CYBERWOMEN

Privacy

Privacy

https://iwpr.net/

Contents

1 Ask me anything! 5
Leading the Exercise 6

2 Privacy 9
Leading the Session 10
Part 1 – Do We Truly Have Privacy? 10
Part 2 – "Self-Doxxing" 11
Part 3 – What Do We Do Now? 12
References 13

3 Networked publics 15
Leading the session 16
References 17

4 Apps and online platforms 19
Leading the session 20
Part 1 – Our Devices, Our Data 20
Part 2 - Who Else is Tracking Us? 21
Part 3 – Promoting Women's Rights Using Social Networks . . 22
Part 4 – Reclaiming Privacy 23
References 24

Ask me anything!

- **Objective(s):** Explicar cómo nuestros conceptos de privacidad cambian radicalmente en los espacios online.
- **Length:** 15 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Privacy[1]
  - Apps and online platforms: friend or foe?[2]
- **Needed materials:**
  - Slides or cards with questions (see below)
- **Recommendations:** It is important that you share the instructions progressively with participants as you move through the exercise, in the order they are included below – if you provide the instructions all at once before actually conducting the exercise, it will give away the twist!

[1] https://cyber-women.com/en/privacy/privacy/

[2] https://cyber-women.com/en/privacy/apps-and-online-platforms-friend-or-foe/

This session is based on a module developed by Elis Monroy from Subversiones collective for the Voces de Mujeres project.

Leading the Exercise

1. Ask participants to choose a partner from the group, and to then find a quiet space for them to talk.
2. Once participants are situated with their partners, ask them to share with each other their answers to the following questions:

    - What is the most funny or embarrassing thing that has ever happened to you?
    - Mention one thing you hate doing the most.
    - Do you have any guilty pleasures with the music you listen to?
    - Did you have a nickname when you were a kid?

    As the trainer, you can add or change the questions as see fit – the goal is to ask questions that are likely to bring up information or anecdotes that could be a bit embarrassing or funny, and to talk about privacy with participants. There are more personal questions you can use, but be careful which ones you choose depending on your context – you don't want to make participants feel uncomfortable.
3. Once participants are done sharing their answers with one another, have them choose another pair to combine with (there should now be four participants in each group)
4. In the new groups they have formed, ask participants to introduce the partner they worked with during the first round, sharing with the new team members their answers to all the questions.
5. Once the groups of four have all introduced one another's stories, you can now ask participants to join with another group (there should now be eight participants in each group) – they should now repeat over again the process from Step 4.

6. Ask participants how they felt during the exercise. Some examples of issues which participants might raise could include:
    - A participant might have shared something because they knew the person they started the activity with at the beginning, or because they felt comfortable in that moment - but they didn't anticipate how the rules of the activity would evolve.
    - A participant might have noticed that her partner told one of her stories incorrectly.
7. Close the activity by talking about **privacy**, and how sometimes people agree to the Terms of Service of an online platform without it being clear what the "rules of the game" are, and how they might change over time. Talk also about **consent**, and how a person may sometimes (for instance) agree to have their picture taken, but that doesn't imply that they also agreed (or gave consent) for that picture to be shared online or with other people.

Privacy

- **Objective(s):** Introducing participants to the concept of privacy and identifying information about ourselves that is available online.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Your rights, your technology[1]
  - Ask me anything![2]
  - Apps and online platforms: friend or foe?[3]
  - Networked publics[4]
  - Doxxing the troll[5]
- **Needed materials:**

[1] https://cyber-women.com/en/rethinking-our-relationship-with-technology/your-rights-your-technology/

[2] https://cyber-women.com/en/privacy/ask-me-anything/

[3] https://cyber-women.com/en/privacy/apps-and-online-platforms-friend-or-foe/

[4] https://cyber-women.com/en/privacy/networked-publics/

[5] https://cyber-women.com/en/online-violence-against-women/doxxing-the-troll/

  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
- **Recommendations:** Some participants may become unsettled or upset by some of the information available about themselves online during the "self-doxxing" part of this session. if this happens, be sure to make plenty of time for the final part of the session where participants will focus on strategizing next steps in response to the information they find. participants should each have access to a device with an internet connection for the practical part of the session.

This session includes information from the "Self-Doxxing and Regaining Control" section of Tactical Technology Collective's manual "Zen and the Art of Making Tech Work for You".

Leading the Session

Part 1 – Do We Truly Have Privacy?

1. Start the conversation by asking participants whether they think privacy truly exists or not. Then, ask them about their own concept of privacy - share your own concept of privacy to provide an example. Transition into the next steps by telling the group that, in this session and during this training, you will all be reclaiming **your right to privacy!**
2. Ask participants to share some examples of factors that could be interfering with the control they have over their data, personal information, and other elements. These could be personal practices, the platforms they trust with their information, the knowledge they have about the tools and devices they use, or the actions of others in their networks.

Part 2 – "Self-Doxxing"

3. Explain to participants what **Doxxing means** – essentially, it's the practice of gathering a substantial amount of personal information about someone and then making it public (usually online). You should also explain how doxxing is sometimes used against people as a revenge tactic, and is often used to endanger, harass, or threaten activists and human rights defenders.
4. Tell the group that, in this part of the session, they will practice "self-doxxing" as a way to find out how much (and what kind) of information can be found about themselves online. Explain that this is useful preventative measure for taking steps to reduce the available amount of this information (when this is possible).
5. Ask participants to open a blank document on their computers, or to have a piece of paper ready to take notes of what information they discover. Then, have participants launch a browser window on their computers with a browser that is not the one they typically use – this is so they are not automatically logged-in to their various online accounts.
6. Ask participants, before they begin, to make a list of all the public accounts or social media profiles they have; then, ask them to make a list of keywords or phrases that could be linked to them, which could include information such as:
    - The city where they were born
    - The city where they currently live
    - Their home address
    - The organization they work for (or organizations they work with regularly)
    - Their activism cause
    - Major projects or campaigns they work on
7. To begin their self-doxxing, participants should first search for their various online accounts and profiles (these should appear as they would to the general public, since they won't be logged-in), taking note

of what information about themselves they are able to find.

8. Next, participants should search for their names and other keywords from the lists they made, using Google and DuckDuckGo as well as Facebook, Twitter, and any other platforms – here are a few additional suggestions for this step:
    - For Google and DuckDuckGo, they should do image and video searches as well as normal searches.
    - If they know of any specific online databases - for cities, governments, or otherwise – where their information could potentially appear, they should search those as well.
    - If they have their own website, they could search for the domain address at https://whois-search.com to see what information about them is available via the public domain registry.

Part 3 – What Do We Do Now?

9. Explain to the group now that, through their self-doxxing, some may have found information about themselves that they didn't know was publicly available, as well as online accounts they don't use anymore which they may have even forgotten that they had.
10. Ask everyone to look back through the notes they took, and then to think about which next steps they could take to assert more control over what others can find out about them online. Have them each make a "to-do" list of these steps, which could include actions such as closing certain accounts, editing their information and/or privacy setting configurations on social media profiles, enabling private domain registration on their website domain hosting, etc.
11. As participants make their to-do lists, share with them some resources that could be helpful for them as they implement some of these next steps – they may also get inspiration for other steps they hadn't yet thought of:

Temporary URL Blocking Tool: Can be used to block search results for websites - does not actually remove content, but blocks older (and potentially more sensitive) content from search results until website(s) can be updated: https://support.google.com/webmasters/answer/1663419?hl=en&lr=all&rd=2

Deleting Facebook Accounts: Contains instructions for deleting or disabling Facebook profiles: https://www.facebook.com/help/224562897555674

AccountKiller: Has instructions on how to remove accounts or public profiles for most popular websites and social networking services: https://www.accountkiller.com

JustDelete Me: A directory of direct links to delete accounts from web services and social networking services: http://justdelete.me

12. To close the session, remind participants that doxxing reveals only the information that is publicly available about them; however, the actual social media platforms and online services themselves can see much more. Emphasize to the group that better privacy is also supported by using stronger passwords, practicing safer browsing habits, and taking advantage of encryption to secure information from others.

References

- https://gendersec.tacticaltech.org/wiki/index.php/Self-dox

Networked publics

- **Objective(s):** Introduce participants to the concept of 'networked publics' to better understand the key issues and implications of technology's expanded role in society.
- **Length:** 20 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Ask me anything![1]
  - Privacy[2]
  - Doxxing the troll[3]
  - What does your metadata say about you?[4]
- **Needed materials:**
  - Slides (with key points included below)

[1] https://cyber-women.com/en/privacy/ask-me-anything/

[2] https://cyber-women.com/en/privacy/privacy/

[3] https://cyber-women.com/en/online-violence-against-women/doxxing-the-troll/

[4] https://cyber-women.com/en/safe-online-advocacy/what-does-your-metadata-say-about-you/

- Laptop/Computer and Projector setup

This session is based on Danah Boyd's research.

Leading the session

1. Begin the session by explaining that it is focused on better understanding what happens when technology becomes an increasingly central and essential component of society, and the impact that this has on identity and privacy.
2. Explain that, to illustrate this, you will be featuring some of the key concepts found in Danah Boyd's research, called Taken Out of Context American Teen Sociality in Networked Publics:

   > Networked Publics: Networked publics are simultaneously the space constructed through networked technologies and the imagined community that emerges as a > > result of the intersection of people, technology, and practice.
   >
   > Content of Networked Publics: The content of networked publics is inherently made out of bits. Both self-expressions and interactions between people produce bit-based content in networked publics.
   >
   > Four Properties of Networked Publics: The features of bits configure the four properties that are key to networked publics:
   >
   > Persistence: online expressions are automatically recorded and archived; Replicability: content made out of bits can be duplicated; Scalability: the potential visibility of content in networked publics is great; Searchability: content in networked publics can be accessed through search.

These four properties structure network publics and the interactions that take place in them.

Dynamics of Networked Publics: Invisible audiences: not all audiences are visible when a person is contributing online, nor are they necessarily co-present.

Collapsed contexts: the lack of spatial, social, and temporal boundaries makes it difficult to maintain distinct social contexts.

The blurring of public and private: without control over context, public and private become meaningless binaries, are scaled in new ways, and are difficult to maintain as distinct.

3. Explain and provide examples of each of the four properties, as well as the dynamic. It will help if you can accompany this with images related to each, to make it easier for participants.

References

- http://www.danah.org/papers/TakenOutOfContext.pdf

Apps and online platforms

- **Objective(s):** To focus on the apps and online platforms they use most – you will help them to identify the kinds of information shared with these platforms, and to strategize tactics for using them safely in their personal activities and online activism.
- **Length:** 120 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
  - Personal perceptions of security[1]
  - How does the internet work?[2]
- **Related sessions/exercises:**
  - Ask me anything![3]
  - Privacy[4]

[1] https://cyber-women.com/en/rethinking-our-relationship-with-technology/personal-perceptions-of-security/

[2] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/

[3] https://cyber-women.com/en/privacy/ask-me-anything/

[4] https://cyber-women.com/en/privacy/privacy/

  - Networked publics[5]
  - Safe online campaigning[6]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - Paper (a few sheets for each participant)
  - Post-it Notes (in multiple colors)
- **Recommendations:** Participants should have their mobiles or one device with internet for the practical part of the session. provide participants with further recommended resources where they can learn more about privacy, and steps they can take to better protect theirs (see references section for links).

Leading the session

Part 1 – Our Devices, Our Data

1. Ask participants to go through all the apps they have on their devices and check the following:
   - Which device permissions each app has;
   - Their privacy policies, to see what can be done with the data each app has access to.
   - Who the developer of each app is.
2. Give participants approximately 15 minutes to do the above. Once time is up, ask participants to share what they found in this quick search. Make sure that you cover issues such as:
   - App permissions that have no clear relationship with their actual function;
   - Terms of Service that are unclear or vaguely written;

[5] https://cyber-women.com/en/privacy/networked-publics/
[6] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/

- Privacy policies that allow companies to sell user data to third parties.

3. Share examples of "menstruapps" - menstrual cycle tracking apps - and other personal health related apps with the group. Explain how according to research that has been done (via Chupadatos[7]), it's been shown that menstruapps can gather quite a bit of personal data from users:

    - Name, phone number and address
    - Bodily details such as menstrual pain, weight, and hours of sleep;
    - Emotional states like stress, lack of concentration or anxiety;
    - Details about sexual health, including any contraceptive methods;
    - Online behaviors like click-throughs and type of devices used;
    - Offline behaviors including medicine taken, or habits like drinking or smoking.

    That's a lot of information, right?

Part 2 - Who Else is Tracking Us?

4. Split participants into groups of 3-4 participants (maximum) and ask each group to make a list of what they know about Facebook and Google – to provide an example, you can have them start buy answering these questions:

    - Are these entities actually companies?
    - What are these companies' missions or objectives?
    - What are the services they offer?
    - Are those services for free or paid?
    - What are the rules/terms of those services?

    Give participants 15 minutes to finish listing all the information they have.

[7] https://chupadados.codingrights.org/es/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/

5. Once time is up, ask each group to then make a list of what these two companies, Facebook and Google, might know about them. If participants have access to internet from their computers or mobile devices, those who have a Gmail account may want to visit the page https://www.google.com/maps/timeline as well to help with this part of the session. Give participants 20-25 minutes to make their lists, which each group should then briefly present to the rest of the participants.

Part 3 – Promoting Women's Rights Using Social Networks

6. For this next part of the session, keep participants in their present groups – you will give each group a question to discuss and work on together (taking from the list below):
    - Which tools or online platforms are we using to organize and exchange information from our social movements, protests and campaigns? What are some of the advantages or disadvantages of using those tools for that purpose?
    - Do we know any examples of censored campaigns, pages taken down from Facebook, videos censored on YouTube or other instances of social media accounts being closed?
    - Companies like Facebook and Google are good friends of our governments, and are known to share users' information with them (https://govtrequests.facebook.com) What are the implications of this?
    - Do we know of any cases of violence against women online? Specifically, any cases involving WHRDs receiving threats online, having their nudes exposed, or social media accounts being created to discredit them or "advertise" their sexual services? On which platforms did these incidents happen, and how did the platform react?
    - Have each group take about 10-15 minutes to answer their question; once time is up, ask each group to share their conclusions

with the rest of the participants.

7. Together as a group, take 5-10 minutes to reflect on how these same social networking platforms also serve as gathering places for many online users – as such, they seem to be ideal places to implement campaigning efforts. Ultimately, Facebook and the various services offered by Google provide different useful ways to interact with followers and community members; therefore, despite some of the concerns or disadvantages of these platforms, it's important to remember that many participants may still want to use them to reach out to their audiences.

Part 4 – Reclaiming Privacy

8. You'll now lead participants through the final closing portion of the session. Explain that you will now look at ways to reclaim privacy online, by learning how to continue using these apps, online platforms and social networking sites for personal use or advocacy efforts, but in a safer way.
9. With participants remaining in the same groups as before, ask them to now focus on collaboratively brainstorming creative ways to reclaim their privacy. Give each group a block of post-it notes along with some markers and pens, and have them generate as many ideas as they can think of in 10-15 minutes. You can provide some example tactics to get them started, such as:
    - Confusing the algorithms that platforms use for advertising or content optimization;
    - Regularly checking platforms' privacy policies and updates to privacy settings;
    - Being aware of app permissions on their devices, specifically things like location settings and geo-tagging of photos and posts;
    - Using alternative platforms that are more committed to privacy

and activism (Riseup, Tutanota, Signal, etc.)

Once they've finished this final part of the exercise, have each group share some of the ideas they came up with – you can post these in a visible place in the training room for participants to refer to as they move through the training process. These ideas will also be useful for you as you adjust the content of your training, especially if participants want to focus more on improving their safe use of social networks for their activism.

References

- https://www.kaspersky.es/blog/digital-detox-advices/6226
- https://rankingdigitalrights.org/2017/08/30/rdr-en-espanol-guest-post
- https://myshadow.org
- https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual
- https://www.digitale-gesellschaft.ch/dr.html
- http://www.europe-v-facebook.org