Digital Integration Teaching Initiative

Northeastern University
NULab for Digital Humanities and Computational Social Science

Social Media Data Privacy

Click to schedule a meeting with the DITI Team

When conducting digital humanities and computational social science projects, social media data can provide valuable insights. This handout will cover some important questions around data privacy on social media and provide privacy tips for several popular social media platforms.

What is data privacy?

At its simplest, data privacy is a person's ability to control what of their personal information is shared and with whom. This can be understood as:

- Knowledge of what information is shared with the application/program/service in question.
- Knowledge of what third parties this data is shared with or exposed to.
- Understanding the right to recall or delete data retained by the application/program/service in question.

How is this data accessed?

Social media, websites, and other online applications collect their users' data, ostensibly in order to provide effective services. Many organizations, including government agencies and technology companies, leverage data to gain insights into users behavior, optimize products and services, and generate revenue.

But is it always clear how or why our data is being collected?

There are two main issues that users often run into when it comes to violations of their data privacy.

The first is that users are often unaware of the extent of data collection that is occurring. This means that users are allowing these platforms and applications to collect more personal information than they are aware of. A famous example of this occurred in the 2010s, when the consulting company Cambridge Analytica collected the personal information of millions of Facebook users without their knowledge (you can learn more by reading this *New York Times* article). Below are links pointing to instructions for downloading your data from several popular platforms:

- **Facebook**: Download a copy of your information on Facebook
- **Google**: How to download your Google data
- **Instagram**: Access and download your information on Instagram
- **TikTok**: Requesting your data
- **Reddit:** How do I request a copy of my Reddit data and information?
- **X:** How to access and download your X data

Once you have downloaded your data, you can review it to determine if you need to adjust your privacy settings to prevent future data gathering.

The second is an unawareness of how data is being shared and with whom. This is often due to the inaccessible nature of a company/program/service's data privacy information—through the use of confusing language, burying the information within terms and conditions, or making it inaccessible to users of differing abilities. In some cases, these platforms and applications also have weak safety mechanisms around their data storage and it results in hacking which then leads to data breaches, where users' personal information is leaked.

What is dangerous about this?

There are a myriad of ways that the collection of a user's personal data can harm the individual. Three, in particular, come up frequently and have especially significant impacts:

- The first, and the one that has received the most attention recently, occurs when platforms and applications sell users' data to outside parties, leading to users receiving unwanted advertising often without their knowledge or consent.
- The second most often occurs when there is a data breach. Such breaches may be done by hackers with criminal intentions—such as identity theft, financial theft, or even harassment.
- The third occurs through data surveillance: when a government, company, or organization uses personal data to perpetuate oppressive or authoritarian practices.

How can data privacy be protected?

The first and most important way to protect your personal information is for you to ensure you are aware of when and how your data is being used on a given platform or application. This often means reading through the fine print that you scroll through before clicking "accept." Sometimes, however, the applications of your data might be couched in language that is purposefully hard to understand. If that's the case, you can always do further research around the data protection policies of that company.

How can I increase my privacy on social media?

While privacy risks vary by platform and individual, it is generally important to be aware of the information you are sharing, who is able to find that information, and how they can find it. You should carefully review the permissions you grant each app on your phone and be on the look-out for requested permissions that may go beyond what would be expected for the app's functionality. For example, some social media apps access your phone's location. You can review app permissions in your phone settings and revoke the app's location permissions and any other permissions you do not want the app to have. You can also review your phone's camera settings to make sure that location information is not automatically being added to your photos. While many social media companies remove this information from the pictures you share, it might be transmitted if you share the photo elsewhere online. Google and Apple provide guidance on how to change these settings in your phone camera. Many social media platforms allow you to select the audience for your posts. If you only want people you are connected with to see your posts, make sure that the audience settings reflect that preference and are not set to public. Some social media platforms also allow you to select to what extent your account information is available to anyone on the Internet, and whether anyone on the Internet is able to search your name or other contact information and find your account. Below are some tips for how to increase your privacy on popular social media platforms:

- Facebook
    - Groups on Facebook can help people with similar interests connect. It is important to know whether a group you are joining or helping to run is public or private. For public groups, anyone on the Internet can find the group and see posts and comments in the group, and anyone on Facebook can see a list of group members. For private groups, group administrators can decide whether anyone on Facebook can find the group or if it can only be found through invitation. Content shared in the group, and group membership, is also only shared with current members in a private group.
- Instagram
    - On Instagram, you can set your account to be public or private. With a private account, your posts will only be visible to approved followers. With a public account, your posts are visible to anyone on the web.

  - Some search engines index public posts on Instagram, making it easier for others to find them. To avoid this, you can set your account to private and revoke “access to third-party apps and websites”.
- TikTok
  - On TikTok, you can set the visibility of each post. If you have a public account and set the visibility to Everyone, then anyone on the Internet will be able to see your post.
- Reddit
  - While Reddit has limited privacy controls and most forum content is public, you can set up and participate in private communities where only moderator-approved community members can see content.
  - When setting up an account you do not have to use your real name.
- X
  - On X, people can search for your account using your email or phone number. To prevent this, you can disable this feature in your Discoverability settings.

Technology and company policies are constantly changing, so it is important to regularly review your privacy settings. Many of these settings rely on you to know the people you are connected with. For example, if you are friends with an account masking their real identity, your information could be shared in ways you did not intend. Also be aware of your friends’ privacy and make sure you are not sharing anything they would not want you to share.

Are there resources for further research?

Yes! There are a myriad of resources available for understanding the ways in which your data is being collected and used by a given platform or application. An easy to use and clear website is Common Sense Privacy Program, which allows you to search for a specific entity, see its privacy rating, and read through an explanation for why it received this rating. The Electronic Frontier Foundation also provides the Surveillance Self-Defense project, a guide to help you protect your privacy online.