

---

# Social Media Data Privacy and Law

[Click to schedule a meeting with the DITI Team](#)

---

This handout will explore data privacy laws in the European Union, the United Kingdom, and the United States. Focusing on social media data privacy, it considers cookie usage and examines a relevant case study. It concludes by providing tips for protecting your data privacy on several popular social media platforms.

## Definitions

Before we delve into laws, let's define some important terms:

- **Cookies:** small text files that a domain (website, application, program, or other service) creates and stores on a user's device. Social media, websites, and other online applications collect their users' data, ostensibly to provide effective services. Many organizations, including government agencies and technology companies, leverage data to gain insights into user behavior, optimize products and services, and generate revenue. This is often done through cookies. Social media platforms like Facebook, Instagram, and TikTok use cookies. There are two types of cookies.
  - **First-party cookies:** these record data such as which pages you visited, as well as data that you voluntarily submit, such as your login credentials, the items you left in your shopping cart, or your location. They are created and only available to the domain (website, app, or other program) that the user visited.
  - **Third-party cookies:** these are created by domains other than the one you visited. They are accessible by multiple domains and track your activity across multiple websites. They are usually used to develop targeted/personalized advertisements. For example, your likes, comments, and engagement on social media may be used to choose advertisements for you on a different website.
- **Data privacy:** the ability to control where and how one's personal information is shared. This involves:
  - Knowledge of what information is shared with the application/program/service being used
  - Knowledge of what third parties this data is shared with

## Digital Integration Teaching Initiative

- The right to recall or delete data retained by the application/program/service being used
- The right for a user to access the data collected on them by an application
- **Personal data:** any information that can identify, or even partially identify, a user. This includes names, phone numbers, emails, addresses, IP addresses, health data, or cookie IDs.

### Laws that Shape Social Media Data Privacy

Several laws dictate your data privacy, and this depends on where you are located when using a particular social media platform. Below is a list that compares data privacy laws between the European Union (EU) and the United States (US).

**European Union:** in the EU, the main law governing data privacy is the General Data Protection Regulation ([GDPR](#)). It outlines the ways in which companies and organizations should use personal data. The GDPR has strict requirements on how organizations handle personal data.

- This includes (but is not limited to):
  - Processing data must be performed fairly and transparently
  - Processing data must be done for specific reasons
  - Personal data must be stored for a specific amount of time and cannot be stored for reasons other than the original purpose
  - Only the data necessary for its specific purpose must be collected, not more
  - Data must be protected from breaches or unlawful access, loss, or damage
- The GDPR regulates cookies because many cookies contain personal data that can be used to identify users
- Cookie consent pop-ups became more prevalent after the GDPR was put into law in 2018

**United Kingdom:** since the UK left the EU, it has adopted its own version of the GDPR: UK-GDPR. The laws are very similar, with very minor differences that generally relate to lawmakers, implementation, and jurisdiction. See [this webpage for more information on these differences](#).

- **United States:** while the EU has the GDPR as the main law on data privacy, the US has multiple laws related to data privacy. For example, [HIPAA and GLBA](#) are two federal laws that require the privacy and protection of personal data related to patients in healthcare systems (HIPAA) and consumers of financial institutions (GLBA). [COPPA](#) is a federal law

that governs how organizations process the personal information of children. But there is no comprehensive federal law that relates to the vast majority of users' personal data collected by organizations, including social media. Some states such as Colorado and California have stricter laws that relate to personal data privacy on social media, but there is no single, federal, comprehensive law relating to data privacy in the US.

The following are articles that detail the differences between data privacy laws in the US and EU:

- [“EU vs US: What Are the Differences Between Their Data Privacy Laws?”](#) by Endpoint Protector
- [“Comparing U.S. State Data Privacy Laws vs. the EU’s GDPR”](#) by Bloomberg Law

### What is dangerous about a lack of data privacy?

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:

- **Selling data:** sometimes, social media platforms use third-party cookies to sell users' data to outside parties, often without users' knowledge or consent. This leads to users receiving unwanted advertising
- **Data breach:** hackers with criminal intentions—such as identity theft, financial theft, or even harassment—may breach data from one platform to outside individuals or companies.
- **Data surveillance:** this occurs when a government, company, or organization uses personal data to perpetuate oppressive or authoritarian practices.

### Case Study: TikTok's Data Collection

Compared with other social media platforms, TikTok has been met with more concern about its data collection methods and transparency. It has faced regulatory scrutiny in the US and the EU for various reasons that differ primarily due to the different laws in place.

- **European Union:** In the EU, in May 2025, TikTok was fined hundreds of millions of Euros for breaking data protection laws. TikTok was accused of allowing EU users' personal data to be accessed by TikTok employees in China. In 2023, TikTok was also fined for processing children's personal data in ways that allegedly violated the GDPR. TikTok representatives have denied both charges, but the cases allow us to consider the impact of data privacy laws on the one hand, and TikTok's data collection practices on the other. The following articles offer more details about TikTok's scrutiny in the EU:

- Readings about the 2023 case:
  - [Reuters' article about TikTok being fined for violating EU children's data protection rights in 2023](#)
  - [The European Data Protection Board's statement about TikTok being fined in 2023 for violating EU children's data protection rights in 2023](#)
  - [TikTok's response to the Data Protection Commission's decision in 2023](#)
- Readings about the 2025 case:
  - [Reuters' article about TikTok being fined for breaching data protection in the EU in 2025](#)
  - [The Irish Data Protection Commission's statement about fining TikTok in 2025](#)
  - [TikTok's response to the Irish Data Protection Commission's fine in 2025](#)
- As of now, TikTok has appealed both charges and has yet to pay any fines as the court process is still ongoing. However, since the first case in 2023, the European Commission, European Parliament, and Council of the EU have banned TikTok from the devices of EU employees.
- **United States:** The US government argued that TikTok's data collection threatens national security and attempted to ban it. Similar to the Irish Data Protection Commission, they accused TikTok of illegally sending data to China. Unlike the EU, the US government is attempting to ban TikTok, not just fine it, which poses questions on [free speech](#). Other analysts point out that TikTok's data collection practices may not be so different from those of other social media platforms.
- The following articles offer different perspectives on this:
  - [New York Times's article on the TikTok ban](#)
  - [CyberNews's article on the TikTok ban](#)
  - [The American Civil Liberties Union's article on the TikTok ban](#)
  - [TikTok's response to the US Supreme Court's decision in January 2025](#)
  - Currently, TikTok is still functional in the US, but there is government pressure to sell it to a US entity or ensure its oversight by the United States government.

See [this article for more details on TikTok's data collection](#).

### Tips on protecting social media data privacy

1. Be 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."

## Digital Integration Teaching Initiative

2. Be aware of the information you are sharing, who is able to find that information, and how they can find it. If you only want people you are connected with to see your posts, make sure that your 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.
  - a. Many privacy 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. It is best practice not to accept a “follow” or “friend” request from someone whose identity you cannot confirm.
  - b. 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.
  - c. Review your [phone's camera settings](#) to make sure that location information is not automatically being added to your photos. This information may be stored in the images you post. [Google](#) and [Apple](#) provide guidance on how to change these settings in your phone camera.
3. Assess your own personal risk and how comfortable you are with your personal data being shared. Certain individuals may face a greater risk when their data is exposed than others. For example, recently, the [United States government has been using social media surveillance targeting immigrants](#) and marginalized groups. Also be aware of your friends’ privacy and make sure you are not sharing anything they would not want you to share.
4. Be aware of how much of your data is being collected. We are often unaware of how much data social media companies collect. Below are links pointing to instructions for downloading your data from several popular platforms. 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.
  - a. **Facebook:** [Download a copy of your information on Facebook](#)
  - b. **Google:** [How to download your Google data](#)
  - c. **Instagram:** [Access and download your information on Instagram](#)
  - d. **TikTok:** [Requesting your data](#)
  - e. **Reddit:** [How do I request a copy of my Reddit data and information?](#)
  - f. **X:** [How to access and download your X data](#)

For more tips on increasing privacy on social media platforms, check out the DITI’s [Handout on Social Media Privacy](#).

## Digital Integration Teaching Initiative

### Further Resources




Resources on data privacy:

- [Common Sense Privacy Program](#): a website that allows you to search for a specific entity, see its privacy rating, and read through an explanation for why it received this rating.
- [Electronic Frontier Foundation](#): provides the [Surveillance Self-Defense](#) project, a guide to help you protect your privacy online.
- [The Markup - Blacklight](#): a tool that allows you to submit website addresses and provides you with information about its data collection and privacy practices.

Resources on privacy laws:

- [“EU vs US: What Are the Differences Between Their Data Privacy Laws?”](#)
- [“Comparing U.S. State Data Privacy Laws vs. the EU’s GDPR”](#)

DITI Resources:

-  Handout: Data Ethics
-  Handout: Data Privacy
-  Handout: Social Media Data Privacy