

Information mapping worksheet

Make a copy: [FILE > MAKE A COPY]

Best Practices when doing this activity

When performing a personal information mapping exercise, below are some best practices:

- **Use private browsing/incognito mode:** Private browsing/incognito mode prevents your browser from storing search history, cookies, and other temporary data. This helps ensure that your search results are not influenced by your previous online activity or search history.
- **Log out of your accounts:** Logging out of your Google, Bing, or other search engine accounts, as well as social media and other online platforms, helps reduce personalized search results. This allows you to see the information that is publicly available about you, rather than the information tailored to your online profile.
- **Try to use a VPN:** A VPN can help mask your IP address and location, allowing you to search as if you were in a different location. This can be useful in finding information that may be region-specific or not available in your current location.
- **Use multiple search engines:** Different search engines may return different results, so it's essential to use more than one search engine during your self-doxxing exercise. This can help ensure that you're finding as much publicly available information about yourself as possible.
- **Conduct the exercise in multiple sittings:** Performing the activity in multiple sittings allows you to take breaks, revisit your search strategy, and approach the task with a fresh perspective, which can help you uncover more information or think of new ways to combine search operators and keywords.
- **Try new search combinations and keywords:** As you continue on the activity, try new combinations of search operators, keywords, and personal information to uncover more results. This can help you discover information that may be hidden or less easily accessible.

- **Remember new places where you may have shared information:** Over time, you may remember additional websites, forums, or platforms where you've shared personal information. Be sure to include these in the worksheet to ensure a comprehensive assessment of your online presence.

Worksheet

Goal: To help you identify and think through your online presence by mapping your digital footprints across various apps, services, and platforms. Then, take action if deemed needed.

Instructions:

1. In the first column ("App/Service/Platform"), list all the apps, services, and platforms where you have an account, shared information, or interacted with others online. Consider social media, email, messaging apps, online forums, blogs, e-commerce sites, activities related to universities or from your time at school, and any other relevant places. Try to think back to your earliest interaction on the internet until today and list as much as you can. Chances are you won't remember everything at this moment - that's fine, refer back to the worksheet when you do. Perhaps someone else added information about you, search yourself to find as much information about yourself as you can. Try dorking.
2. In the second column ("Privacy Settings"), assess your current privacy settings for each app, service, or platform. Indicate whether your information is publicly accessible, visible to friends or connections only, or restricted to specific individuals. If it's a blog post or article that someone wrote about you where you cannot change a privacy setting, indicate that as "n/a". You can later decide whether you want to try to remove or amend that information.
3. In the third column ("Information Shared"), identify the types of personal information you share or store on each app, service, or platform. This may include your name, address, phone number, email address, photos, and other sensitive or identifying details. Add links to the specific sources of information.
4. In the fourth column ("Risk Level"), evaluate the potential risk associated with the information you share on each app, service, or platform. Use the dropdown to rate the risk level, considering factors such as the sensitivity of the information, the likelihood of it being misused, and the potential impact on your privacy and safety.
5. In the fifth column ("Action Plan"), identify specific actions you can take to manage and reduce your digital footprint on each app, service, or platform. This may include:
 - Updating privacy settings (see [Social Media Security & Privacy Checklists](#))

- Removing or hiding information where you can
- Changing your username
- Deleting your account entirely
- Changing the email associated with a certain account (see [Firefox Relay](#))
- Reaching out to the content owners to remove or amend the information
- Using a personal information removal service
- Submitting a search engine removal request (see for [Google](#))
- Creating alerts such as the Google alert or [Mozilla Monitor](#)
- Opt out of data brokers – [Big Ass Data Broker Opt-Out List](#)

App/Service/Platform	Privacy check?	Information shared/found*	Risk Level	Action Plan
Facebook	- ▾		- ▾	
Instagram	- ▾		- ▾	
LinkedIn	- ▾		- ▾	
Wikipedia	- ▾		- ▾	
AirBnB	- ▾		- ▾	
TikTok	- ▾		- ▾	
University club activity shared on website	- ▾		- ▾	
Wikimedia Commons	- ▾		- ▾	
Meta-Wiki	- ▾		- ▾	
Search engine result 1	- ▾		- ▾	
Search engine result 2	- ▾		- ▾	
Search engine result 3	- ▾		- ▾	
...	- ▾		- ▾	
...	- ▾		- ▾	
...	- ▾		- ▾	

*** Example:** Name, work email, private email, phone number, profile photo, workplaces, previous home addresses, current address, CV, salary disclosure, gender, sexual orientation, date of birth, nationality or citizenship, social media handles, usernames on websites/forums, passwords, banking details, financial information, passport number, driver's license number, government-issued ID, medical information, emergency contacts, marital status, family members' details, photos of personal belongings, IP address, device information, location data, search history, browsing data, online shopping history, biometric data, professional associations, memberships, political affiliations, religious affiliations, travel history, education history etc...

Search operators

Search operators are special commands or symbols used in search queries to refine and customize search results in search engines. Search operators can help you find and monitor your personal information online, enabling you to take necessary steps to protect your privacy . The examples provided demonstrate how to use these operators in the context of an information mapping activity, and some examples show how to combine operators for more specific and targeted searches.

Operator	What it searches	Example
Site	Provides results of pages located on a specific domain	site:linkedin.com
AND/OR	Use the AND operator to return results containing two results. Use the OR operator to return results that contain one result or the other result.	"John Smith" AND (Portland OR Salem)
Asterisk	Google treats the asterisk as a placeholder for a word or words in a search string.	"John * Smith"
Hyphen	This operator allows you to exclude the text immediately following it.	"John Smith" -site:yournewssite.com
Filetype	Filter search results by a single file type extension Common File Types:	filetype:xls intext:you@youremail.com

	• DOC/DOCX • XLS/XLXS • PPT/PPTX • TXT • JPG/JPEG/PNG (Image files) • PDF	
--	--	--

Other Relevant links:

- [Diff: Doxing 1: Why should you care?](#)
- [Diff: Doxing 2: Have you tried doxing yourself?](#)
- [Diff: How can a username keep you safe?](#)
- [Digital Safety Considerations for Wikimedians](#)
- [NYT: A Guide to Doxxing Yourself on the Internet](#)
- [Have you been pawnd?](#) This is a website that allows Internet users to check whether their personal data has been compromised by data breaches.