digital defense fund

Online Privacy: Controlling Your Data

Last updated 8/24/22

Take care of yourself!

We know digital security can be a scary topic, especially if you’ve faced online harassment, identity theft, or other online attacks before.

We’re here to support you.

Feel free to take a break and remember to drink water, have a snack, and step away if you need to take care of any needs!

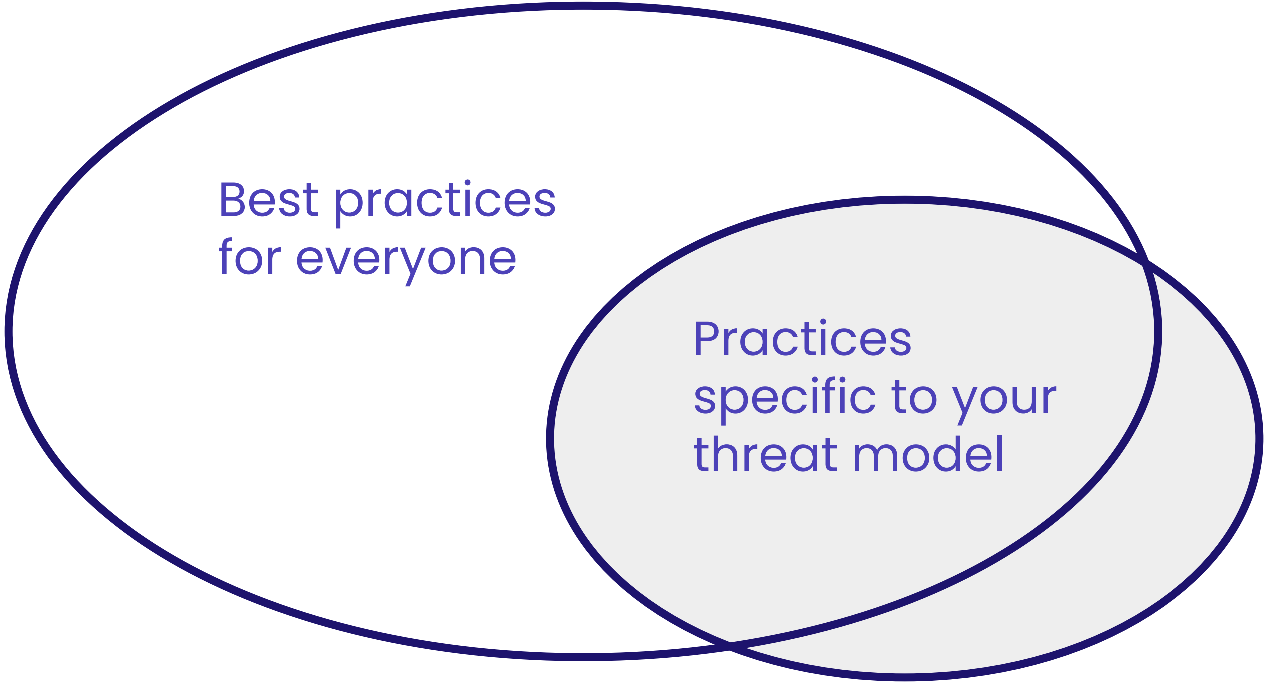
Overview of Common Threats: Privacy & Harassment

Security vs. Privacy

Privacy limits the amount of information about you that people can learn.

Security prevents unauthorized access to your accounts/events.

Threat Modeling: Online Privacy & Doxxing



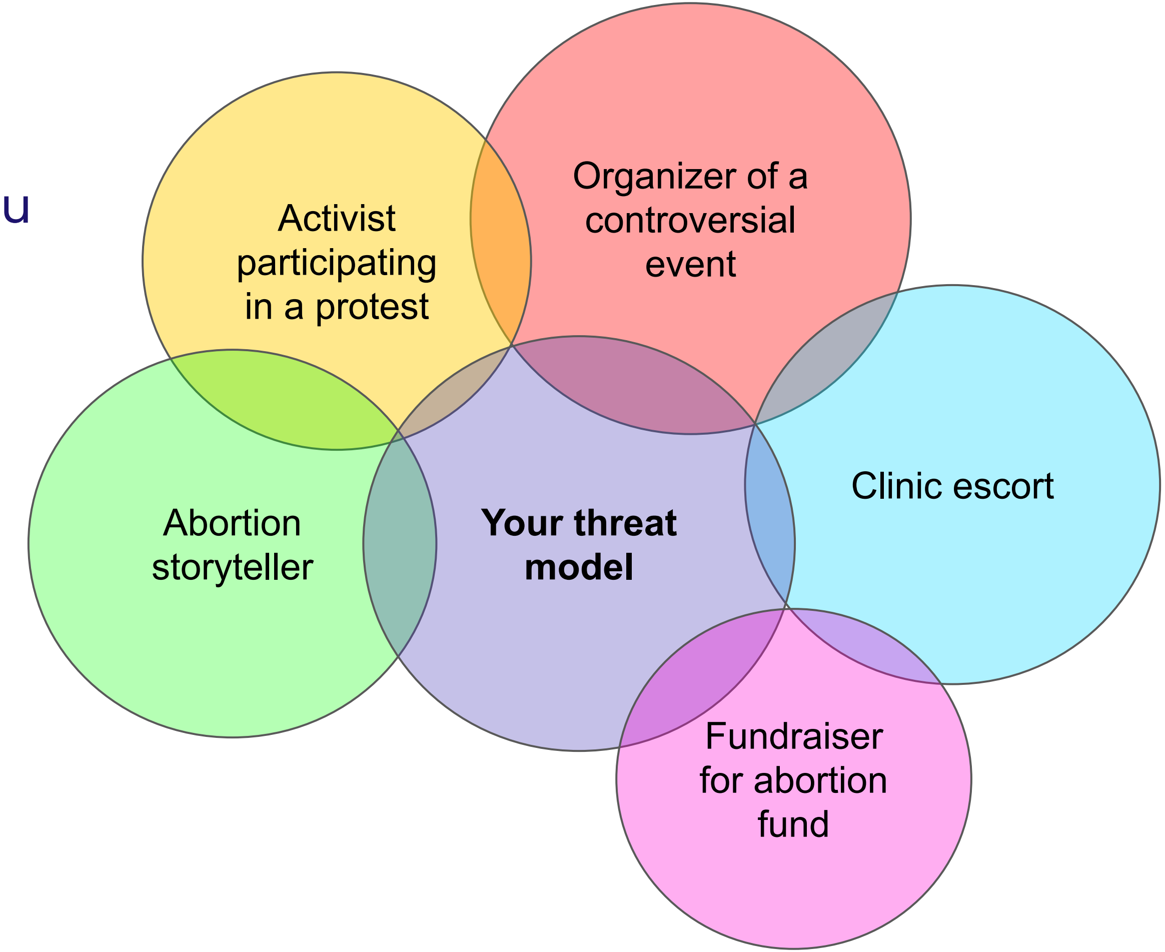
Best practices for everyone

Practices specific to your threat model

Context is key!

What type of work are you doing?

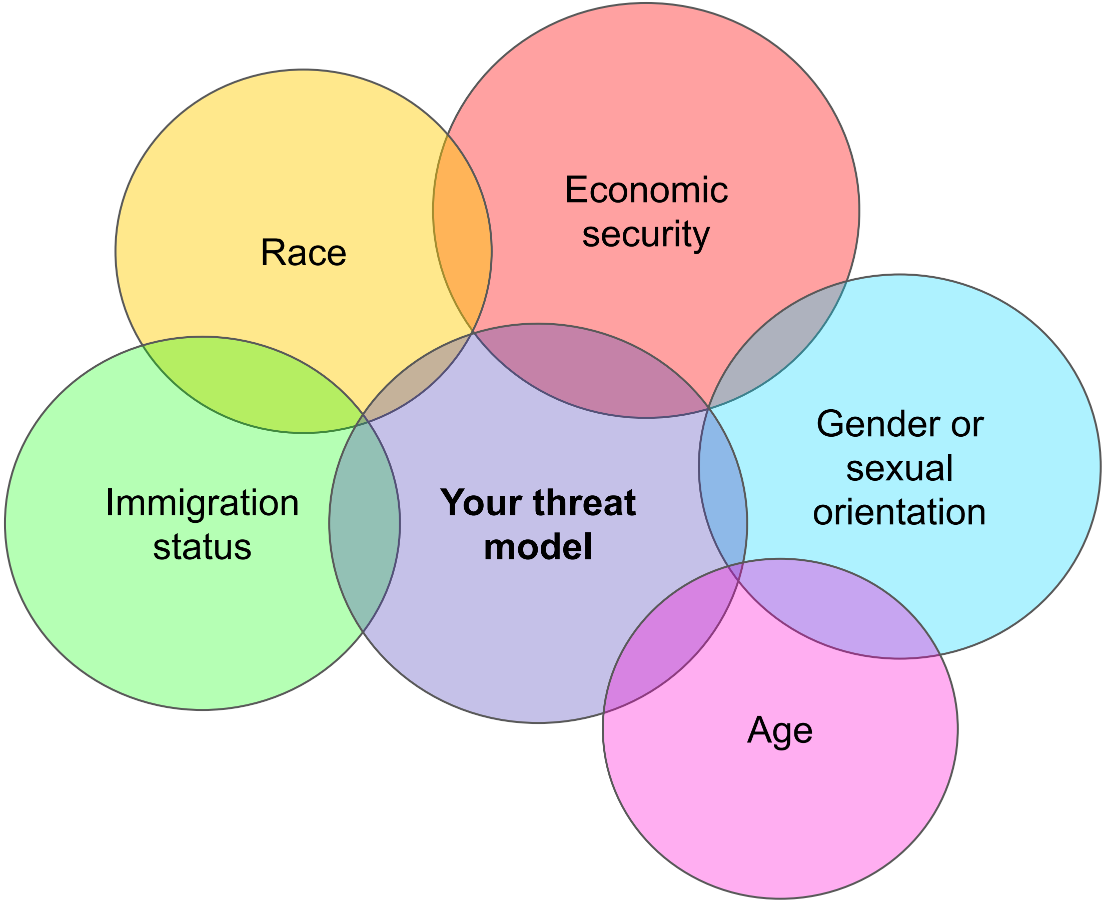
This affects the type of threat you'll face.


Activist participating in a protest
Organizer of a controversial event
Abortion storyteller
Your threat model
Clinic escort
Fundraiser for abortion fund

Context is key!

What about your identity affects how you move through the world?

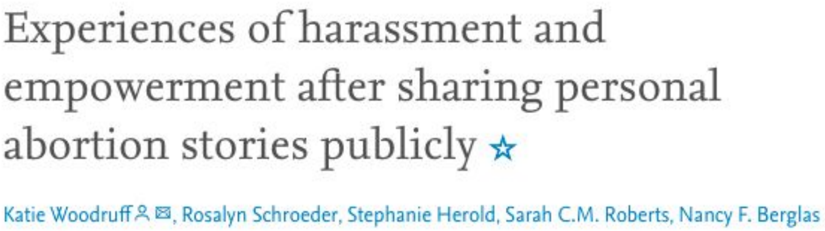
This can affect how severe impact of a threat will be.



Threat modeling helps us ground our fears in reality.

The best way to predict what can happen is by looking at what has happened in the past.

Example: data from abortion storytellers



Experiences of harassment and empowerment after sharing personal abortion stories publicly ☆

Katie Woodruff, Rosalyn Schroeder, Stephanie Herold, Sarah C.M. Roberts, Nancy F. Berglas

https://www.sciencedirect.com/science/article/pii/S2590151620300046

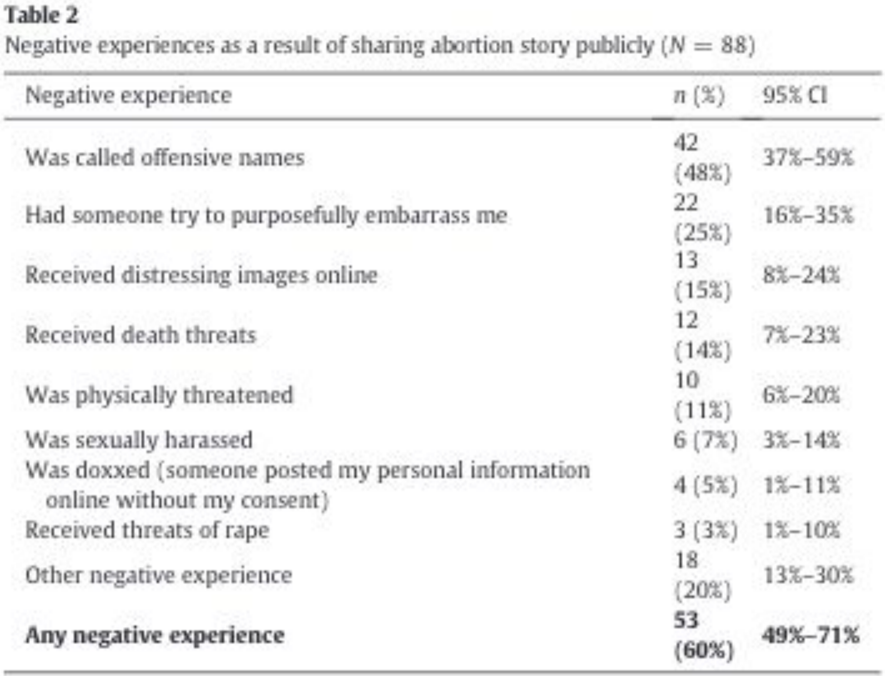
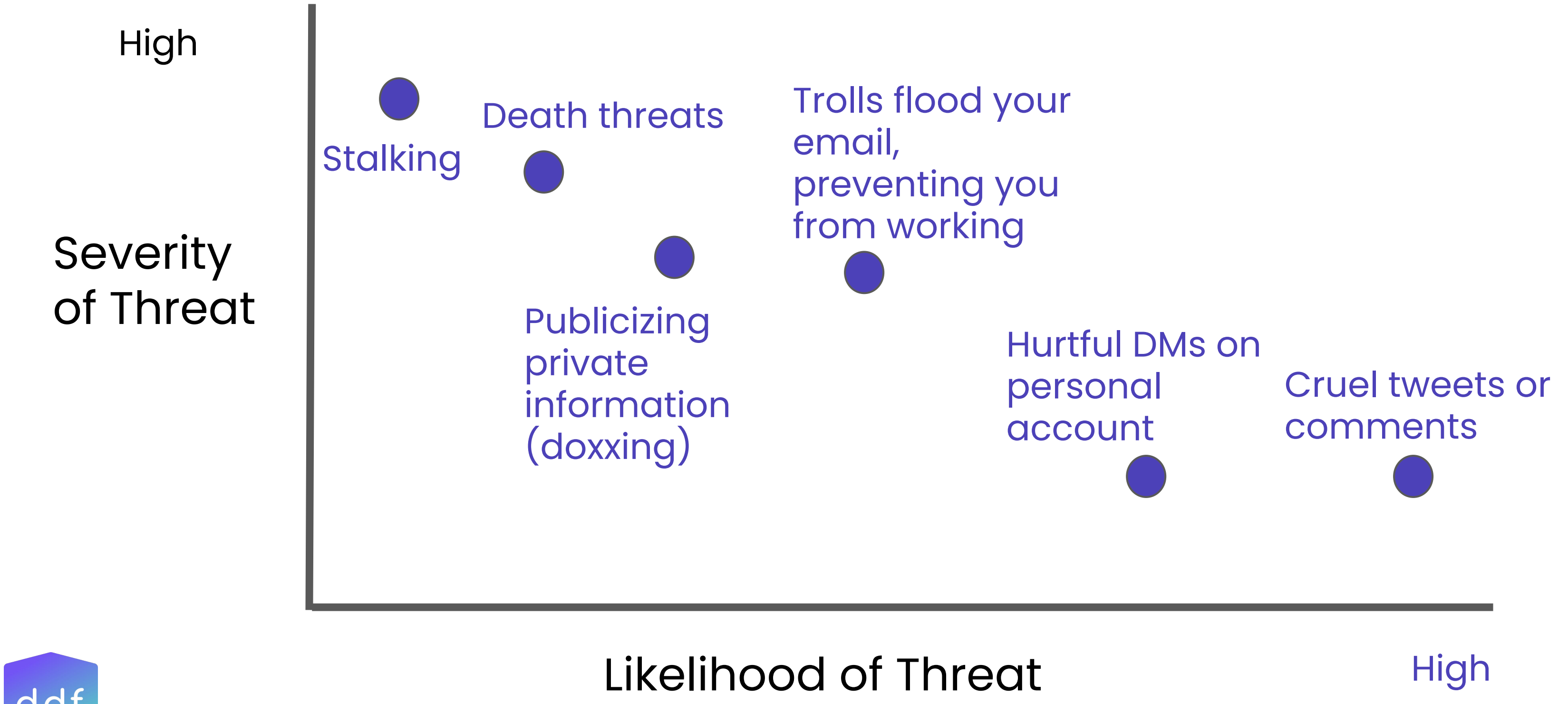


Table 2
Negative experiences as a result of sharing abortion story publicly ($N = 88$)

Negative experience	*n* (%)	95% CI
Was called offensive names	42 (48%)	37%–59%
Had someone try to purposefully embarrass me	22 (25%)	16%–35%
Received distressing images online	13 (15%)	8%–24%
Received death threats	12 (14%)	7%–23%
Was physically threatened	10 (11%)	6%–20%
Was sexually harassed	6 (7%)	3%–14%
Was doxxed (someone posted my personal information online without my consent)	4 (5%)	1%–11%
Received threats of rape	3 (3%)	1%–10%
Other negative experience	18 (20%)	13%–30%
Any negative experience	**53 (60%)**	**49%–71%**

Threat Modeling: Online Harassment



Paths of Escalation

- Taking a threat from one level to the next is called escalation
- Note that as the severity of a threat increases, its likelihood usually decreases

Common escalation paths

Common “escalation paths” that attackers can follow:

1. Get an entire group to start harassing you too
2. Taking attack cross-platform
3. Find your password on a breach list, and attempt to use it
4. Find your home address on a people finder site
5. Find other information about you from social media

Paths of Escalation

- Taking a threat from one level to the next is called escalation
- Note that as the severity of a threat increases, its likelihood usually decreases
- **Our best defense is making escalation more difficult**

Know your doxxing risk: Search yourself!

Why do we search ourselves?

- See what an attacker could find when they start targeting you
- Start making a list of things to remove from your search results
- Be aware of information that can’t be removed

How do data aggregator websites get my address?

- Government records (like property tax records)
- Bought it from websites, apps, and stores (magazine subscriptions, rewards cards, credit cards, travel companies…)
- Scraped it from other people search websites

Think like an attacker: Can you find your private personal info on Google?

- Open an incognito window
- Google “[your name]”
- Google “[your name] + phone number”

You’ve gone incognito.

Beyond Google: What information about you might be public record?

- Home ownership/property records are public.
  - We recommend that you search the local property record/taxes databases so you know what information is out there!
- Licensing records may be public.
  - Are you a lawyer, social worker, nurse, or other professional with licensure requirements?
  - Did you have to submit an address for your licensure documentation? Search your state's database to see what is available about you.
- Website registration records are public.
  - If you have ever purchased a domain, check whether it is registered privately here: https://lookup.icann.org/en

Beyond Google: What information about you might be public record?

- Some non-profit and business filings are public.
    - Are you one of the principal or registered agents with the Secretary of State or the IRS? Look up the relevant filing so you can know what is public there.
        - IRS: https://apps.irs.gov/app/eos/allSearch
        - State: llcuniversity.com/50-secretary-of-state-sos-business-entity-search
- Voter registration records
    - Availability of voter registration records varies by state; see details for your state here: https://www.ncsl.org/research/elections-and-campaigns/access-to-and-use-of-voter-registration-lists.aspx

Solutions: Keeping personal data private

Solutions: Keeping personal data private

Our goal is to make things harder for harassers!

We can’t remove all information, especially public records, so our goal is to make it harder for harassers to find your information.

Proactive privacy protections

Proactive address protection:

- Start compartmentalizing as early as possible and get an address to use for your abortion related work and licensures. Options include:
  - **PO Box:** USPS mailbox, usually cheapest
  - **Commercial Mail Receiving Agency box:** offered by UPS Store or another private company; more expensive, but gives you a street address you can use on official paperwork

Proactive address protection:

- Some people can use address confidentiality programs to get an address for your drivers license & voter registration
- Many states have Address Confidentiality Programs or laws allowing certain people (usually victims of stalking) to have addresses removed from voter lists and other public records
- These laws and who can qualify vary drastically from state to state
  - In California, abortion providers/reproductive healthcare professionals are included!!!
- You can learn more about who can qualify in your state here: Security Positive's Guide to ACP

Proactive phone number protection:

- Get a VOIP number to use publicly. This could be a free Google Voice number or a paid VOIP service like Twilio, Grasshopper, or MySudo.
- Contact your phone company, and ensure they require a password or pin to complete porting requests.
  - This helps prevent someone from stealing your phone number by pretending to be you (an attack called "SIM swapping").
  - VOIP numbers are protected from SIM swapping since they aren't connected to a SIM card and have a more complicated porting process. If you are concerned about SIM swapping, another option is to port your phone number to a VOIP service.

Start Giving Out Fake Information

- When registering or creating a new account, you can often give fake information!
- On consumer websites, you will not get in trouble for giving a fake name, address, or phone number!
    - Try ordering a magazine to your house in a different name. Do you start to get advertisements in that name?
- “Your safety is more of a priority than their consumer data.”

Read the full guide here: https://hackblossom.org/domestic-violence/threats/location.html

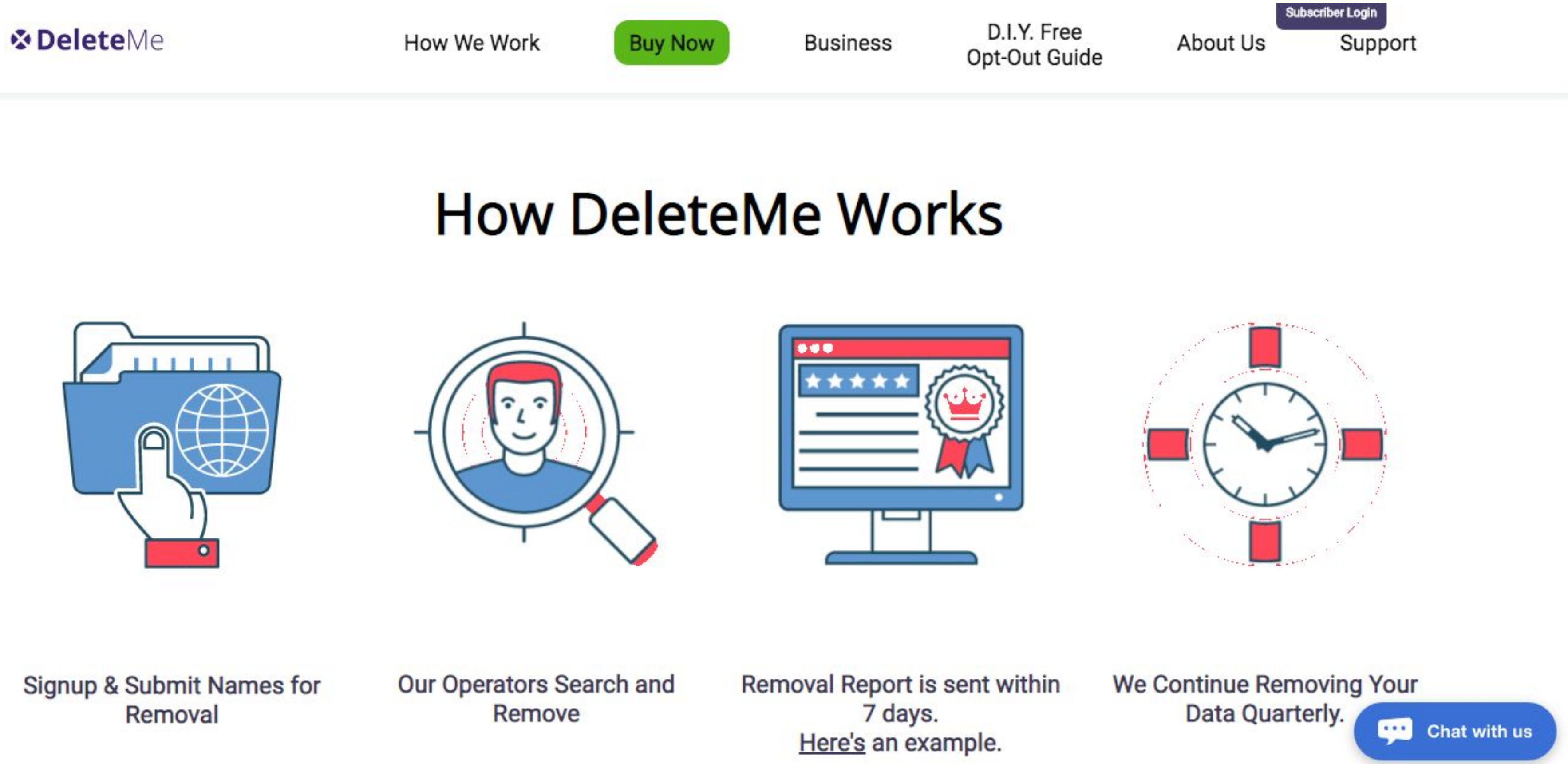
Data aggregator removals

Make it harder to find your address & family members:

- Remove yourself from data aggregator sites
    - These are the sites like Spokeo, Whitepages, etc. that display your name, age, address, phone number, and family members
- For instructions on removing yourself from data aggregator sites, we recommend these guides:
    - Michael Bazzell's Extreme Privacy Opt Out Workbook
    - Yael Grauer's Big Ass Data Broker Opt Out List
    - Abine's https://www.abine.com/optouts.php

Using a paid service to automate removal

- DeleteMe and Kanary are paid services that submit removal requests to data aggregator sites for you
- Costs range from $100-$150/year



How DeleteMe Works

Signup & Submit Names for Removal

Our Operators Search and Remove

Removal Report is sent within 7 days.
Here's an example.

We Continue Removing Your Data Quarterly.

Remember: interrupt escalation!

Even if your address is public record because you ex: bought a home in your name, it’s still worth removing yourself from data aggregator sites.

If someone has to search multiple county tax record databases to find you, that’s a higher bar than just searching Google!

Some attackers will give up if they can’t find your address when they google you. That’s a win!!

Being 100% private is very challenging.

Because harassment isn’t our fault, that means that no matter how hard we try to prevent it, it can still happen.

Making things harder for harassers does lower the likelihood & potential impact of their attacks!

Want to learn more about extreme privacy techniques?

Privacy, Security, & OSINT Show: Podcast by Michael Bazzell

Extreme Privacy: What it Takes to Disappear: Book by Michael Bazzell

Pros: Really thorough podcast & materials about privacy. He's a leading expert on the topic.

Warning: Super dense, technical, and extreme tactics - your threat model may not require such extensive work. He does not approach the topic with an intersectional approach or from diverse viewpoints.

Curate your search results

What bios, press, or other personal/ professional results show up?

Do any of your work or volunteer profiles show up in your search results?

- Bios?
- Photos?
- Direct contact emails?

Consider what you want to be revealed in these public profiles.

What do you want to show up when you're Googled?

- Professional social media accounts?
- Quotes from media appearances?
- By putting content out there, you can make sure the content you want to show up shows up first.

📝 Follow-up:

Search yourself again and sort the results into things you can have removed, things you can update (ex: licensure address), and things you can’t.

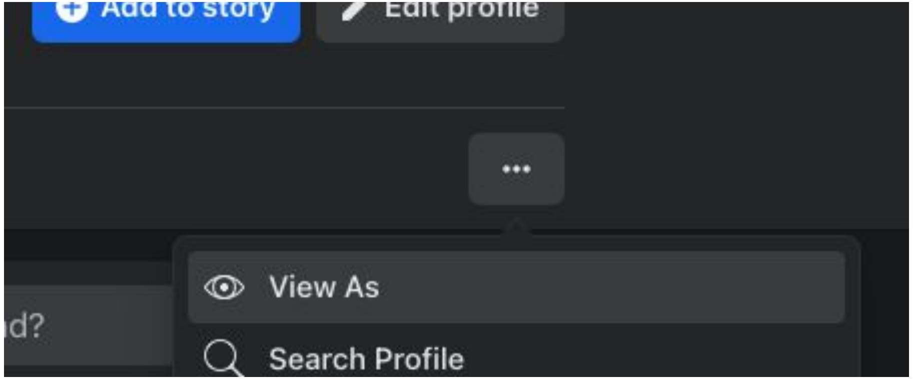
Remove the things you can remove, update what you can, and create a safety plan to manage the risks of the items you can’t remove.

It’s great to learn from different perspectives - check out the resource links at the end of this slide deck!

Knowing your risks:
Look at your social media as someone else!

Look at your social media as someone else.

- Facebook makes this really easy, so we'll start with Facebook if you have a Facebook account!
- Go to your Facebook profile on our laptop and click the three dots at the far right of the page.
- Click "View as"
- Public content will show!



Solutions: Social media privacy

Make your personal social media accounts as private as possible.

If you haven’t already, **create a separation** between your professional social media accounts and your personal social media accounts.

If you use a personal account for both personal and professional activities, consider making a separate personal account (or communicating with friends & loved ones outside of social media!).

Proactive social media privacy

- Familiarize yourself with the privacy settings of your social media accounts
- Consider which accounts you'd like to be public and which accounts you'd like to be private
- Compartmentalize: what will you never share on public accounts? (Ex: photo of your home, photos of your children, etc.)

Pay attention to what is public by default

- Profile photos are public on Facebook, Instagram, WhatsApp, Signal, etc.
- Username links (ex: facebook.com/username) are public
- Consider using a non-face photo as your profile photo for these accounts where a profile photo can be found by people who aren’t connected to you.
- Think broadly: accounts on sites like Etsy, Yelp or other review sites, Goodreads, Reddit, and other sites not traditionally considered “social media” can reveal a lot about your tastes and habits.

Did personal social media accounts show up in your Google search of yourself?

- Make sure your personal social media accounts aren’t findable from Google
  - Almost every social platform has a way to hide your profile from search results.
- If you have professional social media: you may want to consider making sure your professional social media accounts *are* discoverable through Google searches, so that result pops up high on the results page.

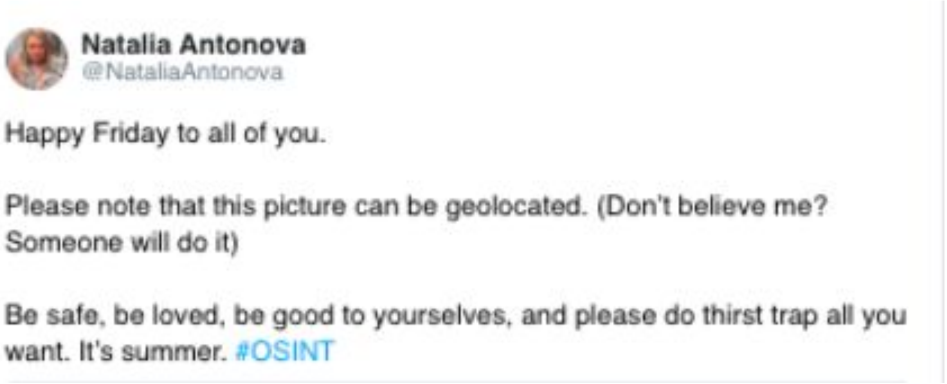
Were any of your locations visible?

- Be mindful and careful with location sharing when you share posts
  - Could someone identify part of your routine (i.e. a coffee shop you frequent)?
  - Could someone identify where you live?
    - Your neighborhood?
- Consider saving photos to post later
  - Once you’re home from vacation
  - Once you’ve left the event

Did you see an option to send yourself a message?

- Limit who can contact you on your personal social media
  - Consider only allowing friends or connections to send you messages

Be aware of what photos can reveal:



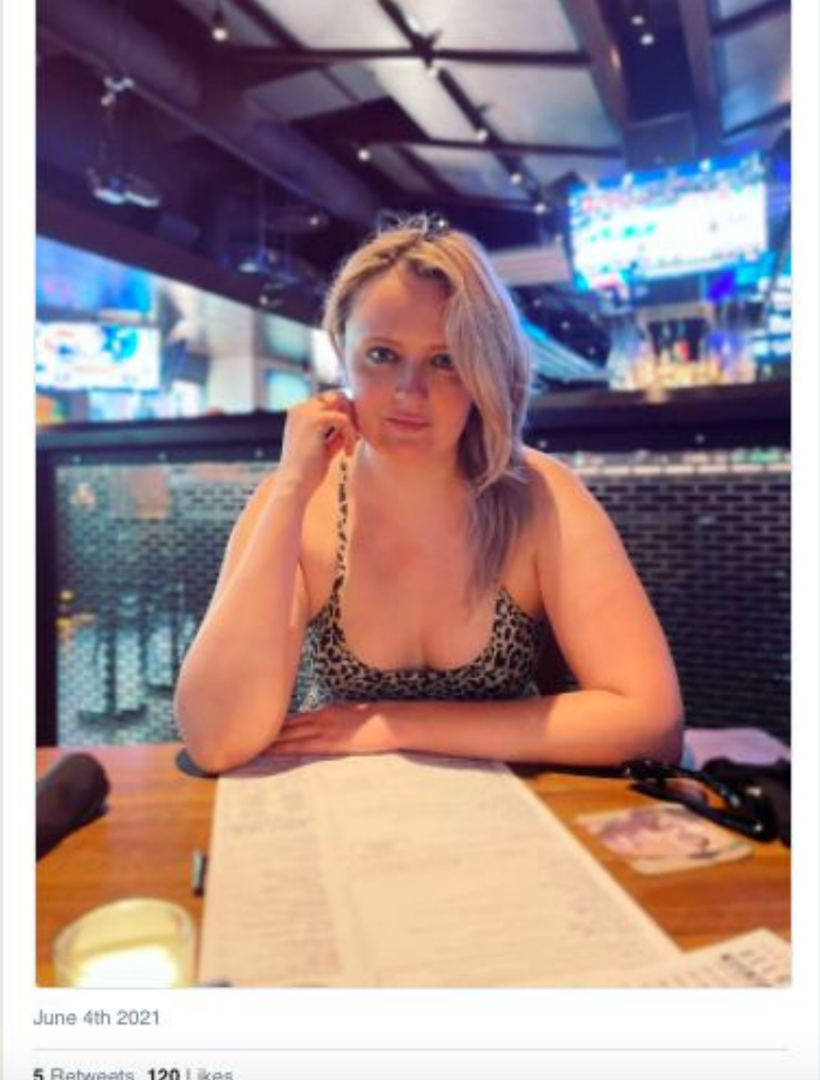
Natalia Antonova
@NataliaAntonova

Happy Friday to all of you.

Please note that this picture can be geolocated. (Don't believe me? Someone will do it)

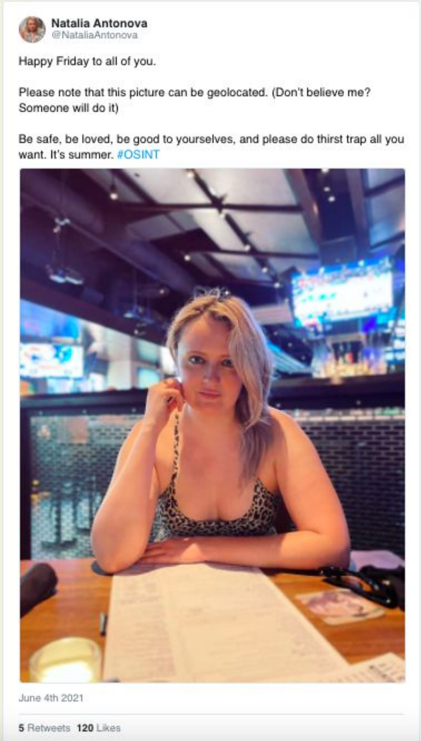
Be safe, be loved, be good to yourselves, and please do thirst trap all you want. It's summer. #OSINT

https://nataliaantonova.substack.com/p/i-asked-for-my-restaurant-thirst



June 4th 2021

5 Retweets 120 Likes



Natalia Antonova
@NataliaAntonova

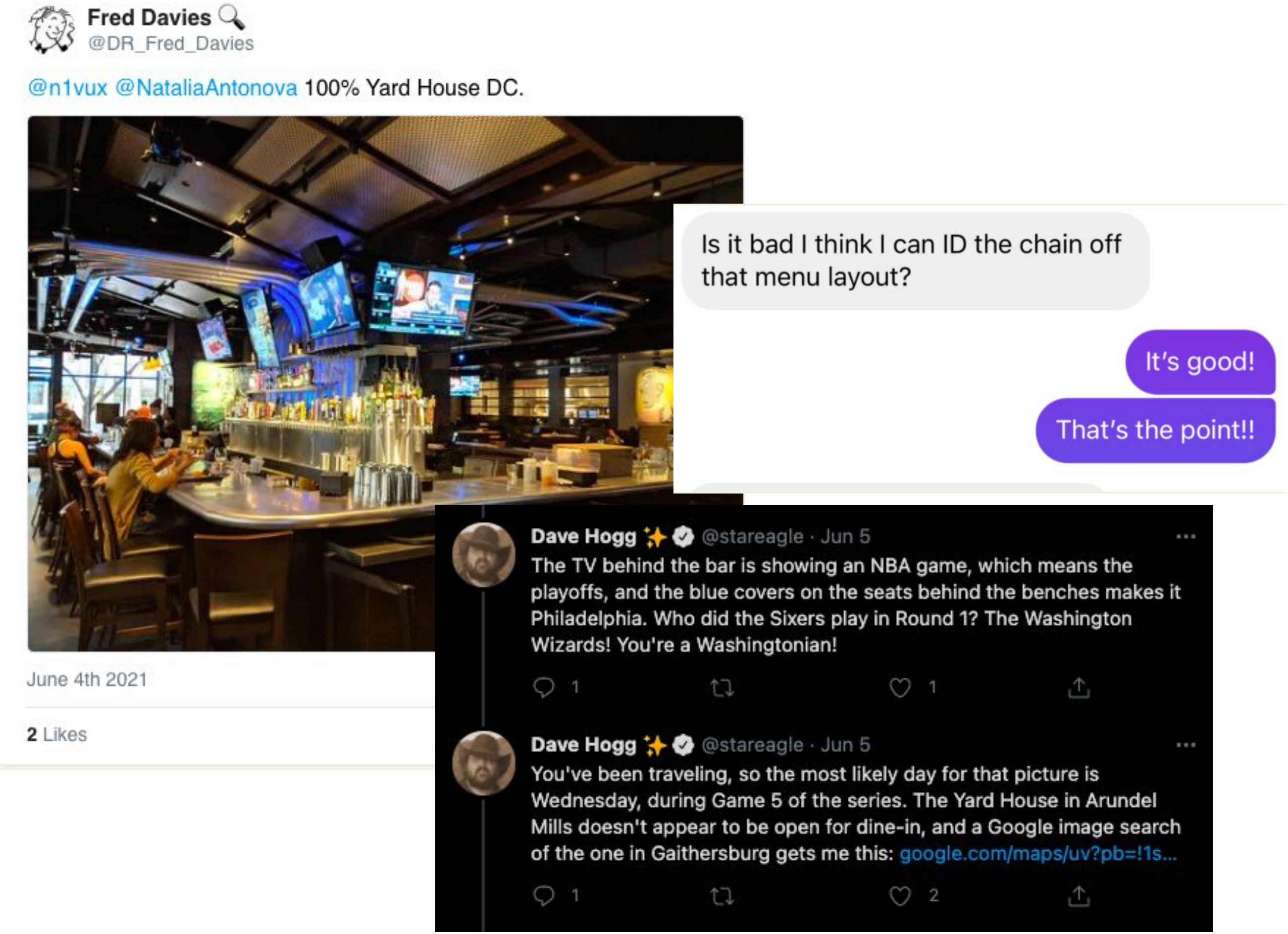
Happy Friday to all of you.

Please note that this picture can be geolocated. (Don't believe me? Someone will do it)

Be safe, be loved, be good to yourselves, and please do thirst trap all you want. It's summer. #OSINT

June 4th 2021

5 Retweets 120 Likes



Fred Davies 🔍
@DR_Fred_Davies

@n1vux @NataliaAntonova 100% Yard House DC.

June 4th 2021

2 Likes

Is it bad I think I can ID the chain off that menu layout?

It's good!

That's the point!!

Dave Hogg ✨ @stareagle · Jun 5
The TV behind the bar is showing an NBA game, which means the playoffs, and the blue covers on the seats behind the benches makes it Philadelphia. Who did the Sixers play in Round 1? The Washington Wizards! You're a Washingtonian!

Dave Hogg ✨ @stareagle · Jun 5
You've been traveling, so the most likely day for that picture is Wednesday, during Game 5 of the series. The Yard House in Arundel Mills doesn't appear to be open for dine-in, and a Google image search of the one in Gaithersburg gets me this: google.com/maps/uv?pb=!1s...

https://nataliaantonova.substack.com/p/i-asked-for-my-restaurant-thirst

You don’t have to delete social media!

In fact, claiming accounts on all the social media sites can help you prevent or take action against impersonation!

Key takeaway:

Be mindful in your use of social media, and familiarize yourself with the privacy settings available.

Resources

- PEN's Online Harassment Field Manual for Journalists
- International Press Institute Protocols for Newsrooms: Responding to Harassment & interactive protocol tool (useful for organizational responses to harassment)
- Speak Up & Stay Safe(r): A Guide to Protecting Yourself From Online Harassment
- A DIY Guide to Feminist Cybersecurity
- Big Ass Data Broker Opt-Out List
- Surveillance Self-Defense Guide
- OnlineSOS