



digital defense fund

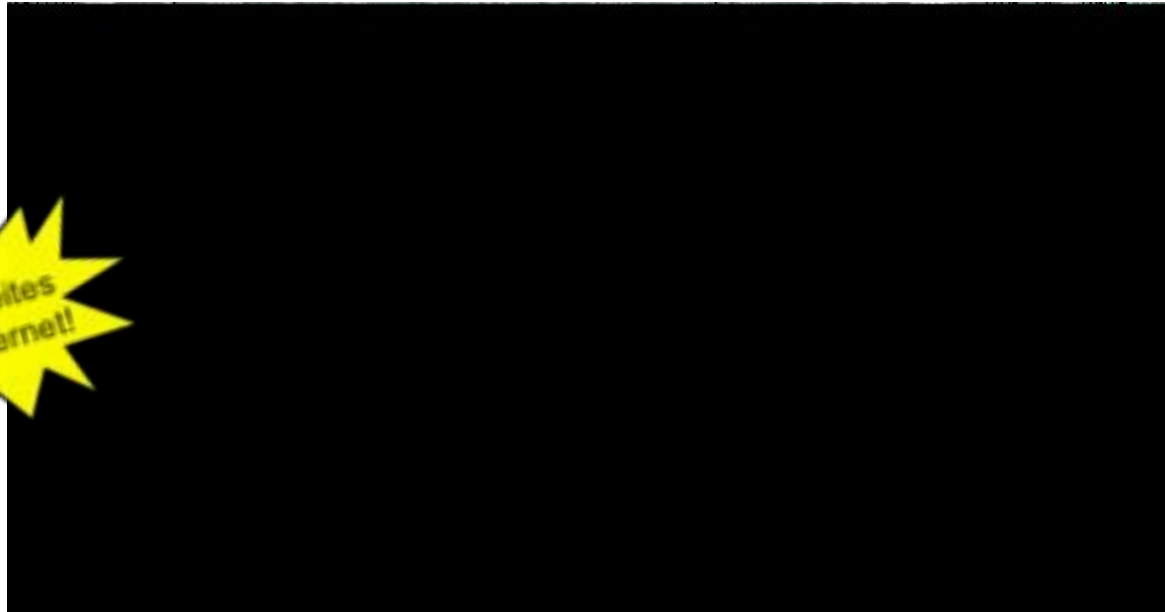
# Periods, Pregnancy, Abortion, and Your Digital Security

Slides prepared by Digital Defense Fund for event hosted by ReproAction  
July 30, 2021

<https://reproaction.org/resource/periods-pregnancy-abortion-digital-security/>

While it may feel private to browse the internet and use your phone to find information about abortion and reproductive health, many watch what we do online and use our phones to track what we do. Large companies – including Google, Facebook, Amazon, your cell phone service provider, your Internet service provider, and apps – keep records of our data and metadata that we create while browsing online.

# The internet is not a cloud...it's cables & computers



Source: [https://www.youtube.com/watch?v=ts7v5dkQs\\_w](https://www.youtube.com/watch?v=ts7v5dkQs_w)

# Lots of actors want our information!



Image credit: [Electronic Frontier Foundation](https://www.eff.org/)



# The responsibility of blocking those actors is shared between platforms and users

## What they control:


- Security of our data in transit
- Security of our data storage
- What and how they share our data with other services, or entities

## What we control:

- Our login
- What and how we share with services
- What and how we share with other users
- Our devices we use to access those platforms



# Data is used for targeted advertising...

 **Karla Ray** ✓  
@KRayWFTV

Facebook ads are there to remind women that from age 27-37, you ought to be having kids.

**About This Facebook Ad** ✕

**Why Am I Seeing This Ad?** Options ▾

One reason you're seeing this ad is that **Little Nomad Play Mats** wants to reach people who have visited their website or used one of their apps. This is based on customer information provided by Little Nomad Play Mats.

There may be other reasons you're seeing this ad, including that Little Nomad Play Mats wants to reach **women ages 27 to 37 who live or were recently in the United States**. This is information based on your Facebook profile and where you've connected to the internet.

⚙️ Manage Your Ad Preferences

**Tell Us What You Think**

Was this explanation useful? Yes No

📘 Learn more about Facebook Ads

2:26 PM · Mar 1, 2017 · Twitter Web Client

 **Coding Rights** ...

Why are you seeing this green mom holding a baby vampire? Because Facebook classified you as a "green mom" that likes "horror movies". Is that you?



<https://www.thecut.com> › 2019/09 › period-tracking-apps... ⋮

## Period-Tracking Apps Are Telling Facebook When You Have ...

Sep 9, 2019 — ... extremely personal detail, including when the user last had sex. ... Is Your Period-Tracking App Telling Facebook When You Last Had Sex?

Learn more about periods, pregnancy, abortion, and the data economy:

### **Privacy International Reports:**

- [Investigation into data sharing by menstruation apps](#)
- [Investigation into anti-abortion CPC privacy violations](#)
- [Documentation of data exploitation in reproductive health](#)

### **Coding Rights [Chupadatos](#) (Datasucker):**

- [Gendered targeted ads](#)
- [Menstruation apps making money off your data](#)
- [Pregnancy is a jackpot for the data economy](#)



...and for reproductive coercion and criminalization.

FASTCOMPANY

02-26-20

## How an online search for abortion pills landed this woman in jail

The internet is an incredible tool to increase access to medication abortion. But prosecutors are using searches, browsing history, and text messages to punish some women for ending their pregnancies.

INVESTIGATIONS ABORTION

### Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits

May 25, 2016, 6:52pm Sharona Coutts





Privacy International investigation into data usage by anti-abortion organizations found that

“intrusive data collection software and digital marketing systems are being developed and promulgated around the world by powerful and politically connected US-based anti-abortion organisations.”

<https://www.privacyinternational.org/long-read/3669/documentation-data-exploitation-sexual-and-reproductive-rights>



Learn more about how digital evidence has been and will be used to criminalize pregnant people:

[Surveilling the Digital Abortion Diary](#) by Cynthia Conti-Cook

Learn more about how police collect digital evidence:

[Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones](#) by Upturn



# Who can be affected?

- Individuals researching their abortion options online
- Individuals seeking abortion support in online forums
- Those who have pregnancies they wish to keep private from certain people
- Those who are accused of crimes when seeking medical treatment for a pregnancy outcome

What are some other circumstances where someone might be worried about collection of data?



# Disclosure of pregnancy or abortion-related data can have consequences

## Personal:

- Revealing a pregnancy to a partner or parent
- Targeting from advertisers after a miscarriage
- Targeting by anti-choice services and facilities

## Legal:

- Criminalization of pregnancy
- Criminalization of abortion and miscarriage experiences

So...what can we do?



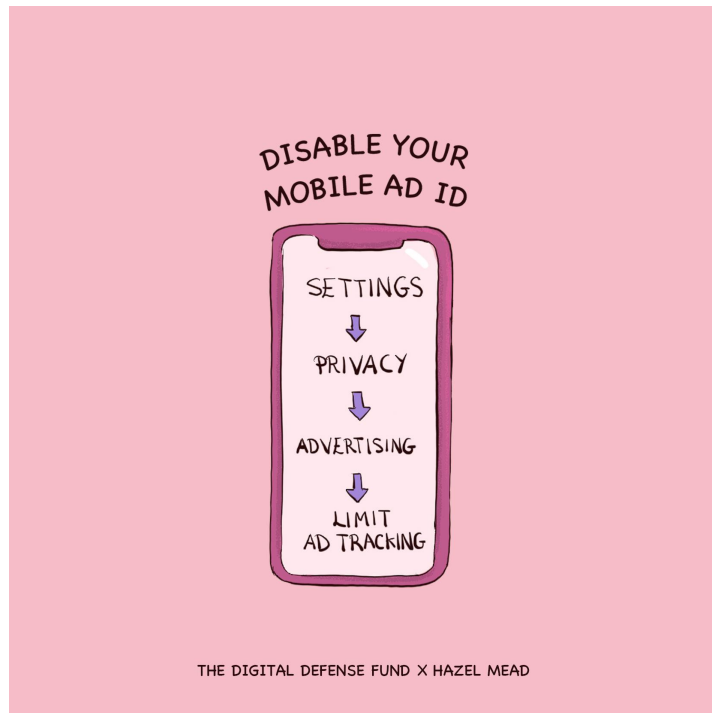
# Take control of what affects you!



# Disable your ad ID on your phone, social media, and Google

*Helps protect against: ads related to pregnancy/abortion; limits data shared across platforms*

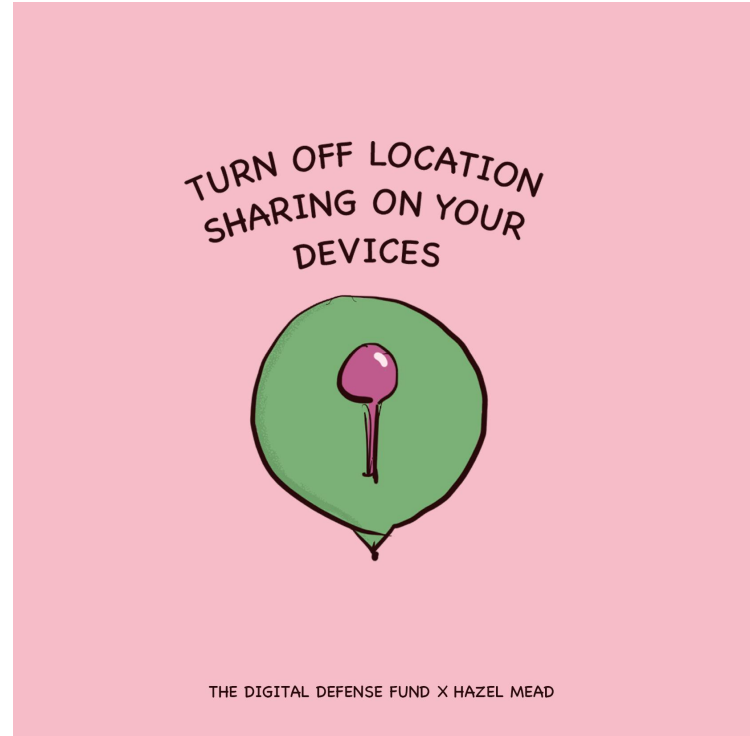
- Disabling your ad ID usually triggers a warning about getting “less personalized ads” - good! That’s what we want!
- These links contain instructions for disabling your personalized ad ID on [your phone, Facebook and Instagram](#), and [Google accounts](#), or search “turn off ad ID on [platform]”



# Limit the location data you share

*Helps protect against: ads related to pregnancy/abortion; geofenced ads or warrants; nonconsensual tracking*

- Law enforcement doesn't have to collect this data – they can just buy it (for example, the US military bought location data from a Muslim prayer app)
- [Turn off location sharing](#) for your whole device, or turn it off app by app if you use apps that legitimately require your location
- You can type in your address in rideshare apps and Google maps instead of sharing your location!





# Protect your phone with a strong PIN

*Helps protect against: someone getting unauthorized access to your phone*

- All iPhones and most Androids are automatically encrypted when you add a PIN. Double check this in your settings.
- Turn on an alphanumeric passcode to make your PIN even stronger!
- If someone demands access to your phone, you may decide it is safer to give them the PIN than to resist. Combine this with other tactics to limit data on your phone.



# Browse in an incognito window

*Helps protect against: unauthorized access to your browsing history*

- Use an incognito or private browser window, which automatically deletes your browsing history. You can use a private window in [Safari](#), [Chrome](#), and [Firefox](#).
- Manually clear your browsing history in [Safari](#), [Chrome](#), or [Firefox](#). You can delete the whole history or in Chrome and Firefox, you can choose specific sites to delete.



# Use platforms that protect your privacy

*Helps protect against: ads related to pregnancy/abortion; third party trackers; unauthorized access to search history*

- Search histories have been used to criminalize people for pregnancy outcomes
- DuckDuckGo is a privacy-respecting search engine
- DuckDuckGo doesn't store your search history or share it with advertisers
- Browsers will allow you to set DuckDuckGo as your default search engine instead of Google



# Use platforms that protect your privacy

*Helps protect against: ads related to pregnancy/abortion; third party trackers; unauthorized access to browser history*

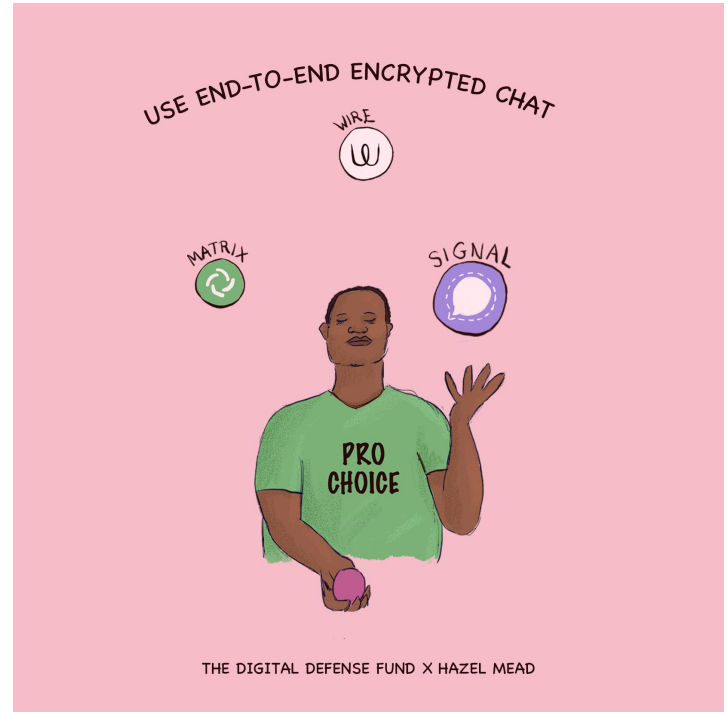
- Firefox automatically protects against third party trackers
- Firefox Focus (app for your phone) automatically clears your browser history when you close the app
- Other browsers may work better with apps like Zoom, so it's okay to pick and choose which apps you use for what!



# Use end-to-end encrypted chat apps

*Helps protect against: someone else seeing private messages; limits data your phone company stores about you*

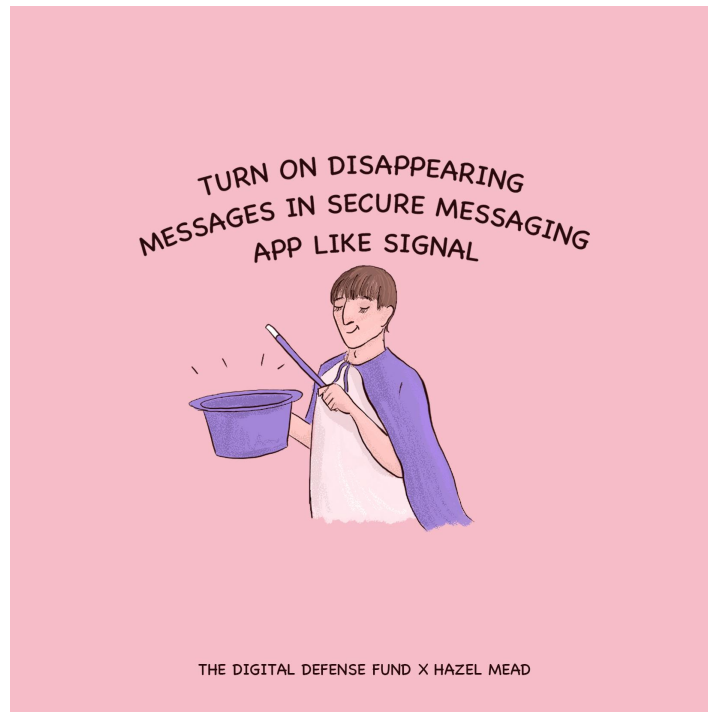
- Your phone company has copies of all your SMS texts, plus metadata about who you text and when
- Open source, end-to-end encrypted apps like Signal are highly recommended for all your chatting!
- Choose privacy-focused apps like Signal over advertising-focused apps like WhatsApp



# Bonus: turn on disappearing messages in Signal!

*Helps protect against: someone with access to your phone seeing your past messages*

- Phones can be confiscated at border crossings or during an arrest, and the pressure to unlock your phone can be intense
- Disappearing messages prevent someone with access to your phone from seeing your past messages



# Use Tor or a no-logs VPN

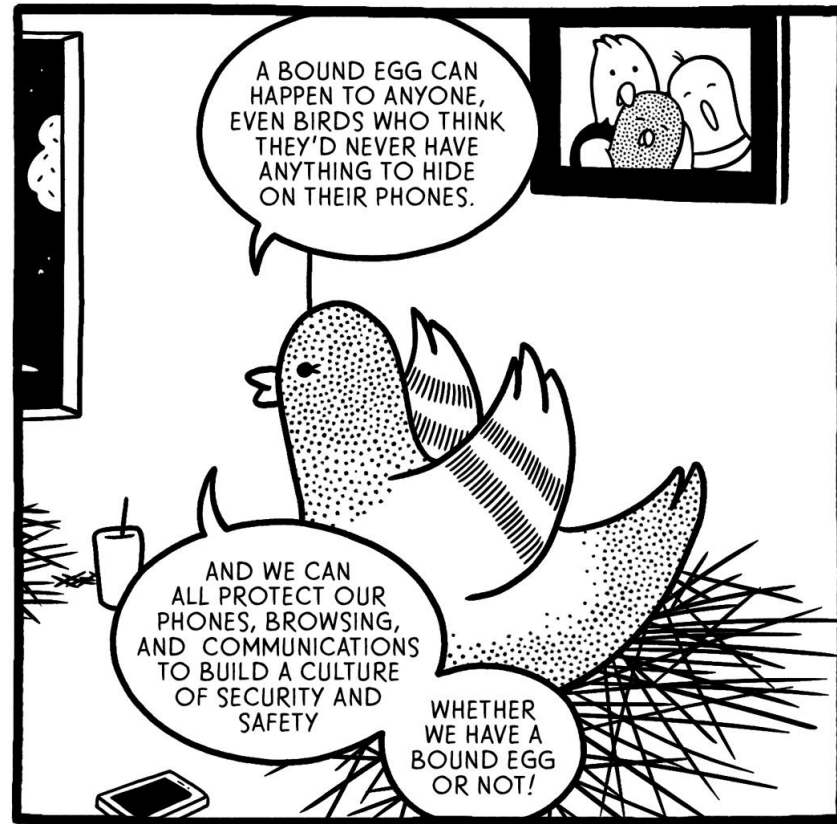
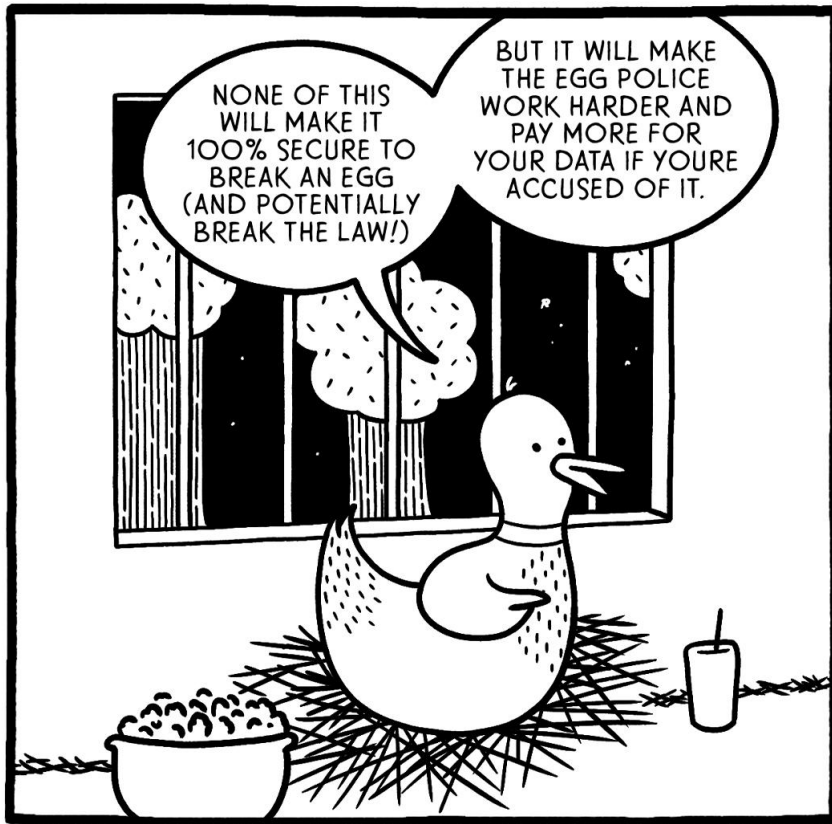
*Helps protect against: limits data that Big Tech and your phone company and Internet Service Provider have about you*

- Using a VPN or Tor transfers your data - and your trust- from your carrier/ISP to the VPN provider (choose a trustworthy, no-logs VPN) or Tor (a trustworthy, open source, private browser)
- VPNs & Tor also hide your IP address
- [Download Tor](#) for free
- Pay a few dollars a month for a [no-logs VPN](#)









# Resources:

The illustrations from this presentation are from Digital Defense Fund's resources:

- [Guide to Abortion and Pregnancy Privacy](#)
- [Pigeon Zine 5: Know Your Cyber Civil Rights](#)

See these and additional resources at our website:

- [digitaldefensefund.org/learn](https://digitaldefensefund.org/learn)



# Additional resources:

## Legal Resources:

[Repro Legal Helpline](#)

[Repo Legal Defense Fund](#)

## Legal Analysis:

[Roe's Unfinished Promise & 2019](#)

[Update](#)

[Surveilling the Digital Abortion Diary](#)

## On Surveillance Technology:

[Upturn, Mass Extraction](#)

[Media Justice, Defend Our Movements](#)

[Just Futures Law, Take Back Tech:](#)

[How to Expose and Fight Surveillance Tech in Your City](#)

[hacking//hustling, Posting into the Void](#)

[EFF's Atlas of Surveillance](#)

[Mijente's Take Back Tech Guide & #NoTechforICE](#)

