NYC Digital Safety
Privacy & Security

Online Surveillance
Facilitation Guide

Dig into issues surrounding online surveillance through discussion, reflection, and exploration of different examples.

Overview

This module introduces learners to trends and developments in online surveillance. Learners are encouraged to discuss, explore, and consider the issues and challenges posed by surveillance and to reflect on how surveillance might affect their own experiences with the internet and digital tools.

For more information, be sure to watch Series 5 training videos from NYC Digital Safety.

Outcomes

By the end of this module, participants will be able to:

- Define surveillance, particularly in an online context
- Describe issues and challenges surrounding surveillance in online environments
- Identify ways to continue learning about online surveillance issues

Format + Time Frame

This module provides a more conceptual overview of the topic of surveillance, particularly in online environments, and introduces learners to trends and ongoing issues posed by different kinds of online surveillance. This module is designed to both introduce terms and concepts and to provide participants with a space for discussion, reflection, and exploration.

This module will take approximately 55 to 60 minutes to complete. The content in this module can be delivered in different ways, whether via a discussion-based workshop session or as a component in another, more hands-on, skill-building module. See below for more suggestions.

NYC Digital Safety
Privacy & Security

Materials

- Slide deck
- Facilitation guide

Lesson Plan

Activity	Materials	Time Needed
Introduction and welcome Greet learners and review the plan for this module.	Slides 1 and 2	2 minutes
Define surveillance and discuss this definition Start by introducing a broad definition of surveillance. Then, open a discussion and have participants share their own thoughts and impressions about the term.	Slides 3 and 4	8 minutes
Surveillance mechanisms Review the information here on how and where surveillance tends to occur. Share the technologies used to engage in surveillance and the different entities that engage in surveillance, including governments and private companies.	Slide 5 and 6	5 minutes
Activity: Online surveillance examples Briefly pause to see if any of your learners have any examples of online surveillance that they have heard about and would like to share.	Slide 7	5 minutes

Debates on surveillance Review some of the debates surrounding surveillance, especially online surveillance. These debates include situations where surveillance might be beneficial, situations where it is damaging and harmful, and questions arising from surveillance and data-gathering practices online.	Slides 8 through 11	10 minutes
Activity: Surveillance debate Begin by introducing some discussion guidelines and what to do if the discussion gets heated or uncomfortable. Next, have participants engage in individual reflection for about 5 minutes to consider how surveillance affects their online experiences. Break your learners into small groups. Pose the questions on the slide around online surveillance in different situations to them and encourage them to discuss and share their views for about 15 minutes.	Slides 12 through 14	20 minutes
Wrap up, final tips, and final questions Review the closing thoughts and share the suggested resources. See if anyone has any final questions.	Slides 15 through 18	5 minutes

Considerations

The topics covered in module 5 are all complex and at times contentious. For surveillance, many of your learners might come in with certain preconceptions, impressions, experiences, and ideas

that will shape their view of the topic. Given the nature of the topic and the fact that some might have had negative experiences with surveillance in the past, you might consider using a pre-test question to get a sense of your learners' questions and views to help you better prepare for the workshop. See suggestions below.

The main goal of the modules in lesson block 5 is to give learners a chance to explore, reflect, and discuss some of the major issues surrounding digital safety and our online experiences more broadly. As such, you might consider keeping the structure of this workshop fairly loose and making adjustments as needed based on how the discussion flows and the questions your learners may have. Feel free to bring in your own examples, recent stories you have read on this issue, or revise the discussion questions posed on the slides to your liking.

You might also consider taking some time to immerse yourself in this topic before your workshop to ensure that you are comfortable and confident with the content. The NYC Digital Safety videos and the resources suggested on the slide deck can all be great places to go to learn more. This workshop could potentially benefit from having a co-instructor to provide support and expertise, help lead discussion, or offer different perspectives.

Options and Variations

This module is designed to be conceptual in nature and can be offered in a variety of ways. You could pair parts of this module (including key definitions, examples, or discussion prompts) with other, more hands-on modules for a richer learning experience. Additionally, this module could work well as part of a longer workshop series on various digital safety topics. The content here is designed to be flexible and you can either run this module as is, make it part of a series, or take portions of this module to use with another digital safety module of your choosing.

One option you could consider is combining the modules on censorship, surveillance, and privacy as a way to have a more wide-ranging discussion of these connected issues. You could also run these workshops together as part of a discussion series.

Note that this module contains numerous places for discussion. If you are looking to add more discussion elements or reflection opportunities to another digital safety workshop, you could consider utilizing the prompts from this module.

This content here works best when introduced in a workshop setting where there can be a chance for questions and guided discussions. However, you can emphasize the themes and concepts included here if you are engaging with a patron one-on-one at a service point and if you are providing them with handouts and materials from other digital safety modules. You might also consider sharing some of the resources listed on the slides with patrons who wish to learn more about the topics and issues covered here.

Assessment

The following are some suggested assessment questions that you can use and adapt for your own purposes. These questions can help you assess various things, including knowledge retention, personal views and preferences, and concept application.

You might consider asking these as a pre or post test, or you can have learners answer these as part of an exit survey or a follow-up survey. Keep reading for suggested questions and an answer key with further details and explanations.

Questions for Participants

What is surveillance?

A. The suppression of speech, information, and public communication by different entities, including governments or private companies

B. Freedom from being observed or disturbed by other people

C. The monitoring of behavior, activities, or information in order to gather information or influence someone's behavior or actions

D. Being free from danger or threats

Do you think surveillance is ever appropriate in certain situations?

A. Yes

B. No

C. Unsure

Who or what can engage in surveillance? Select all that apply:

A. Governments

B. Private companies

C. Individuals

D. Corporate advertisers

What questions do you have about online surveillance? What would you like to learn more about in the future?

[Free text response]

Answer Key

What is surveillance?

Answer: C, The monitoring of behavior, activities, or information in order to gather information or influence someone's behavior or actions

Surveillance is essentially the monitoring of someone's activities and behavior to gather information or to influence that person.

Do you think surveillance is ever appropriate in certain situations?

Answer: no correct answer, individual poll

This is an opinion poll that you might consider using to get a sense of your learners' views. This could be interesting to do as a pre and post test question to see if anyone comes away from the workshop with changed views.

Who or what can engage in surveillance? Select all that apply.

Answer: A, Governments; B, Private companies; C, Individuals; D, Corporate advertisers

While surveillance often gets associated with governments, all of these entities can engage in surveillance.

What questions do you have about online surveillance? What would you like to learn more about in the future?

> *Answer: Free text response*

> You might consider using this as a pre-test question in order to get a sense of what your learners are interested in and hope to discuss. You can use these responses to pose questions or guide discussion in your workshop.

Connections to Other Modules

This module connects to many other modules. The following suggestions provide opportunities for exploration, connection, and potential programming. However, feel free to explore and make connections between other modules not listed here as well!

This module in particular can connect with nearly every other module here, given the foundational and conceptual nature of the content included. While we have listed a few suggested ones, note that this module can really connect with all other modules.

1.1 Data Generation Online

1.2 Data Minimization

2.1 Algorithms
2.1 Targeted Advertising

2.2 Doxing
2.2 Data Brokers
2.2 Social Media Settings

4.1 Avoiding Social Engineering

These and other modules can be found at this project's website, nycdigitalsafety.org.

About This Project

These materials were released in October 2022 as part of NYC Digital Safety: Privacy & Security.

NYC Digital Safety: Privacy & Security is a partnership between New York City's three library systems — Brooklyn Public Library, The New York Public Library, and Queens Library — and METRO Library Council. With support from the New York City Office of Technology and Innovation, this project ensures that NYC residents can rely on public libraries for their questions about internet privacy and security.

Visit nycdigitalsafety.org for more information.