona Coutts, 'Anti-Choice Groups Use Smartphone Surveillance to Target "Abortion-Minded Women" During Clinic Visits', *Rewire News Group* (25 May 2016), https://rewirenewsgroup.com/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/ (accessed 18 February 2023).

[17] Abby Ohlheiser, 'Anti-Abortion Activists are Collecting the Data They'll Need for Prosecutions post-Roe', *MIT Tech Review* (31 May 2022), https://www.technologyreview.com/2022/05/31/1052901/anti-abortion-activists-are-collecting-the-data-theyll-need-for-prosecutions-post-roe/ (accessed 18 February 2023); Harriet Barber, 'Abortion

https://doi.org/10.1017/bhj.2023.16 Published online by Cambridge University Press

Experts have further highlighted the risks of sharing user data in response to government requests. While companies regularly share information with law enforcement agencies to prevent crimes such as money laundering or online child sexual abuse, governments also request information from companies for investigations that could lead to human rights violations.[18] With abortion criminalized in several states across the United States after *Dobbs*, there is an elevated risk of law enforcement agencies using personal data to infer sensitive information regarding an individual's reproductive choices.[19] This can lead to the arrest and criminal prosecution of women and girls who undergo abortions, and for those who assist them.

Company Practices Not Fit for Purpose

A recent analysis from the Business & Human Rights Resource Centre of the policies of 63 companies operating in the United States relating to third party access to user data revealed significant shortcomings in these policies, as well as discrepancies between policies and company statements about their actual practices. Overall, the surveyed companies were not able to demonstrate robust human rights due diligence processes to identify, prevent and mitigate the risks to reproductive rights of allowing third-party access to user data.[20]

The company responses indicated a lack of comprehensive knowledge on how their data collection, storage, sharing and processing could contribute to privacy violations.[21] They also indicated significant gaps in company policies regarding third-party access to user data,[22] increasing the risk of data being used to target people seeking or facilitating access to abortions. Digital rights experts have also repeatedly pointed out vulnerabilities in companies' policies and practices that compromise the privacy and security of user data, including with regard to health-related data.[23] In the United States, this has resulted in multiple instances where users' privacy was compromised, and online data were used to prosecute individuals ending their pregnancies or facilitating access to abortions.[24]

As companies have become increasingly aware of the human rights risks associated with sharing user data with governments, many have taken steps to mitigate these risks, including by requiring a warrant before disclosing user data and publishing transparency reports on government requests.[25] However, these steps are often not enough to protect users' reproductive rights. For example, governments can use broad warrants known as geofence and keyword search warrants to request large groups of data and identify

Surveillance: How Women's Bodies are Being Monitored', *The Telegraph* (10 October 2022), https://www.telegraph.co.uk/global-health/women-and-girls/new-abortion-surveillance-state-keeping-tabs-women/ (accessed 18 February 2023).

[18] Dunstan Allison-Hope, 'A New Transparency Challenge for Business and Human Rights', *BSR Blog* (25 February 2019), https://www.bsr.org/en/blog/transparency-business-and-human-rights-government-law-enforcement (accessed 23 March 2023).

[19] Laperruque et al, note 5; McSherry and Trendacosta, note 5.

[20] Business & Human Rights Resource Centre, *Damaging Data: Corporate Due Diligence and Reproductive Rights* (London: Business & Human Rights Resource Centre, 2022).

[21] Ibid, 6.

[22] Business & Human Rights Resource Centre, note 20, 7.

[23] Privacy International, note 5; Laperruque et al, note 5; McSherry and Trendacosta, note 5.

[24] Runa Sandvik, 'How US Police Use Digital Data to Prosecute Abortions', *TechCrunch* (27 January 2023), https://techcrunch.com/2023/01/27/digital-data-roe-wade-reproductive-privacy/ (accessed 27 March 2023).

[25] Rainey Reitman, 'Who Has Your Back? Government Data Requests 2017', *Electronic Frontier Foundation* (10 July 2017), https://www.eff.org/who-has-your-back-2017 (accessed 27 March 2023).

https://doi.org/10.1017/bhj.2023.16 Published online by Cambridge University Press

individuals that may have visited abortion clinics.[26] Government entities have also obtained user data from private data brokers, circumventing the judicial process entirely.[27]

While several companies have policies outlining how they will respond to government requests for user data and note that they will challenge unlawful requests, many may not be equipped to deal with this new legal landscape in the United States.[28] Indeed, user data obtained via law enforcement requests have already been used to charge individuals for ending their pregnancies or facilitating access to abortion. In 2015 and 2017, women in Mississippi and Indiana were prosecuted for ending their pregnancies in cases which used their search histories and text messages as evidence.[29] After *Dobbs*, cases like these are likely to increase. In 2022, Meta provided Facebook Messenger records to police who brought felony charges against a mother who helped her 17-year-old daughter access abortion pills.[30]

III. The Corporate Responsibility to Ensure Privacy and Security of User Data

The human rights risks outlined above demonstrate a clear need for companies to proactively adopt policies to limit and protect the user data they collect, store, share and process. These human rights risks are not new, nor are the impacts on reproductive rights following the *Dobbs* decision. In the most restrictive states across the United States, user data were already being used to prosecute people for terminating pregnancies before *Dobbs* struck down the constitutional right to abortion.[31] To address these concerns, companies should take steps to prevent, mitigate and remedy the human rights harms associated with the data they collect, in line with international human rights standards and norms.

The Office of the United Nations High Commissioner for Human Rights and Special Rapporteur on the promotion and protection of the right to freedom of expression have both emphasized the importance of adopting and implementing the UNGPs to protect human rights in the digital age.[32] However, as evidenced by the Business and Human Rights Resource Centre's research mentioned earlier, many companies have not taken the necessary steps to identify, assess and mitigate the risks to reproductive rights of collecting user data.[33]

In addition to adopting human rights due diligence processes, there are several steps companies can take to protect user data from being used to restrict reproductive rights and other fundamental rights and freedoms. This includes limiting data collection, allowing anonymous or pseudonymous access to products and services, allowing users to choose the types of data collected or to completely erase all data, and strengthening data encryption.[34]

[26] Johana Bhuiyan, 'How Can US Law Enforcement Agencies Access Your Data? Let's Count the Ways', *The Guardian* (4 April 2022), https://www.theguardian.com/technology/2022/apr/04/us-law-enforcement-agencies-access-your-data-apple-meta (accessed 27 March 2023); McSherry and Trendacosta, note 5.

[27] Caitlin T Chin, 'Statement Before the House Judiciary Committee – Digital Dragnets: Examining the Government's Access to Your Personal Data', *Center for Strategic & International Studies* (19 July 2022), https://csis-website-prod.s3.amazonaws.com/s3fs-public/congressional_testimony/ts220719_Chin.pdf?VersionId=tUyXcdbLnovu3CpK73x0nC9zZiHyW6lj (accessed 27 March 2023).

[28] Business & Human Rights Resource Centre, note 20, 8.

[29] Zakrzewski et al, note 7.

[30] Koebler and Merlan, note 7.

[31] Zakrzewski et al, note 7; Sandvik, note 24.

[32] HRC, 'The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights', A/HRC/27/37 (30 June 2014), paras 43–45; HRC, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', A/HRC/38/35 (6 April 2018), para 10.

[33] Business & Human Rights Resource Centre, note 20, 3.

[34] McSherry and Trendacosta, note 5; Laperruque et al, note 5.

https://doi.org/10.1017/bhj.2023.16 Published online by Cambridge University Press

Companies can further ensure transparency by publishing easily accessible information about privacy policies, third-party access to user data and government requests for user data broken down by location, type of information requested and reasons for the requests.[35] Companies should also find ways of warning users of the types of data that could be used by third parties to infer health-related and other sensitive information and put their reproductive and other human rights at risk.

Companies should further refrain from sharing users' data with third parties unless informed consent for sharing the specific category of data is provided, and a human rights due diligence assessment has been conducted on those third parties.[36] With regard to government requests for user data, companies should adopt clear policies that set meaningful limits to the data provided, and challenge unlawful and overly broad requests.[37] If companies are legally required to share data, they should limit the types of information to only that which narrowly responds to the request, and notify users at the earliest opportunity when information is shared.[38]

These actions represent best practices as identified by human rights and digital rights experts,[39] and are all the more critical after the *Dobbs* decision. While many companies have already adopted such policies, a significant number is still falling behind.[40] In addition, these steps alone may not be sufficient when protections for long-established rights are repealed. Therefore, companies must remain vigilant to changes in regulatory frameworks and assess how their data collection practices may increase risks to human rights in light of those changes. This includes considering the aggravated or disproportionate impacts that collecting user data can have on certain groups of rights-holders, such as women, girls and people with diverse sexual orientations and gender identities.

Competing interest. Meagan Barrera is employed by the Business & Human Rights Resource Centre and Danny Rayman Labrin is a consultant with the Business & Human Rights Resource Centre.

[35] McSherry and Trendacosta, note 5.

[36] McSherry and Trendacosta, note 5; Verónica Ferrari, 'Facebook and Privacy in the post-Roe Era', Association for Progressive Communications (13 September 2022), https://www.apc.org/en/news/facebook-and-privacy-post-roe-era (accessed 30 March 2023).

[37] McSherry and Trendacosta, note 5; Laperruque et al, note 5.

[38] Ibid.

[39] Privacy International, note 5; Laperruque et al, note 5; McSherry and Trendacosta, note 5.

[40] Business & Human Rights Resource Centre, note 20, 6–8; Reitman, note 25.

https://doi.org/10.1017/bhj.2023.16 Published online by Cambridge University Press