PRIVACY AND SAFETY EXPERIENCES AND CONCERNS OF U.S. WOMEN USING GENERATIVE AI FOR SEEKING SEXUAL AND REPRODUCTIVE HEALTH INFORMATION

Ina Kaleva, Xiao Zhan, Ruba Abu-Salma, and Jose Such

King's College London

Background and Rationale. Generative AI (GenAI) chatbots have transformed how people access information, increasingly complementing, or in some cases replacing, traditional search engines [10]. Their use has expanded into healthcare, where they are emerging as a new source of sexual and reproductive health (SRH) information [1]. Many users find these tools appealing because they offer a conversational, human-like experience [9], provide personalized responses to individual queries [7], feel private and discreet [7], and are easy to use [9]. The 2022 United States (U.S.) Supreme Court decision Dobbs v. Jackson Women's Health Organization overturned Roe v. Wade and intensified legal restrictions on abortion in the U.S. As a result, people seeking abortion and other SRH services now face heightened safety risks, including surveillance, criminalization, stigma, gender-based violence, and targeted misinformation [5]. In states with limited access to abortion care, concerns have also increased about how digital traces may be used to identify or prosecute individuals seeking abortion- or other SRH-related information [5]. While prior research has mainly focused on technical aspects of privacy and the clinical efficacy of GenAI chatbots, users' privacy concerns and experiences with these tools remain largely understudied. To address this gap, we conducted semi-structured interviews with 18 individuals who used GenAI chatbots to seek SRH information in the post-Roe era, examining their privacy and safety concerns. Our research questions (RQs) are as follows:

RQ1. What factors facilitate or hinder the adoption and use of GenAI chatbots for seeking SRH information?
RQ2. What beliefs do users hold about data flows and practices when using GenAI chatbots to seek SRH information?
RQ3. What privacy and safety concerns do users have when using GenAI chatbots to seek SRH information? How do these concerns differ between restrictive and non-restrictive states and across various SRH topics?
RQ4. What privacy and safety protection strategies do GenAI chatbot users employ, or would consider employing, and how can GenAI chatbots be improved to better safeguard users seeking SRH information?

Methods. We conducted semi-structured interviews with 18 participants assigned female at birth and residing in the U.S. who sought SRH information via GenAI chatbots in the post-Roe era, exploring their privacy and safety experiences. We then employed thematic analysis [2] to analyze the data.

Results. We found that participants used GenAI chatbots for a wide range of SRH-related questions, often following the advice they received and frequently sharing personal details such as demographic information and sensitive SRH experiences (e.g., abortion). Participants valued GenAI chatbots for their convenience, accessibility, perceived credibility, privacy, and human-like interactions. Reported barriers included limited usefulness for serious health issues, usability challenges, doubts about accuracy, concerns about bias, and the lack of human empathy (RQ1). Participants were often unsure or held misconceptions about how GenAI chatbots collected, stored, shared, and deleted their data (RQ2). They generally perceived these tools as posing greater privacy risks than other sources of SRH information, including search engines, period-tracking apps, social media, or healthcare providers, largely due to the large amount of personal information disclosed during conversations. Participants also expressed concerns about risks related to model training, government access, profiling, advertising, and weak regulation. They identified potential harms such as criminalization, emotional harm, harassment, and stigma (RQ3). While most participants were willing to share SRH information if their GenAI chatbot was useful, many avoided asking abortion-related questions and, in some cases, other stigmatized topics, such as sexual orientation and gender identity. Finally, participants reported using relatively few privacy-protection strategies beyond data minimization or deleting conversations (RQ4).

Discussion and Recommendations. Many participants' concerns are well-founded. Although there is no evidence that tools like ChatGPT engage in proactive surveillance, law enforcement can subpoena companies to obtain

user data, and companies are legally obliged to comply [8]. Participants' worries about weak privacy protections are also justified, as sensitive health information shared with general-purpose GenAI chatbots is not covered by medical privacy laws such as HIPAA and remains in a regulatory grey area. Their concerns about advertising are consistent with recent industry practices: major GenAI providers (e.g., Meta, Microsoft, Google, OpenAI) have indicated plans to use user data for ad targeting, and Meta AI has stated it will collect users' text and voice interactions for advertising, except in the UK, EU, and South Korea [6]. Finally, concerns about data deletion are valid, since removing data from GenAI systems is extremely difficult once it has been used for training [3], making opt-in to training effectively an opt-out of permanent deletion. We propose practical and policy recommendations to improve privacy and safety in GenAI chatbots used for SRH information seeking.

- **GenAI regulatory protections:** Implement co-regulation (collaborative policymaking) between regulatory agencies and industry to create regulatory sandboxes that provide controlled environments for testing new policies; develop dedicated "health" models that comply with medical privacy laws; and enable healthcare providers to deploy GenAI models securely under strict local data controls.
- **Public awareness and involvement:** Implement educational programs to improve GenAI literacy for both users and clinicians, and conduct co-design workshops as part of a Participatory Action Research approach.
- **Privacy by Design:** Apply conservative filtering to remove or obfuscate sensitive content before user data enters the training pipeline; enable opt-outs of model training by default; advance machine-unlearning techniques and auditing tools to ensure data deletion; and use Reinforcement Learning from Human Feedback (RLHF) to train models to handle sensitive prompts responsibly.
- **Interactive privacy:** Implement explicit consent prompts during sensitive conversations in real time; gently discourage oversharing of personal information; provide safety warnings; offer reminders about available privacy settings; and redirect users to trusted resources.
- **Improved transparency:** Employ Explainable AI (XAI) approaches [4], including open-source models, data visualizations, alerts, and privacy nudges.

References

[1] Anas Alhur. "Redefining healthcare with artificial intelligence (AI): the contributions of ChatGPT, Gemini, and Co-pilot". In: *Cureus* 16.4 (2024). DOI: 10.7759/cureus.57795.

[2] Virginia Braun and Victoria Clarke. "Thematic analysis: A practical guide". In: (2021).

[3] Antonio Ginart et al. "Making ai forget you: Data deletion in machine learning". In: *Advances in neural information processing systems* 32 (2019).

[4] AKM Bahalul Haque, AKM Najmul Islam, and Patrick Mikalef. "Explainable Artificial Intelligence (XAI) from a user perspective: A synthesis of prior literature and problematizing avenues for future research". In: *Technological Forecasting and Social Change* 186 (2023), p. 122120.

[5] Michela Meister and Karen Levy. "Digital security and reproductive rights: Lessons for feminist cyberlaw". In: *Feminist Cyberlaw (Meg Leta Jones and Amanda Levendowski, eds.), University of California Press, Forthcoming* (2022). DOI: 10.2139/ssrn.4262774.

[6] Meta. *Improving Your Recommendations on Our Apps with AI.* Meta Newsroom. Accessed: 2025-11-18. Oct. 2025. URL: https://about.fb.com/news/2025/10/improving-your-recommendations-apps-ai-meta/.

[7] Rhiana Mills et al. "Chatbots to improve sexual and reproductive health: realist synthesis". In: *Journal of medical Internet research* 25 (2023), e46761. DOI: 10.2196/46761.

[8] OpenAI. *OpenAI ROW Privacy Policy.* Accessed: 2025-12-15. 2025. URL: https://openai.com/policies/row-privacy-policy/.

[9] Zhiping Zhang et al. ""It's a fair game", or is it? Examining how users navigate disclosure risks and benefits when using LLM-based conversational agents". In: *Proceedings of the CHI Conference on Human Factors in Computing Systems.* 2024, pp. 1–26. DOI: 10.48550/arXiv.2309.11653.

[10] Tao Zhou and Songtao Li. "Understanding user switch of information seeking: From search engines to generative AI". In: *Journal of Librarianship and Information Science* (2024), p. 09610006241244800. DOI: 10.1177/09610006241244800.