

INSTRUCTOR GUIDE AND NOTES

Ad trackers and surveillance

A Take Back Your Bytes lesson: what is wrong with advertising trackers and surveillance, and what you can do about it. A 50-minute lesson with a lab, a hands-on audit and discussion.

Series	Take Back Your Bytes, PrivacySafe Foundation's cybersecurity education campaign ^[17]
Audience	Teens and adults. No technical background needed. Adapt the language for younger learners.
Length	50 minutes, with a 30-minute cut
Format	4 slides, live tracker lab, 4 slides, hands-on audit, discussion
You will need	Slides (light for print, dark for projecting), the tracker lab page, flash cards, and learners' own devices if they choose to take part
Facts checked	October 27, 2026. Tools, browsers and phone menus change. Re-check before you teach.

PrivacySafe Foundation, Inc. | Take Back Your Bytes | These materials are dedicated to the public domain under CC0 1.0 and shared for the public good. The PrivacySafe and PrivacySafe Foundation names and logos are trademarks and are not included in that dedication. Names of other products and projects belong to their owners and are used as examples.

The lesson in five sentences

1. Many websites and apps send information about you to outside companies through cookies, pixels, fingerprinting, app tracker code and advertising IDs, and the pieces are combined into profiles^[1].
2. The harms are real but varied: loss of privacy, scams and malware carried by ads, manipulation, little real control, risks for young people, and the everyday cost of heavier pages^{[1][2][3][4]}.
3. No single tool fixes this. List-based blockers, behavior-learning blockers, built-in browser protection, a search that does not build a profile and app tracker reports each help in different ways and have limits^{[5][7][11][14]}.
4. Reports and blockers can be wrong or incomplete: finding tracker code is not proof it is active, and blocking more can break sites^[11].
5. Choose a mix that fits your browser, phone and needs, install tools only from official sources, and review them regularly, because tools and settings change.

LEARNING OUTCOMES

By the end, students can:

1. Explain how identifiers, third-party requests and profiles let companies track people across sites and apps^[1].
2. Describe at least four harms and one fair counterpoint, such as ads funding free sites.
3. Compare list-based and behavior-learning blockers, and say what each can miss^{[5][7]}.
4. Read an app tracker report and say what it does and does not show^[11].
5. Write a short, realistic personal plan for browser, search, phone and habits.

Session plan

SEGMENT	MINUTES	NOTES
Before the demo, slides 1 to 4	12	Includes the prediction: how many requests go to outside companies.
Tracker lab	12	Sections 1 to 4. Section 5 feeds the hands-on audit.
After the demo, slides 1 to 4	10	Blockers, search, phones, plan.
Hands-on audit	10	Learners choose one audit. Taking part is optional.
Discussion	6	Two questions.

30-MINUTE CUT

Skip the hands-on audit and show one audit on the instructor device. In the lab, do sections 1, 3 and 5. Cover after-demo slides 1 and 3. Use one discussion question.

Before class

- ☐ Optional: the lesson page has a walkthrough video of under five minutes, in a light version for the page and a dark version for projecting, each with a subtitles file. Play it as a recap, or share it with learners who missed the session. Check that it plays on the room computer first.
- ☐ Open the lab page and try each section. Set browser zoom to about 125% for the back row.
- ☐ **Check device policy.** Learners should not install extensions or change settings on school or work devices without permission. Offer a demo on the instructor device for anyone who cannot or does not want to take part.
- ☐ **Think about minors.** Follow your organization's rules on parental permission and on accounts and app installs. Do not require learners to share which apps they use. Use the made-up examples in the lab for anything that goes on the screen.
- ☐ Read the current pages for each named tool, because browser support and menus change^{[5][6][7][11][16]}.
- ☐ Prepare one news page you are comfortable projecting for the hands-on audit demonstration.
- ☐ Print the flash cards, double-sided, flipped on the long edge.

TEACH IT FAIRLY

- **Tools are examples, not endorsements.** Present uBlock Origin, Privacy Badger and Exodus Privacy as examples of kinds of tools. Others exist, and learners may choose differently.
- **Disclose the affiliation.** PrivacySafe Search is run by the same Foundation that publishes this lesson. Say so, offer it as one option, and teach learners how to compare search services: who runs it, what the privacy policy says, and what trade-offs come with it^[14].
- **Be fair to publishers.** Advertising pays for much of the web. Blocking ads reduces income for sites people value. Discuss supporting them in other ways.
- **Avoid fear and absolutes.** Not every ad or use of data is harmful. The concern is scale, secrecy and lack of choice^[3].

WHAT THE LAB IS, AND IS NOT

Every site, company and app in the lab is made up, and the lab runs in the browser and sends none of your choices anywhere. Request lists, sizes and blocking results are teaching illustrations, not measurements of real sites or tools. Real blockers and browsers differ in what they block. The learning-blocker simulation uses the three-site rule that Privacy Badger describes^[7], and some tools also ship with results learned in advance. Use the exercise in the guide to check real pages.

Slide notes: before the demo

Slide 1: Title

about 2 min

SAY

Who is watching what you read, search and tap? Our promise: plain facts and steps you can take today. Our job: see the trackers, understand the harms, and choose tools and habits that fit you. The four-segment bar is the plan: browser, search, apps, habits.

DO

Introduce Take Back Your Bytes as the Foundation's cybersecurity education campaign^[17].

CHECK FOR UNDERSTANDING

Ask: "Have you ever searched for something and then seen ads about it everywhere? What did you think happened?"

Slide 2: How tracking works

about 4 min

SAY

1. **Identify:** a cookie, a device detail or an advertising ID marks you.
2. **Collect:** pages and apps send what you view and tap, and where you are.
3. **Combine:** ad companies and data brokers join the pieces into a profile.
4. **Use:** ads and offers are chosen for the profile.

Methods: third-party cookies and pixels, fingerprinting, tracker code in apps, the advertising ID, and data brokers^{[1][16]}. Many free services are paid for by advertising that runs on data about you.

DO

Draw the four steps. Point out that you did not visit most of the companies that collect the data.

CHECK FOR UNDERSTANDING

Ask: "What is the difference between the site you chose to visit and the companies that load on it?"
First party and third party.

WATCH FOR

Do not claim that every cookie is a tracker. Cookies keep you signed in, too. The concern is third parties following you across sites.

Slide 3: What is wrong with it

about 4 min

SAY

- **Privacy:** detailed profiles built without a clear choice^{[1][3]}.
- **Security:** criminals buy ads to impersonate brands, and the FBI advises checking the URL and using an ad blocking extension when searching^[4].
- **Manipulation:** messages aimed at moments of worry or weakness.

- **Little control:** consent pop-ups and hidden settings.
- **Young people:** data collected from children and teens, with concerns about weak protections^[3].
- **Everyday cost:** heavier pages, slower loading, more battery and data use.

DO

Give one concrete example for each, and ask the room for others.

CHECK FOR UNDERSTANDING

Ask: "Which of these matters most to you, and why?" Different answers are good.

WATCH FOR

The FBI notes that search ads are not malicious in themselves. The risk is criminals abusing them^[4]. Keep that precision. Also stress the fair counterpoint: not every ad or use of data is harmful.

Slide 4: What to watch for, and the prediction

about 2 min

SAY

On the web: which requests go to outside companies, what each learns, what blockers stop and miss, what breaks, and what a search reveals. On your phone: trackers found in code, permissions, why a report is not proof, the advertising ID, and questions to ask before installing.

DO

Read the prediction: "When you open a news article, how many of its requests go to companies other than the site itself?" Give 60 seconds. Collect numbers.

WATCH FOR

Learners may think of only the ads they see. Many requests are invisible.

Tracker lab script (about 12 minutes)

Section 1: Open a page

5 min

SAY

Choose "A news article" with "No protection". The page makes **28 requests, 21 of them to outside companies**, including 10 that are tracking or advertising companies, and nine kinds of data are shared. Read the Shares column aloud for a few rows. Compare with the prediction. Then switch protection: the browser's built-in protection blocks 9, the list-based blocker 16, and the behavior-learning blocker 14.

DO

Turn on Strict for the list-based blocker: it blocks 18 and the note lists what may break (fonts, share buttons). Turn on the Global Privacy Control signal: it blocks nothing, and the note shows how many companies say they honor it^{[9][10]}. Try the shop and the recipe blog.

CHECK FOR UNDERSTANDING

Ask: "What did each protection miss, and why?" The list misses an unlisted tracker, the learner misses one it has not yet seen on three sites^{[5][7]}.

WATCH FOR

The numbers are made up for teaching. Do not present them as typical figures. Use the hands-on audit to count real pages. Also note that the uBlock Origin project advises against running other similar blockers beside it^[5].

Section 2: How a learning blocker decides

2 min

SAY

Click "Visit next site" five times. The learner counts, for each outside company, on how many sites it appears to track you. At three it blocks. A company that appears on five sites but does not track stays allowed. Turn on "start with trackers learned in advance" to show tools that ship with results^[7].

CHECK FOR UNDERSTANDING

Ask: "What could go wrong with a rule like this?" Missed trackers, false alarms, and a tracker that appears on only two sites.

Section 3: Read an app tracker report

3 min

SAY

Pick "BrightBeam Flashlight (example)": six trackers and permissions that do not fit a flashlight. Compare with "Plain Notes (example)" with none. Exodus Privacy's reports list tracker code found by static analysis and the permissions an app asks for^{[11][12][13]}.

DO

Read the questions to ask. Then read the limits under the report.

CHECK FOR UNDERSTANDING

Ask: "If a report finds a tracker, does it prove my data was sent?" No. It says tracker code is present, "not a proof of activity"^[11].

WATCH FOR

Do not say an app with trackers is spying on the user, or that an app with none is safe. Reports can miss unknown trackers, and permissions listed are requests, not always grants.

Section 4: What a search reveals

1 min

SAY

Toggle "signed in" and "cookies allowed" in the left column. In the right column, a metasearch engine sends your query on to other search engines on your behalf, and says it does not store search data or build a profile^{[14][15]}. Results can be less personalized, and you trust the operator.

CHECK FOR UNDERSTANDING

Ask: "What would you want to check before switching search engines?" Who runs it, the privacy policy, and whether results meet your needs.

Section 5: Make your plan

1 min

SAY

Choose a device and browser. The page builds a short checklist: today, this week, every few months. Learners can tick items and copy the plan. Point out that extension support differs by browser^[6].

DO

Hand over to the hands-on audit.

Close the prediction

1 min

SAY

On the example news page, 21 of 28 requests went to outside companies. Real pages differ, which is why we check our own.

DO

Return to slide 4 and compare numbers.

Slide notes: after the demo

Slide 1: Block trackers in your browser

about 3 min

SAY

KIND	EXAMPLE	POINTS TO TEACH
List-based content blocker	uBlock Origin ^[5]	Free and open source. A wide-spectrum blocker that uses filter lists. Browser support differs: after Chrome's move to Manifest V3, Chrome offers only a reduced "Lite" version, while some other browsers still support the full one ^[6] . Check the current status.
Behavior-learning blocker	Privacy Badger ^{[7][8]}	From the EFF, free and open source. Learns which outside companies track you across sites and blocks one after it sees it on three sites. Also sends the Global Privacy Control signal ^[7] .

DO

Teach criteria for any tool: who maintains it, is it open source, what permissions does it ask for, does it update, where do you get it. Privacy Badger's own FAQ warns that its permission prompt reads "access your data for all websites" and that you should install extensions only from organizations you trust^[7].

CHECK FOR UNDERSTANDING

Ask: "Why does a blocker need to read data on every site?" To see and stop requests, which is also why trust matters.

WATCH FOR

Do not tell learners to stack many blockers. Overlapping tools can conflict^[5]. Do not call any tool "the best".

Slide 2: Search without a profile

about 3 min

SAY

A profile-based search keeps your words with your history, records your IP address and device details, uses cookies or an account to recognize you, and personalizes results. A metasearch engine such as PrivacySafe Search sends your query to other search engines on your behalf, is hosted in Iceland, is built on SearXNG, has public source code, and says it does not generate a profile about you. Its own About page says results may be less personalized^{[14][15]}.

DO

Disclose that the Foundation operates PrivacySafe Search. Say that it is one option, and show how to compare.

CHECK FOR UNDERSTANDING

Ask: "What are the trade-offs of switching?" Less personalization, different results, and trust in a different operator.

WATCH FOR

Avoid claiming it makes you anonymous. A search service is one part of a larger picture.

Slide 3: Phones: apps and advertising IDs

about 4 min

SAY

Exodus Privacy is a French non-profit. Its platform analyzes Android apps and lists the tracker code and permissions found. Its Android app checks the apps already on your phone^{[11][12][13]}. Counts are colored: no trackers green, fewer than five yellow, five or more red^[11]. It uses static analysis, so it finds tracker code but cannot show whether it runs. Android lets you delete the advertising ID in Settings, Privacy, Ads, and menus vary by phone^[16]. On iPhone, use the Tracking setting in Privacy settings.

DO

Show an Exodus report for a real app of your choosing, if you have checked it first.

CHECK FOR UNDERSTANDING

Ask: "What would you do after seeing six trackers in a flashlight app?" Check permissions, look for alternatives, contact the developer, or remove it.

WATCH FOR

Exodus covers Android apps. Do not suggest it works on iPhone. Static analysis has limits, so present reports as a starting point.

Slide 4: Your take-back plan

about 4 min

SAY

1. See what loads on pages you visit.
2. Choose a blocker for your browser and install it from the official source.
3. Check its permissions and who maintains it.
4. Turn on tracking protection and Global Privacy Control^{[9][10]}.
5. Try a search engine that does not build a profile.
6. Check phone apps and delete the advertising ID.
7. Remove apps and sign-ins you do not use.
8. Review again in three months.

DO

Say that the Global Privacy Control is a request, not a block. In California, the Attorney General's position is that businesses must treat it as an opt-out request, and rules differ elsewhere^[10].

Hands-on audit (about 10 minutes)

Learners choose one audit. Taking part is optional, and nobody has to show their own devices or app lists.

1. **Count requests (computer).** Open a news page. Open the browser's developer tools and the Network tab, reload, and look at the Domain column. Count the domains that are not the site's own. Compare with your prediction.
2. **Check a blocker's counter (computer).** If you already use a blocker, note how many items it blocked on that page. If not, look at your browser's own tracking panel or privacy report.
3. **Check one app (phone).** On Android, look up one app at the Exodus Privacy report site or with its Android app and note its tracker count and permissions^{[12][13]}. On iPhone, open the app's privacy label in the App Store.
4. **Change one setting.** Delete or reset your advertising ID^[16], or turn on tracking protection. Note what you changed.
5. **Try a search.** Run the same search on your usual search engine and on a search without a profile. Compare the results and note what feels different.

TROUBLESHOOTING

- The Network tab shows many requests. Filter by the Domain column or sort by it, then count the unfamiliar ones.
- The extension is not available for a browser. Availability differs by browser^[6]. Use built-in protection instead.
- An app is not in the Exodus database. Check the platform's FAQ about analyzing new apps^[11].
- A blocked page breaks. Turn the blocker off for that site, or reduce its strength.

Discussion (about 6 minutes)

QUESTION 1: WHOSE JOB IS IT?

"Whose job is it to protect your privacy: you, companies or lawmakers? What could your school or workplace do?"

- Individuals can act, but it should not all fall on them.
- Companies can collect less and be clear. Laws and regulators set limits^{[3][10]}.
- Schools and workplaces can set device policies, teach, and choose tools thoughtfully.

QUESTION 2: WEIGHING THE TRADE-OFF

"Blocking ads can cut income for sites you value. How do you weigh that, and what else could you do to support them?"

- Many sites rely on ads. Others have found other models, such as subscriptions or donations.
- Options: pay or donate, allow ads on sites you trust, choose sites with less tracking, or block only trackers.
- There is no single right answer. Respect different views.

Answer key and assessment

QUESTION	ANSWER
What is a third party?	A company other than the site or app you chose, whose code or content loads on it ^[1] .
Name three ways trackers identify you.	Cookies, fingerprinting, app tracker code, advertising IDs ^{[1][16]} .
Why can ads be a security risk?	Criminals buy ads to impersonate brands and lead to malicious sites ^[4] .
How does a learning blocker decide?	It blocks a company it sees tracking across three sites ^[7] .
Does an Exodus report prove data was sent?	No. It shows tracker code is present ^[11] .
How do you delete an Android advertising ID?	Settings, Privacy, Ads, Delete advertising ID. Menus vary ^[16] .

EXIT TICKET (3 MINUTES)

1. Name one harm of tracking and one fair counterpoint.
2. Name one thing a blocker can miss.
3. Write one action you will take this week.

HOMEWORK

- Complete your plan from section 5 and report which steps you did and what you learned.
- Pick one tool named in the lesson. Read its own page and write three sentences on who maintains it, what it does and one limit.
- Stretch: ask someone at home how they handle ads and privacy, and share one idea.

Common questions and misconceptions

QUESTION OR BELIEF	RESPONSE
"Private browsing stops tracking."	It mainly stops your own device from saving history. Sites, networks and trackers can still see your activity.
"An ad blocker makes me anonymous."	No. It stops some requests. Other signals, such as your IP address, remain.
"If I have nothing to hide, I do not need privacy."	Privacy protects you from scams, manipulation, discrimination and leaks, not only from embarrassment ^{[1][3]} .
"A tracker in a report means my data was stolen."	It means tracker code is present. Check permissions and what the app does ^[11] .

"Free tools are always safe."

Extensions can read what you do on every site. Install from official sources and trust the maintainer^[7].

"Opting out online fixes it."

Opt-outs and signals help, but they depend on companies and laws^{[9][10]}.

References and further reading

Citations in this guide use bracketed numbers. Links were checked on October 27, 2026. Browser support, menus and tool features change, so confirm details before you teach.

#	SOURCE	WHAT IT SUPPORTS
[1]	Electronic Frontier Foundation, Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance https://www.eff.org/wp/behind-the-one-way-mirror	How third-party tracking, pixels, fingerprinting and data sharing work, with tips for users.
[2]	Electronic Frontier Foundation, FTC Report Confirms: Commercial Surveillance is Out of Control https://www.eff.org/deeplinks/2024/09/ftc-report-confirms-commercial-surveillance-out-of-control	A summary of the FTC's 2024 findings on data collection by large platforms.
[3]	U.S. Federal Trade Commission, A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services (staff report, September 2024) https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services	Findings on data collection, retention, sharing and protections for teens.
[4]	FBI Internet Crime Complaint Center, Public Service Announcement PSA221221 https://www.ic3.gov/PSA/2022/PSA221221	Criminals buying search ads to impersonate brands, and the advice to check URLs and to use an ad blocking extension when searching.
[5]	uBlock Origin on GitHub https://github.com/gorhill/uBlock	A free, open-source, wide-spectrum content blocker that uses filter lists. Advises against stacking similar blockers.
[6]	Wikipedia, uBlock Origin https://en.wikipedia.org/wiki/UBlock_Origin	Background, and how Manifest V3 changed browser support, including the reduced uBlock Origin Lite.
[7]	Privacy Badger (Electronic Frontier Foundation) https://privacybadger.org/	How it learns to block trackers, the three-site rule, Global Privacy Control, and its extension permissions.
[8]	Privacy Badger source code on GitHub https://github.com/EFForg/privacybadger	License (GPL) and the description of what it sends and blocks.
[9]	Global Privacy Control https://globalprivacycontrol.org/	The browser signal for opting out of the sale or sharing of personal data.
[10]	California Attorney General, announcement of the Sephora settlement as part of ongoing CCPA enforcement https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement	California's position that businesses must honor user-enabled global privacy controls.

[11]	Exodus Privacy, Frequently Asked Questions https://exodus-privacy.eu.org/en/page/faq	Static analysis of APKs, matching against a list of trackers, "not a proof of activity", and the tracker and permission count colors.
[12]	Exodus Privacy, report platform https://reports.exodus-privacy.eu.org/	Searchable reports listing trackers and permissions found in Android apps.
[13]	Exodus Android app on F-Droid https://f-droid.org/app/org.eu.exodus_privacy.exodusprivacy	The app that shows trackers and permissions for apps installed on a phone.
[14]	PrivacySafe Search, About https://privacysafe.is/info/en/about	The service's description: hosted in Iceland, built on SearXNG, does not generate a profile, results may be less personalized.
[15]	SearXNG documentation https://docs.searxng.org/	How the metasearch engine software works.
[16]	Google, Play Console Help: Advertising ID https://support.google.com/googleplay/android-developer/answer/6048248	Resetting or deleting the Android advertising ID in Settings, Privacy, Ads.
[17]	PrivacySafe Foundation https://privacysafe.foundation/	The Take Back Your Bytes education campaign and the Foundation's other work.
[18]	Creative Commons, CC0 1.0 Universal https://creativecommons.org/publicdomain/zero/1.0/	The public-domain dedication that covers these lesson materials.

ABOUT THESE MATERIALS

The slides, lab, flash cards and this guide were written for the PrivacySafe Foundation's Take Back Your Bytes campaign. They are dedicated to the public domain under CC0 1.0^[18]. The Foundation names and logos are trademarks and are not included in that dedication. The tools named in the lesson are examples. This lesson is independent of the projects and organizations named in the references.