USER ERROR: THE INTERNET POST-ROE
Sometimes life's most difficult questions get answered there, sometimes we slip and share something vulnerable and are met with open arms, and sometimes we find corners we wish we'd never visited.

On June 24, 2022, the Supreme Court of the United States overturned Roe v. Wade. The decision the court made regarding Dobbs v. Jackson Women’s Health Organization stripped away reproductive freedom from any person who can get pregnant. Our digital spaces were buzzing with activity.

Doctors who provide life-saving care sought urgent counsel on how to support those waiting in their clinics.

People and families in need of reproductive care feared being punished and turned to advocacy and support networks online. Many healthcare providers had to shutter their abortion care, including, in some cases, support for people experiencing pregnancy loss.

Funds were raised in the millions to advance local efforts to protect abortion access where it was vulnerable and find care for those in need.

Within days it became clear that supporting reproductive justice in our current post-Roe reality faced a familiar threat:

**THE CORPORATIONS THAT GOVERN OUR DIGITAL SPACES COLLECT AND STORE DATA THAT LAW ENFORCEMENT CAN USE TO PUNISH THOSE SEEKING REPRODUCTIVE CARE.**

In this report, we'll outline the ways that Google and Meta (formerly Facebook) have aided and abetted organizations and lawmakers police, prosecutors, state attorneys general i.e. Meta and Google

Let’s take a step back to examine the players in this post-Roe environment:
First, let's examine the interests of most Americans. According to Pew Research, the “majority of the U.S. public disapproved of the Supreme Court decision to overturn Roe,” making anti-abortion supporters the minority.

Anti-abortion groups have been running a decades long-project to build a sympathetic Supreme Court and get Roe overturned, but that isn’t the final goal of the project. Anti-abortion groups continue to try and increase their power. A central part of their strategy is to intentionally spread disinformation about abortion that not only prevents people from accessing abortions or comprehensive reproductive healthcare, but also sways them to vote against reproductive freedom.

The anti-abortion faction also leverages law enforcement to prosecute people seeking reproductive healthcare. Law enforcement is historically designed to control marginalized communities and even gives incentives for individuals to turn on their own communities. One example is Texas’s SB8 (Senate Bill 8), a law that not only bans abortion, but creates a bounty system where Texas citizens can sue anyone they suspect being involved in performing an abortion. If the plaintiff wins the lawsuit, they are awarded $10,000.

Enter Big Tech. The biggest of Big Tech—Google and Meta—run ad-driven platforms that make billions of dollars. Despite headlines about decline, in just one quarter (July to September 2022) Google made $69.1 billion and Meta made $27.7 billion for a combined $96.8 billion. You would have to save $10,000 every single day for over 26,000 years to save $97 billion. This business model relies on companies collecting enormous amounts of user data.

But when it comes to answering questions about how they manage abortion-related traffic on their platforms, the companies don’t pick a “side.” Because picking one side means alienating another and that’s not good for their business.

When Big Tech chooses to do nothing, legislators see this as an opening. For example, earlier in 2022, South Carolina lawmakers tried to pass a law banning websites that give people in the state information about how to access abortions.

Meta is not just a social media platform and Google is definitely not just a search engine.

WHAT WE’RE NOW SEEING IS THE CONSEQUENCES OF TECH COMPANIES DODGING ABORTION ISSUES.

This avoidance effectively supports what anti-abortion and law enforcement groups want and leaving the rest of us, the majority, unsafe on the internet: unable to access necessary healthcare information and in jeopardy of legal assault.

BIG TECH MAKES BILLIONS FROM USER DATA

$97 BILLION
Combined revenue for Meta and Google, July to September 2022

YOU WOULD HAVE TO SAVE $10,000 EVERY SINGLE DAY FOR OVER 26,000 YEARS TO SAVE $97 BILLION.

THIS DATA CAN INCLUDE YOUR AGE, LOCATION, RACE, WHO YOU ARE CONNECTED TO, AND INTERESTS BASED ON WHAT YOU INTERACT WITH ONLINE. ALL OF THIS INFORMATION IS GIVEN TO ADVERTISERS, WHO THEN TARGET YOU.
Here's a breakdown of what decisions Meta and Google have made since the Supreme Court decision in 3 areas: disinformation, data privacy, and law enforcement.

**DISINFORMATION**

**META**

Meta's decision to profit from disinformation about “abortion reversal.”

Before Roe v. Wade was overturned, abortion disinformation was rampant on Facebook and Instagram, despite a company policy about banning the promotion of medical misinformation. Before Roe was overturned, safe medication abortion accounted for half of all U.S. abortions. Now, that percentage is likely to increase as clinics close. Disinformation about abortion pills is being spread easily and rapidly. Some of the most dangerous disinformation on Meta's platforms have been focused on “abortion reversal pills,” a procedure that is unlikely to work and is deemed unethical.

NARAL's research team found that in the first quarter of 2022 nearly half of the top-performing posts on Facebook about medication abortion contained disinformation, despite long-confirmed facts about its safety and effectiveness. Posts promoting “abortion reversal pills” spiked in interaction the day of the Supreme Court decision. Meta has made tens of thousands of dollars from ads about abortion reversals by letting anti-abortion groups take advantage of their advertising machine.

**GOOGLE**

Google's decision to promote harmful crisis pregnancy centers.

A quarter of the top 10 Google search results across the country show crisis pregnancy centers (CPCs) when users are searching for abortion clinics near them. CPCs use the pretense of medical authority to give people disinformation about pregnancy and abortion. And all CPCs share the central mission to sway people's medical decisions by any means necessary.

CPCs also run ads on Google, masquerading as legitimate reproductive healthcare providers. Even though Google said they use “does not provide abortions” labels for advertisers that do not in fact provide abortions, the labeling is inconsistent, allowing Google to still collect ad revenue from CPCs on abortion-related searches.

**THE BOTTOM LINE**

Disinformation increases fears and has real health consequences, especially for communities that already face barriers to all reproductive health services. As more people use the internet to look into self-managed abortions or seek reproductive healthcare outside of their state, the more responsibility Meta and Google have to make sure targeted lies are not on their platforms.
### DATA PRIVACY

#### META
**Meta's decision to not encrypt messages**

Although users think direct messages (DMs) are private, they are not. Facebook Messenger and Instagram direct messages are not end-to-end encrypted, leaving its hundreds of millions users’ conversations available to be accessed by anyone—the company, hackers, law enforcement, you name it. Meta announced a rollout of end-to-end encryption in Messenger next year. This news broke days after Meta was exposed handing over access to a teen's chats about her abortion. The company says their announcement and the story are unrelated.

#### GOOGLE
**Google's decision to auto-delete location data**

On July 1, 2022, Google announced it would start auto-deleting abortion clinic location data “soon after” the visit. This is a welcome move but more action is needed. We still don't have specifics on what “soon after” means, for example. And there are more data points that Google collects that can be used against people, including what Google is known for: searches.

### THE BOTTOM LINE

Our data is a valuable commodity and it deserves to be treated as such. From end-to-end encryption to automatic deletion of sensitive information, there are ways for companies to protect our data.

### LAW ENFORCEMENT

#### META
**Meta's decision to hand over messages to police**

News broke in August 2022 after Meta handed over a teenager’s Facebook messages to the police. These messages were exchanges between the teen and her mother regarding the teenager’s abortion care. The messages were used to prosecute both the girl and her mother, who both live in Nebraska where abortion is illegal. Meta released a statement saying the company received “valid legal warrants” from local law enforcement that didn't indicate this was about abortion. But prior to this story and after, Meta has remained largely silent on how it will deal with abortion-related law enforcement requests.

#### GOOGLE
**Google’s decision to hide behind press talking points**

In a blog announcement, the company stated it will push back on “overly broad demands from law enforcement” and “notify people when we comply with government demands, unless we’re prohibited from doing so or lives are at stake.” Google receives thousands of government requests for data a year and its own data shows it produces data for nearly 84% of those requests. There is no public evidence or transparency of Google resisting a warrant. Google’s employees are demanding real action from the company instead of statements and press releases.

### THE BOTTOM LINE

Meta and Google are increasingly becoming the cornerstone of policing. We shouldn’t have to wait and find out what Big Tech companies plan to do with our info when approached by law enforcement. Companies can and should scrutinize warrants to make sure they are not overbroad, alert users when warrants come through, and add this information to their transparency reports.
Tech tries to claim a place on the sidelines, but it is a major player, making decisions for all of us that can increase risk and harm for people seeking reproductive healthcare.

It doesn’t have to be this way. The digital realm can be a place where people find the care and community they need, regardless of their zip code. As a first step, we are demanding that Google and Meta:

1. Protect users seeking reproductive healthcare by stopping the collection and retention of individual location, search data, and messages.

2. Publically address how they will handle law enforcement requests for data, scrutinize warrants to make sure they are not overbroad, and alert users when warrants come through.

3. Remove abortion disinformation in all languages.

WE NEED COLLECTIVE ACTION AGAINST THE COMPANIES THAT MANAGE OUR ONLINE SPACES BECAUSE ULTIMATELY THEY RELY ON US. THE INTERNET SHOULD BE A PLACE WHERE PEOPLE SEEKING HELP AND SUPPORT CAN DO SO WITHOUT FEAR OF BEING TRACKED AND SURVEilled.