London
dcwriter89@gmail.com
Cite this as: *BMJ* 2022;378:o2075
http://dx.doi.org/10.1136/bmj.o2075
Published: 26 August 2022

How overturning Roe *v* Wade has eroded privacy of personal data

The US Supreme Court decision is making many women vulnerable to criminal prosecution, David Cox reports

David Cox *freelance journalist*

In early August, prosecutors from the Madison County attorney's office in Nebraska became the first law enforcement agency in the US to use private Facebook data to support a case against a teenager accused of having an illegal abortion.[1]

The messages between the accused, 17, and her mother were accessed after prosecutors sent a search warrant to Meta, Facebook's parent company, back in June. It represents the first instance of investigators accessing an individual's data from a tech company as part of an abortion case since the US Supreme Court's decision to overturn the 1973 Roe *v* Wade ruling.[2]

"We've learnt that Facebook cannot be trusted with anything," says Laura Shipp, a cyber security researcher at Royal Holloway, University of London. Shipp advises anyone seeking abortion information, or wishing to discuss the matter with family members or friends, to always do so through private browsers or encrypted messaging services to ensure that the information will not be stored on any database or shared with third parties.

The case has sparked campaigns calling for people to delete their accounts on the social media platform.[3] Now, Google employees are petitioning Alphabet, Google's parent company, to offer abortion benefits to contractors, suspend donations to anti-abortion politicians, and provide better protection for users against possible police requests.[4] But these tech giants are just one of many digital mediums that could be exploited as a way of obtaining information relating to a person's reproductive history, as US states look to clamp down on abortion.

Legal experts say that text messages, emails, geolocation data, online payment records, Google searches, and information accumulated by apps could all be used as means of proving guilt.

"The tech industry is built on this idea that your data is one of your most precious commercialisable resources," says Carmel Shachar, executive director of the Petrie-Flom Centre for Health Law Policy, Biotechnology, and Bioethics, at Harvard Law School. "People need to worry about the way they interact with the digital world when they're pregnant and they don't want to be pregnant."

In particular, the so called femtech industry has come under increasing scrutiny, with popular digital tools such as the period tracker app Flo becoming viewed as potential liabilities, especially as their business models involve collecting personal data and selling it to third parties. While many of these companies have announced new privacy protection measures in the wake of the Supreme Court decision—for instance, Flo has added an anonymous mode feature to let users remove identifiers such as name and email address from their profiles[5]—it remains to be seen whether this provides any real protection.

"If they have this data, I find it hard to know how they can protect it from subpoena if that happens," says Shipp. "I've not seen anything solid enough to suggest that that's not the case, at the moment."

Who owns your health data?

The possibility that femtech apps might be used to build legal cases against people suspected to have had abortions has thrown open the question of whether they should be more tightly regulated in future, to add more layers of protection over how this information is shared.

"These everyday apps have incredibly intimate details about our health, and yet they're not regulated as health devices," says Gina Neff, executive director of the Minderoo Centre for Technology and Democracy at the University of Cambridge. "They're falling into an ethical grey zone, where consumers are increasingly relying upon them, and yet they don't have the kinds of protections that they would have when sharing information with their doctors."

In the US, even private medical records are not considered sacrosanct when it comes to what investigators might be able to access. While medical privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA) provide some protection, personal medical data can still be subpoenaed if there is reason to believe that an illegal abortion has occurred.[6] Patients have little control over what happens because in virtually all US states, the law specifically states that either medical providers or hospitals own the data.

Nicole Huberfeld, professor of health law, ethics, and human rights at the Boston University School of Public Health, says that healthcare providers are not always obliged to cooperate with prosecutors. There has to be a specific reason for needing to access such confidential data.

"HIPAA does not stop subpoenas, but neither does it require healthcare providers to comply with broad subpoenas that are seeking unspecified information," she says. "Prosecutors cannot go on fishing expeditions by making a blanket request for all patients who appear to have had abortions that may have violated state laws."

Shachar predicts that the Nebraska case is likely to be something of an exception. Instead, she believes the majority of court cases in the coming years will be US states taking action against physicians or

hospitals suspected of providing abortions, rather than patients themselves, although the predicted rise of self-administered abortions could see more instances of patients being directly targeted.

"There's the worry that people will not seek out medical care, out of worry that these records will be discoverable," Shachar says. "The most important thing is that if patients have self-induced abortion and it's not going well, that they go get the care they need."

While the effect of the fall of Roe *v* Wade on medical data privacy has been felt most keenly in the US, the reverberations have reached other countries that have taken an anti-abortion stance, such as Poland.

On 6 June 2022, the Polish health minister signed a new regulation requiring doctors to record both past and current pregnancy information in a central register,[7] a move which was met with consternation from both women's rights groups and politicians.[8]

According to Atina Krajewska, a researcher in human rights law within health and medicine at the University of Birmingham Law School, the register is most likely to be used to build cases against those suspected of helping people access abortion services within Poland, which is illegal.

"While women are not criminalised, criminal sanctions have recently affected their family members," says Krajewska. "The internet behaviour of women has certainly changed. They are more careful ordering abortion pills online, seeking information about abortion, or organising abortion travel abroad. The disclosure of personal data can create an atmosphere of fear, surveillance, and uncertainty and undermine public trust in the healthcare system."

How much does the NHS protect the UK?

Even within the UK, researchers point out that people are not as protected as they might think, citing an ongoing court case in which a 25 year old woman in Oxford is facing trial for allegedly self-administering misoprostol, which is routinely prescribed by doctors at abortion clinics, with intent to procure a miscarriage.[9] The woman is being prosecuted under the 1861 Offences Against the Person Act, which was introduced to stop black market abortions in Victorian England, for acting without medical authorisation, a charge that carries a maximum sentence of life imprisonment. She is pleading not guilty, with a trial set to take place next February.

Shipp says that at the moment legislation such as the General Data Protection Regulation (GDPR) offers people in the UK more protection regarding sensitive information that tech companies hold about their reproductive health or their search history and social media conversations.

GDPR could be overturned as part of a drive to move away from European data privacy rules in the wake of Brexit,[10] although in reality, many data controllers operate across borders and so will remain subject to the European Union GDPR or other privacy laws.[11]

In 2021, NHS Digital announced plans to pool medical records onto a database and share them with third parties.[12] Although the NHS says that this could save lives,[13] researchers say that questions remain about some of the possible implications.

"In terms of the NHS, I think it's really interesting to ask how protected we are, and how private our data is," says Shipp. "It might be doing a deal with Palantir, which is involved in this new data platform that will contain a huge amount of confidential patient data without very clear guidance on who will have access to it and under what terms. So it's definitely getting more of a grey area."

As a result, Shipp has some advice for anyone looking to engage with tech platforms regarding their reproductive health. "Find an app that is privacy first, as that doesn't store any data other than on your phone," she says. "Other ways of just keeping safe are using fake names or email addresses and avoiding the community and forum aspects of apps, as a lot of them have polls or quizzes but then they treat that as data that they can just scrape."

Competing interests: I have read and understood BMJ policy on declaration of interests and have no relevant interests to declare.

Provenance and peer review: Commissioned; not externally peer reviewed.

1 Sanderford A. Facebook data used to prosecute Nebraska mother, daughter after alleged abortion. *Nebraska Examiner* 2022 Aug 10. https://nebraskaexaminer.com/2022/08/10/facebook-data-used-to-prosecute-nebraska-mother-daughter-after-alleged-abortion

2 Tanne JH. US Supreme Court ends constitutional right to abortion. *BMJ* 2022;377:. doi: 10.1136/bmj.o1575 pmid: 35760421

3 Reed S. Delete Facebook trends after Nebraska cops use messages to prosecute teen for an abortion. *Glamour* 2022 Aug. https://www.glamour.com/story/delete-facebook-messages-prosecute-teen-for-an-abortion

4 Google employees petition bosses for abortion policy changes. https://www.nbc-news.com/tech/tech-news/google-employees-petition-bosses-abortion-policy-changes-rcna43732

5 Flo, the leading female health app, launches 'anonymous mode' to further protect reproductive health information in wake of Roe v. Wade decision. Press release, 30 Jun 2022. https://flo.health/press-center/flo-launches-anonymous-mode

6 Health Information Privacy. HIPAA privacy rule and disclosures of information relating to reproductive health care. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html

7 Holt E. Poland to introduce controversial pregnancy register. *Lancet* 2022;399:. doi: 10.1016/S0140-6736(22)01097-2 pmid: 35717978

8 Kosc W. Outrage over Polish government plan to register each pregnancy. *Politico* 2021 Nov 24. https://www.politico.eu/article/outrage-over-polish-government-plan-to-register-each-pregnancy

9 Seaward T. Woman, 24, in court accused of 'procuring abortion'. *Oxford Mail* April 2022. https://www.oxfordmail.co.uk/news/20083264.woman-24-court-accused-procuring-abortion/

10 Allen F. What is next for GDPR in the UK, is change on the horizon? Kingsley Napley blog, 2 Sep 2021. https://www.kingsleynapley.co.uk/insights/blogs/public-law-blog/what-is-next-for-gdpr-in-the-uk-is-change-on-the-horizon

11 UK government announces extensive post-brexit changes to data privacy laws. https://www.lexology.com/library/detail.aspx?g=ad824063-1e7d-4631-8b12-4a5147aea06b

12 March S. GPs warn over plans to share patient data with third parties in England. *Guardian* 2021 May 30. https://www.theguardian.com/society/2021/may/30/gps-warn-plans-share-patient-data-third-parties-england

13 Chapman M. TREs in the NHS—how health data sharing is saving lives. NHS Digital blog, 13 June 2022. https://digital.nhs.uk/blog/inside-story/2022/tres-in-the-nhs---how-health-data-sharing-is-saving-lives