Oregon Department of Justice's
CIVIL RIGHTS UNIT

ANTI-DOXING SAFETY GUIDE

Doxing: Publicly publishing or sharing personal, private, or identifying information about another individual with malicious intent. Often such publishing occurs on the internet, and the intent is to place the other person in fear, or otherwise intimidate, silence, stalk, harass, or threaten the person, or to encourage another person to do so.

PROTECTIONS AGAINST DOXING FOR GOVERNMENT EMPLOYEES

- ☐ Your work and work-related emails and texts may be subject to public records request laws.
- ☐ Do not email/text something that you would not be proud to have published on the front page of the newspaper.
- ☐ Do not email or text anyone your personal phone number, home or mailing address, or family, spouse/partner, or children's names on your work devices.
- ☐ Check with your IT and HR departments about protections that may be available to you if you have been doxed, including managing forwarding preferences, if there are encryption options, removing your information from your agency's website, and in-office safety planning.

SOCIAL MEDIA SAFETY

- ☐ Keep accounts and handles set to private in your settings.
- ☐ Remove any addresses, places of work or school, and locations from your account (not just hidden).
- ☐ Do not announce where you're going, including restaurants/parks/events and towns/cities/states/countries.
- ☐ Only accept friend invitations from known individuals.
- ☐ Only allow known friends to view your posts.
- ☐ Review who can share your posts.
- ☐ Vary your usernames/handles.

- ☐ Use different and strong passwords across social media platforms.
- ☐ Don't post photos showing your or others' faces.
- ☐ Don't post photos where someone could determine where you are/were.
- ☐ Scrub meta-data from photos you post. Remember, your photos can reveal your location and the date/time the photo was taken.
- ☐ Identify where to report doxing or hate speech on social media.
    - Facebook, Snapchat, Twitter, Instagram, Google, Yelp, etc. all have differing terms of use.

SAFETY MEASURES AFTER YOU HAVE BEEN DOXED

- ☐ Document what is happening.
- ☐ Take screenshots of everything.
- ☐ Try to include dates/times/usernames.
- ☐ Delete, if you can, but document quickly first.
- ☐ Report to police if there are threats. Be sure to include:
    - Protected class information, both actual and perceived
        - Oregon and federal hate crimes do not require that a perpetrator correctly identify your protected class.
    - Safety concerns
        - Family/kids/partners
        - Travel
        - Public appearances
    - Specific information regarding:
        - Imminence: does the perpetrator live close by?
        - What exact words were used? (Slurs, threats, weapons)
    - Any evidence, including screenshots. Remember that the timeliness of your report to police can affect evidence preservation.
    - Note that "true threats" stated online, sent via postal mail, or made through a phone call/left on your voicemail may be a federal crime. Make a report to FBI, or encourage your local police to cross report to federal law enforcement.
- ☐ Change passwords to your phone, email, and social media accounts. Ensure that each password is different and complex.
- ☐ Report to the platform and request the information be removed.

- Request that your handle/name/information is added to a "closely monitored" list so that information can be removed as soon as it pops up elsewhere.

☐ Talk to someone that you trust for support. You are not alone.
☐ Oregon's 2021 HB 3047 provides civil legal remedies for doxing. Talk to an attorney to see if you have additional civil legal remedies.
- Oregon State Bar Lawyer Referral Program
- Legal Aid
- Oregon Crime Victim's Law Center (OCVLC)

☐ Consider a Civil Protective Order
☐ Consider information that you *can* control such as whether you're on the platform at all, what you post, location sharing, etc. vs. what you do not have control over.
☐ Set up google alerts for your name, number, address to receive alerts if info pops up online.
☐ Use data broker opt-out options – some services you may have to pay for such as DeleteMe or Reputation Defender.
☐ Consider using separate email addresses for different purposes.
☐ Safety plan:
- At work – talk to HR.
- At home – make a clear plan with your family, talk to trusted neighbors, ask police for increased safety patrolling.
- In public – travel with a friend, take alternate routes, tell a trusted person where you are going and when you expect to return.

☐ Have conversations with family members/friends about information they share about you online.

ADDITIONAL RESOURCES FOR ONLINE SAFETY

Tips for creating strong passwords:

Internet Safety: Creating Strong Passwords (gcfglobal.org)
Create a Strong Password & a more Secure Account – Google Account Help

Learn more about internet safety:

Doxing: What it is and how to protect yourself | NortonLifeLock
5 Tips for Social Media Security and Privacy | Norton.com

Removing content from Google:
Removing Content from Google – Legal Help
Remove your personal information from Google
Remove select personally identifiable info or doxing content from Google Search

Anti-Doxing Legislation:
Press Release Oregon Senate Passes Anti-Doxing Legislation

End-to-end encryption:
Signal app
Whatsapp