20 YEARS OF
Business & Human Rights Resource Centre

Photo by Seattle City Council

Damaging data

CORPORATE DUE DILIGENCE AND REPRODUCTIVE RIGHTS

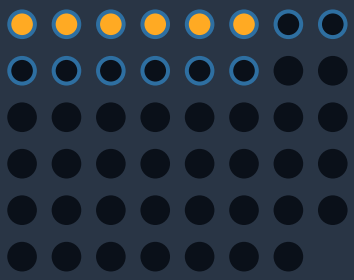
DECEMBER 2022

Executive summary

A wide range of rights were served a far-reaching and catastrophic blow by the United States (US) Supreme Court's June 2022 decision in *Dobbs v. Jackson Women's Health Organization*, which rolled back reproductive rights and access to abortion across the country. In addition to the deleterious effect on health rights, including access to reproductive healthcare, the ruling has broader repercussions – not least in the under-explored area of tech and rights. Digital and human rights experts are already warning data collection by technology and financial companies could be used in investigations and court cases to enforce anti-abortion laws. This poses significant risks to people's right to privacy, as well as other fundamental rights and freedoms. It is clear that companies dealing in data need to be alert to what this means for them.

With the *Dobbs* decision, historic abortion bans – deemed unconstitutional by the landmark 1973 *Roe v. Wade* decision but never repealed – took effect, as did numerous restrictive abortion laws passed since 1973. Chillingly, in some of the most restrictive states this has put pregnant people's lives at risk. It has also opened the possibility for people to be punished for seeking abortions, healthcare professionals to be punished for providing them, and friends and family members to be punished for helping people access abortions.

63 tech and finance companies surveyed



14/63 responded

6/63 acknowledged the changed landscape for reproductive rights and described actions taken

0/63 described their human rights due diligence risk assessment methodologies

The concern that user data and payment data amassed by technology and financial companies could be called as evidence has long been legitimate, even before stricter bans came into effect. 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. In a recent case, Meta provided Facebook Messenger records to police who brought felony charges against a mother who helped her 17-year-old daughter access abortion pills. Meta commented that warrants were received prior to the Supreme Court decision and did not mention abortion. Civil society experts have 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.

In response to these concerns, Business & Human Rights Resource Centre invited 63 technology and financial companies operating in the US and collecting user or payment data which may be used to target people seeking, providing, or facilitating access to abortions and reproductive healthcare to respond to survey questions on their transparency and human rights due diligence processes. The results revealed limited transparency, gaps in human rights due diligence processes to understand rights implications associated with data collection in this context, a woeful lack of knowledge on how data collection could contribute to violating users' rights, and apparent gaps in company policies and practices regarding third-party access to data, including government requests for access to information.

Company transparency on the collection, storage, and use of sensitive data is a critical part of ensuring users' right to privacy. Companies must have in place robust human rights due diligence processes to assess how their collection, storage, and use of data may be used to infringe upon users' rights, and to put in place policies and processes to mitigate or remedy harms. Failure to assess the risks in a post-*Roe* context may contribute to violations of users' rights to privacy, freedom of expression, and the exercise of reproductive rights. These findings paint a bleak picture of the sector's awareness of its role in the possible infringement of its users' rights as a consequence of the *Dobbs* decision; urgent action to mitigate these impacts is required.

Analysis

The 63 companies invited to respond to our survey were selected based on their appearance in media coverage on the topic and identification by digital rights experts. Twenty-five of the companies are reproductive health apps, 24 companies are financial institutions or payment providers, two are telecommunications companies, two are third-party data providers, and the remaining 10 are tech companies.

Sector: Finance & banking · Internet & social media · Technology, telecom & electronics · Transport

Response: No response · General response · Partial response · Full response

- 1199 SEIU Federal Credit Union
- Alphabet
- Amazon.com
- Amalgamated Bank
- American Airlines Credit Union
- American Express
- Apple
- AT&T
- Bank of America
- Binance
- Capital One
- Citigroup
- Clue (BioWink)
- CashApp
- Coinbase
- Discord
- Discover
- Everyday Health, Inc.
- Flo Health
- Frost Bank
- Garmin
- Glow Inc.
- Goldman Sachs
- GP International LLC
- HealthEquity
- JPMorgan Chase
- Kochava
- The Knot Worldwide Inc.
- Lyft
- Mastercard
- Med ART Studios
- Meta
- Navy Federal Credit Union
- Natural Cycles
- Oura
- Ovuline, Inc., doing business as Ovia Health
- Philips Digital UK Limited
- Placer.ai
- Plackal Tech
- Preglife AB
- Prosperity Bank USA
- SafeGraph
- Signal
- Simple Design LTD or ABISHKKING LIMITED
- SimpleInnovation
- Snap
- T-Mobile
- TikTok
- Twitter
- Uber
- University of Wisconsin Credit Union
- USAA
- US Bank
- Venmo (part of PayPal)
- Verizon
- Visa
- Wachanga
- WebMD
- Wells Fargo
- Western Union
- WhatsApp
- Whoop
- Women Help Women International Foundation

Fourteen companies (just over a fifth, 22%) responded to the survey questions that focused on human rights due diligence processes, third-party access to data, and responding to government requests for data. Our analysis revealed both shortcomings and examples of better practice among the 14 responding companies.

Key findings:

- Eight out of 14 companies acknowledged the US Supreme Court decision in *Dobbs vs. Jackson Women's Health Organization* restricting access to abortion and reproductive healthcare.

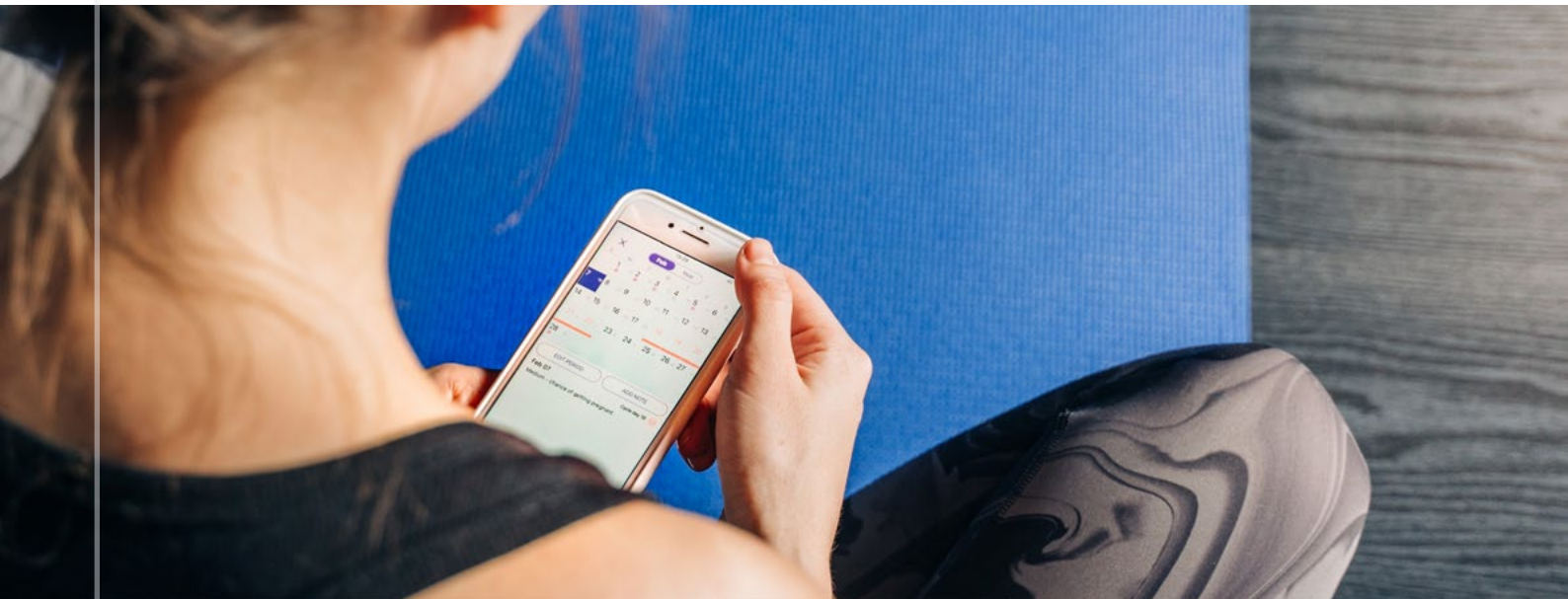
- Six companies (**Clue**, **Flo Health**, **Natural Cycles**, **Philips Digital UK**, **Preglife**, and **TikTok**) acknowledged the changed landscape following the Supreme Court decision and described actions taken to respond. Some actions, such as introducing "anonymous mode" and strengthening encryption of user data, are in line with recommendations from digital rights experts and represent best practice among the surveyed companies.

- Only two companies (**Clue** and **Flo Health**) acknowledged privacy as a human right; the remaining 12 companies reiterated their commitment to protecting users' privacy and shared privacy policies. **Natural Cycles** and **SimpleInnovation** adapted their privacy policies, while **Philips Digital UK** and **TikTok** described processes to review their policies following the Supreme Court decision.

- None of the 14 respondent companies explained their human rights due diligence risk assessment methodologies or outlined how human rights factor into those risk assessments. Only one company, **Natural Cycles**, stated it had conducted a risk assessment, described the main risk identified as a potential subpoena for user data, and explained how it plans to mitigate that risk.

- Five companies (**Bank of America**, **Citigroup**, **Glow**, **Med ART Studios**, and **Meta**) did not share information regarding their policies or guidelines to address government requests, notifications to their users, or steps to challenge unlawful government or law enforcement requests for user data.

Companies which did not reference any steps taken to respond to the changed context following the decision or said their general privacy policies already protected user data so did not require changes were the weakest responses.



Human rights due diligence

Overall, companies did not share sufficient information to determine whether they are conducting effective human rights due diligence (HRDD) processes in line with the UN Guiding Principles on Business and Human Rights (UNGPs) to identify, prevent, and mitigate human rights risks associated with data that could be used to restrict health rights and access to reproductive healthcare. Based on the responses received, companies do not appear to be aware of the full range of human rights risks associated with the data they collect or the steps needed to mitigate those risks.

Four companies (**Flo Health**, **Natural Cycles**, **SimpleInnovation**, and **Clue**) acknowledged the health-related data they collect and store is particularly at risk and described steps taken to ensure data is safe. **TikTok** was the only non-health tech company to acknowledge that while the data it collects is not directly health-related, it could potentially be used to infer health-related information.

None of the 14 respondent companies explained their HRDD risk assessment methodologies or outlined how human rights factor into those risk assessments. Only one company, **Natural Cycles**, stated it had conducted a risk assessment, described the main risk identified as a potential subpoena for user data, and explained how it plans to mitigate that risk.

Two companies (**Meta** and **TikTok**) referenced HRDD and risk assessment processes generally without clarifying whether a risk assessment had been conducted since the *Dobbs* decision to identify new risks. **Flo Health** and **Glow Inc.** described general third-party privacy and security assessments and **Preglife** described an internal auditing process.

Communicating risk assessment results, including how identified risks are being addressed, and showing stakeholders that adequate policies and practices are in place are key features of HRDD as outlined by the UN Working Group on Business and Human Rights. Based on the responses received, few companies appear to be fulfilling this responsibility.

Rights to privacy and freedom of expression

Based on the responses we received, companies appear to lack comprehensive knowledge on how the collection, storage and use of data may contribute to violations of users' rights to privacy and freedom of expression, and how that impacts other rights.

Only two companies, **Clue** and **Flo Health**, explicitly acknowledged privacy as a human right; the remaining 12 companies reiterated their commitment to protecting users' privacy and shared privacy policies. None of the 14 companies stated clearly how their collection and storage of user data may inhibit the right to freedom of expression or steps they were taking to address that risk.

The strongest privacy protections described by companies included implementing "anonymous mode", allowing users to choose the type of data collected or revoke consent to collect data, limiting data collection, and providing the option to permanently delete all data. One company, **Med ART Studios**, stated it does not collect sensitive data for its Sprout pregnancy app and therefore only provided a general response that did not address all the questions in the survey. However, the privacy policy of Sprout's period and fertility tracker app states that it may collect personally identifiable and user-entered information which may present risks not addressed in **Med ART**'s response. **Med ART** did not explain how it evaluated risks to privacy and freedom of expression associated with other types of user data from the app, such as location and usage data.

Five out of 14 companies provided information on complaint mechanisms. Two companies (**Flo Health** and **Natural Cycles**) stated they employ Data Protection Officers (DPO) and share their contact information within their privacy policies for users to raise concerns. While Clue also provides an email address for users within its privacy policy, it did not specify who receives those complaints. Two companies (**SimpleInnovation** and **TikTok**) described processes for users to provide feedback to their customer support team or via a form.

Preglife stated it did not have a mechanism for users to raise complaints on the use of their data, however the company employs a DPO. Nine companies did not share any information about complaint mechanisms, and none of the 14 companies described how they review and act on complaints.

Third-party access to data

Survey responses indicate significant gaps in companies' policies and practices regarding third-party access to user data. Moreover, companies failed to disclose robust human rights due diligence processes to identify, prevent, and mitigate the risks posed by potential third-party access to user data.

Eight companies (**Flo Health**, **Natural Cycles**, **Preglife**, **SimpleInnovation**, **Glow Inc.**, **Clue**, **TikTok**, and **Western Union**) stated they do not sell data to third parties. Glow further asserted it does not share personal data, however there is a discrepancy between the response and what is declared in its privacy policy, which outlines that user data could be shared with third-party apps and third-party advertisers can engage with users' data.

TikTok stated it does not sell its users' personal data to advertisers or other third parties. The company also said its advertisers agree to terms prohibiting the collection or sharing of health-related information on **TikTok**'s behalf, but does not address when user data may be collected or shared on third parties' behalf. **TikTok** answered that it evaluates third parties via its risk management programme, which includes a review of third-party data privacy policies.

Flo Health explained that its "anonymous mode" ensures no single party processing user data has complete information on who the user is and what they are trying to access. **Clue** stated that following the Supreme Court decision it reviewed sub-processors to ensure they pose no additional risk. **Preglife** answered that it conducts an evaluation process before entering into any agreement where data may be available to third parties and has an auditing process for sub-contractors.

Government requests for data

Companies' survey responses indicate a lack of sufficient policies to respond to government requests for user data, such as subpoenas from law enforcement.

Five companies (**TikTok**, **T-Mobile**, **Western Union**, **Meta**, and **Flo Health**) referred to policies to address government requests for user data with detailed steps outlining the information they might disclose. However, only **Flo Health**, **T-Mobile**, **Meta**, and **TikTok** shared documents with guidelines related to government requests and stated they publish information on government requests for user information. **T-Mobile** shared its law enforcement Transparency Report for 2021, which provides information about responses prepared during 2021 to legal demands for customer information, including the types and number of legal demands in 2021. **TikTok** said it publishes a biannual report on government requests which provides information about the volume, type, and location of requests. **Natural Cycles**, **Preglife**, and **Flo Health** also explained they would notify users if they disclose information. However, only **Flo Health** and **TikTok** elaborate this process in their policies.

Six companies (**Flo Health**, **Philips Digital UK**, **Clue**, **TikTok**, **Western Union**, and **SimpleInnovation**) said government data requests are reviewed by their legal staff and explained that they would respond to compulsory law enforcement requests and would reject unlawful or overbroad requests. **Flo Health**, **SimpleInnovation**, **TikTok**, and **Western Union** further stated they would challenge or seek to narrow overly broad or unlawful requests. **Natural Cycles** and **Clue** additionally stated they are exploring legal avenues to resist such requests, and **Natural Cycles** noted it is setting up its app to avoid having access to such information to disclose.

Five companies (**Bank of America**, **Citigroup**, **Glow**, **Med ART Studios**, and **Meta**) did not share information regarding their policies or guidelines to address government requests, notifications to their users, or steps to challenge unlawful government or law enforcement requests for user data.

Conclusion and recommendations

Companies collect vast amounts of user data, from health-related data to location and payment data. They must take steps to protect users' rights to privacy and freedom of expression, and address how that data may impact other rights including reproductive rights and access to healthcare. The recent prosecution of a woman in Nebraska following an abortion case which relied on evidence from private Facebook messages between her and her 17-year-old daughter puts the warnings of digital rights experts into stark relief: failure to conduct meaningful human rights due diligence in line with the UNGPs to identify, prevent, and mitigate human rights risks will result in the restriction of health rights and reproductive freedom.

Recommendations for companies:

- Strengthen **human rights due diligence** processes in line with requirements set out in the UNGPs and OECD Guidelines for Multinational Enterprises to effectively identify, prevent, and mitigate human rights risks associated with the collection, storage, and use of user data, particularly with regard to health-related data or data that may be used to infer health-related information.

- Conduct and continually update a **human rights risk assessment**, with participation from impacted groups, to identify user data that may lead to restriction of health rights, including access to reproductive healthcare, and take action to prevent and mitigate those risks.

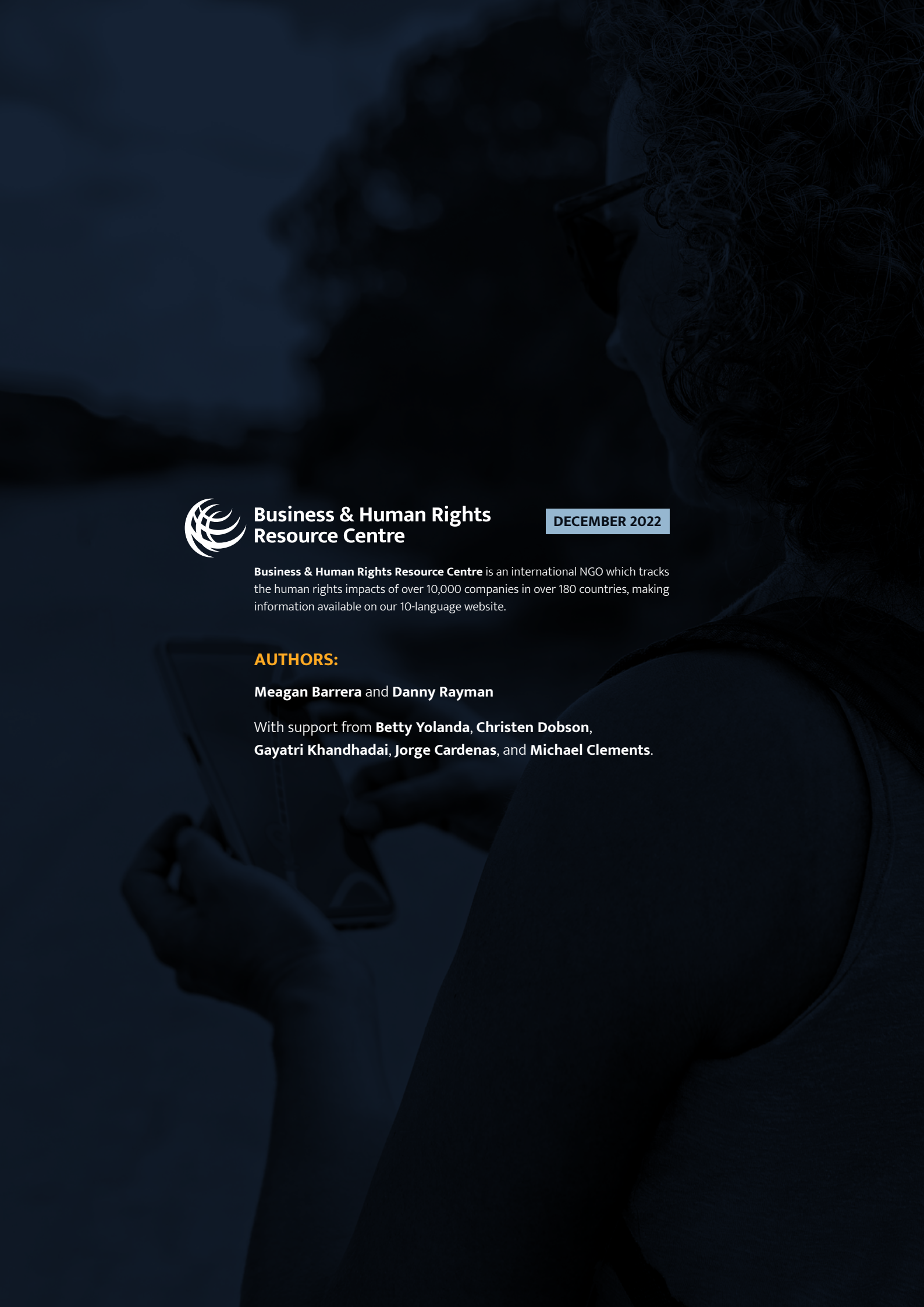
- Limit data collection, allow **anonymous access**, strengthen **data encryption** including end-to-end encryption for messaging, and provide easily actionable options for users to choose the types of data collected and to completely erase all data.

- Refrain from sharing users' data with third parties unless **informed consent to data sharing** for the specific category of data is provided, and conduct **due diligence on third parties** which may have access to data.

- Develop policies on responding to **government requests for user data** which set clear and meaningful limits to the data given in response to any request.

- Challenge **unlawful and overly broad government requests for user data**. If legally required to share data, limit the types of information that can be shared in response to requests and notify users at the earliest opportunity when information is shared.

- Ensure **transparency** by publishing easily accessible information regarding company privacy policies, third-party access to user data, and government requests for user data broken down by location, type of information requests, and reasons for request.



Business & Human Rights Resource Centre

DECEMBER 2022

Business & Human Rights Resource Centre is an international NGO which tracks the human rights impacts of over 10,000 companies in over 180 countries, making information available on our 10-language website.

AUTHORS:

Meagan Barrera and **Danny Rayman**

With support from **Betty Yolanda**, **Christen Dobson**, **Gayatri Khandhadai**, **Jorge Cardenas**, and **Michael Clements**.