READING & WRITING ASSIGNMENTS

Data Literacy & Privacy

One theme - four different reading options.

In this packet (suggested pairings):

- **AP Computer Science Principles**
  Who's Watching the Road? (Flock Cameras)
- **AP Computer Science A**
  What Are You Worth? (Data Brokers)
- **Cybersecurity**
  The School Is Watching (Student Monitoring)
- **Independent Study**
  The Data You Can't Take Back (23andMe)

Each assignment shares the same spine: a specific story, the broader concept, at least four of your own sources, tiered questions, and an optional for/against debate.

READING & WRITING ASSIGNMENT

Who's Watching the Road?

Flock Cameras, Surveillance, and the Price of Being Tracked

The Story That Started This

Something dominating my newsfeed recently is the Flock Camera. I discovered my first one while I was driving around Houston a few weeks ago. Small, boxy, with a little solar panel on top, and pointed straight at the road. And once I'd seen one, I couldn't stop noticing them: by the on-ramp, outside the grocery store, at the entrance to a neighborhood.

I was reading the news and saw a story out of Dayton, Ohio where city workers there had gone around and covered 72 of their own police cameras - the same Flock cameras - with *trash bags*. Not because they were broken, but because an audit found the city's camera data had been accessed and searched more than 7,100 times for immigration enforcement, which the city's own policy flatly forbade. The contract the city had signed gave them no clean way to switch the Flock system off, and so the workers reached for trash bags.

I keep thinking about the cameras I drive past in my local community. Who can search where I've been? Under what rules? And what happens when nobody's actually checking?

Who watches the watchers?

The Bigger Idea

A Flock camera is an **automated license plate reader (ALPR)**. Every time a car passes, it photographs the plate, converts it to text, and stores the plate number, the location, and the exact time in a searchable database. Newer models also log a car's make, model, color, bumper stickers, even scratches - all of these things can form a "vehicle signature" that can pick you out with no plate at all.

One photo of one car seems harmless. But billions of scans a month, connected across a national network, become something else entirely: a searchable map of where ordinary people go, when, and how often. Police can run nationwide searches. For example, in one seven-month stretch, San Francisco's Flock database was queried more than 1.6 million times by outside and federal agencies - including the FBI, ICE, and CBP.

Supporters say ALPRs solve real crimes: stolen cars, Amber Alerts, hit-and-runs. Critics - the ACLU and EFF among them - say a system that tracks everyone to catch a few is mass surveillance, and point to officers who've misused it to stalk exes or monitor protesters. Both of those can be true at the same time - and therein lies the tension.

A Question From Across the World

Here's something that doesn't quite sit well with me.

For over a decade, plenty of people in the West - journalists, politicians, privacy advocates - pointed at China as the cautionary tale. Hundreds of millions of cameras. Facial recognition that can find one face in a crowd. A government that can map where you go, who you meet, what you do, and give you a social credit score that dictates what you are allowed to do. We called it dystopian. We called it authoritarian overreach and a gross invasion of privacy. *That could never happen here*, or so the story went.

Now there are more than 100,000 Flock cameras logging American drivers, and that data has been searched millions of times by agencies including ICE and the FBI - sometimes against the local rules that were supposed to govern it. The tech isn't identical: plates instead of faces. But the underlying question is the same one we asked about China: how much of an ordinary person's movement should be automatically recorded and searchable - and by whom?

You don't have to land where I might. But you do have to wrestle with the comparison.

Step 1 - Read

Start with these three. The first is the trash-bag story; the second explains how the technology actually works; the third is Flock's own defense of its product.

- **The trash-bag story (Fortune)** - why Ohio city workers covered their own cameras.
  https://fortune.com/2026/06/03/why-are-ohio-city-workers-covering-flock-cameras-immigration-enforcement-data-sharing-policy-violations/

- **How they work (Malwarebytes)** - "What the Flock is happening with license plate readers?"
  https://www.malwarebytes.com/blog/privacy/2025/11/what-the-flock-is-happening-with-license-plate-readers

- **The company's case (Flock Safety)** - how Flock describes its own product.
  https://www.flocksafety.com/products/license-plate-readers

Step 2 - Research on Your Own

Find **at least four more** reputable sources on ALPRs or Flock that you dig up yourself. News outlets, the ACLU, the EFF, court filings, or your own city's camera policy all count. Random social-media posts do not. You'll need to cite these in your paper (and lean on them if we debate).

Step 3 - Written Response

Turn in a typed paper. Answer in complete sentences. Point values are shown; total is **25 points**.

Comprehension

1. What is an ALPR, and exactly what does a Flock camera capture and store about a passing car? (1 pts)

2. Why did Dayton officials resort to trash bags instead of just switching the cameras off? What does that reveal about the contracts cities sign? (1 pts)

Analysis

1. Who benefits from this system, and who bears the risk? Name at least two groups on each side and explain each. (3 pts)

2. Data collected to "find stolen cars" ended up searched by ICE, the FBI, and CBP over a million times. Why does data gathered for one purpose so often get used for others, and what does that tell you about how collected data behaves over time? (3 pts)

3. What are some historical, non-Flock examples of data being collected and falling into the wrong hands? What is a possible consequence of this Flock data falling into the wrong hands? (3 pts)

4. For years the West called China's camera-and-facial-recognition surveillance authoritarian over-reach and an invasion of privacy. Compare that system with a nationwide network of ALPRs here at home. What is genuinely different, and what is uncomfortably similar? Use evidence. (4 pts)

Position

Take a clear position on the resolution below and argue it - this is the required part.

1. Where do you stand on the resolution? Argue your side using evidence from at least two of the sources you found, then fairly state the single strongest argument against your view and respond to it. (10 pts)

(OPTIONAL) Prepare Both Sides

Your teacher may ask you to be ready to argue *either* side. If so, also prepare a short case for each:

1. The strongest case **FOR** the resolution, backed by evidence you found yourself.

2. The strongest case **AGAINST** the resolution, backed by evidence you found yourself.

Step 4 - (OPTIONAL) Class Debate

Resolved: *"Our community should ban automated license-plate reader cameras like Flock."*

If your teacher runs the debate, you'll defend a position on this resolution, and you may be **assigned a side at random** - which is why the optional prep above asks you to be ready for both. (You won't have your paper or notes with you, so know your evidence well enough to argue from memory.)

Two rules make the debate work:

1. Evidence only. Every claim points to a specific source for evidence, not a feeling.

2. Steelman first. Before you rebut the other side, restate their strongest argument fairly enough that they'd nod along. Then tell your tale.

One More Thing

What you learn in this class is about the world you actually live in. These cameras are real, some of them are probably in your neighborhood, and the people deciding how they get used are making choices you are fully capable of understanding and weighing in on. So go ahead and weigh in on it - that's the whole point.

And on length of paper (since someone always asks): some people say a lot with a little, and others can go on and on with superfluous, over-adjectived sentences and end up saying almost nothing. Which one are you currently? *Let's strive towards working for the first kind.*

READING & WRITING ASSIGNMENT

What Are You Worth?

Data Brokers and the Price of a Person

The Story That Started This

Have you ever searched for a product, or clicked on an ad, and it seems to follow you everywhere? A few months ago I signed up for a clothing company's newsletter. Now, it seems like that company follows me everywhere: my email, Google Ads, Instagram Ads, ads within a game. That part everybody notices. What most people never think about is the quieter machine behind it: an entire industry whose whole business is buying, packaging, and selling information about you, usually without you ever hearing its name.

The one that made me sit up was a company called **Kochava**. In 2022 the Federal Trade Commission sued it for selling precise location data from hundreds of millions of phones - data specific enough to trace a person's visits to a reproductive health clinic, a place of worship, or a domestic-violence shelter. Kochava pulled that location data through little bundles of code (SDKs) installed in more than 10,000 apps. In May 2026 the FTC finally reached a settlement. You had probably never heard of Kochava - Kochava had heard plenty about you.

The Bigger Idea

A **data broker** is a company that collects information about people and sells it - to advertisers, insurers, landlords, employers, even the government. You are rarely their customer; you are their product. They stitch together your app activity, purchases, public records, and location into a profile, then sell access to it. The global data-broker industry was valued at roughly $277 billion in 2024.

Here's the part that matters: none of this is magic. Your "profile" is really just a bundle of records tied to your name, and "selling" it just means letting a paying stranger look. It's ordinary, old-school detective work - the kind of files a private investigator once built on a single person - now done automatically on millions of people at once, and opened up for millions more to search.

Why This Is Tricky

It's easy to say "ban it," but data brokers also power things people like: fraud detection that flags a stolen credit card, background checks, the free apps you use precisely because someone else pays for them with your data. The difficult question isn't whether data is useful - it obviously is - it's who gets to decide when your information becomes a product, and whether "I clicked Agree once" should count as a yes forever.

Step 1 - Read

The first two explain the problem and the Kochava case; the third is a law firm's more business-friendly read on the same settlement, so you hear how the industry frames it. The fourth is a podcast episode on other data brokers.

- **The Overview (The Conversation)** - "Data brokers know everything about you." https://theconversation.com/data-brokers-know-everything-about-you-what-ftc-case-against-ad-tech-giant-kochava-reveals-218232
- **The Case (FTC)** - the government's complaint against Kochava. https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other
- **The Industry's Perspective (White & Case)** - a law firm's "takeaways for businesses." https://www.whitecase.com/insight-alert/ftc-settles-data-broker-kochava-over-sale-sensitive-location-data-key-takeaways
- **Hieu: A Hacker's Perspective (Darknet Diaries)** - buying & selling information. https://darknetdiaries.com/transcript/162/

Step 2 - Research on Your Own

Find **at least four more** reputable sources you dig up yourself - news reporting, the FTC, a state privacy law (like California's CCPA), or a data broker's own site. Random social-media posts don't count. You'll need to cite these in your paper (and lean on them if we debate).

Step 3 - Written Response

Turn in a typed paper. Answer in complete sentences. Point values are shown; total is **25 points**.

Comprehension

1. In your own words, what is a data broker, and how did Kochava obtain the location data it sold? (1 pts)
2. Name three specific kinds of information a broker might combine to build a profile of you. (1 pts)

Analysis

1. Who benefits from the data-broker industry, and who bears the risk? Name at least two groups on each side and explain each. (2 pts)
2. A data broker builds and sells a profile of you without you ever seeing it happen. Explain how that profile gets assembled from scattered pieces of information and passed around. (3 pts)
3. How could data collection be made more visible; should it be? Do you think changing the visibility would help, hinder, or have no effect on the data collection process, and why? (3 pts)

4. Companies argue that clicking “I agree” is real consent. Do you think a one-time click should let a company sell your data forever? Make sure to support your position with evidence. (5 pts)

Position

Take a clear position on the resolution below and argue it - this is the required part.

1. Where do you stand on the resolution? Argue your side using evidence from at least two of the sources you found, then fairly state the single strongest argument against your view and respond to it. (10 pts)

(OPTIONAL) Prepare Both Sides

Your teacher may ask you to be ready to argue *either* side. If so, also prepare a short case for each:

1. The strongest case **FOR** the resolution, backed by evidence you found yourself.
2. The strongest case **AGAINST** the resolution, backed by evidence you found yourself.

Step 4 - (OPTIONAL) Class Debate

Resolved: *“Selling a person’s data should require their explicit, specific consent.”*

If your teacher runs the debate, you’ll defend a position on this resolution, and you may be **assigned a side at random** - which is why the optional prep above asks you to be ready for both. You won’t have your paper or notes with you, so know your evidence well enough to argue from memory.

Two rules make the debate work:

1. Evidence only. Every claim points to a specific source for evidence, not a feeling.

2. Steelman first. Before you rebut the other side, restate their strongest argument fairly enough that they’d nod along. Then tell your tale.

One More Thing

At some point in your life, you’ll almost certainly work with data. Data is neutral - it can power fraud detection or fuel surveillance. What decides the difference is the person choosing what to collect, what questions to ask, and what story to tell with the answers. That person is going to be you. Think on it.

READING & WRITING ASSIGNMENT

The School Is Watching

Student Monitoring, Safety, and Your Digital Privacy

The Story That Started This

This one is about you.

In Lawrence, Kansas, nine high school students sued their district in 2025. Their school used a monitoring tool called **Gaggle** that scans everything students do in their school accounts: emails, documents, images, attachments. According to the lawsuit, Gaggle intercepted student journalists' drafts before they could be published, seized original artwork off school accounts, and made mental-health emails to trusted teachers quietly disappear. The students argued the district had run illegal searches of their private work. The district stopped using Gaggle by the end of that school year.

Then it got worse. When reporters from The Seattle Times and The Associated Press investigated school surveillance, they were accidentally handed access to roughly **3,500 sensitive, unredacted student documents** - sitting online with no password and no firewall. The tool meant to keep students safe had become a data breach of its own.

The Bigger Idea

Software like Gaggle and GoGuardian works by scanning student accounts for keywords tied to "concerning behavior" - words like *suicide*, *self-harm*, *gun*, *bomb* - and flagging matches with a mix of AI and human reviewers. The goal is real and serious: catching a student in crisis before something terrible happens. Schools that use these tools can point to cases where they believe monitoring saved a life.

However, there is the other half of the story. Every one of those scans creates a copy of a student's private words, stored on someone else's servers. That store of data is a target. A keyword filter can't tell a suicide note from a poem, a threat from a history essay, an art project from contraband - so it over-flags, and humans you've never met read what you wrote. Safety and surveillance are running on the exact same wire - opposite sides of the same coin.

Why This Is Tricky

If monitoring stops even one tragedy, is that worth scanning tens of thousands of students who did nothing wrong? Does a school account belong to the school, to the student, or to both? And if the safety data itself leaks - as it already has - who's responsible? There's no clean answer here, which is exactly why it's worth arguing.

Step 1 - Read

The first two report what happened; the third explains why schools adopt these tools in the first place, so you hear the safety case in its own words.

- **Who's watching (EdSurge)** - "What Do We Know About the Edtech Services That Watch Students?"
  https://www.edsurge.com/news/2025-10-14-what-do-we-know-about-the-edtech-services-that-watch-students

- **A district pulls the plug (Lawrence Journal-World)** - why Lawrence dropped Gaggle.
  https://www2.ljworld.com/news/schools/2025/oct/29/lawrence-school-district-ceases-its-use-of-student-surveillance-software-gaggle/

- **The safety case (Christian Science Monitor)** - why schools use AI like Gaggle.
  https://www.csmonitor.com/USA/Education/2025/0312/ai-surveillance-schools-gaggle

Step 2 - Research on Your Own

Find **at least four more** reputable sources you dig up yourself - news reporting, your own district's technology policy, the ACLU or EFF, or a monitoring vendor's own site. Random social-media posts don't count. You'll need to cite these in your paper (and lean on them if we debate).

Step 3 - Written Response

Turn in a typed paper. Answer in complete sentences. Point values are shown; total is **25 points**.

Comprehension

1. How does a tool like Gaggle technically decide what to flag, and who reviews the flags? (2 pts)

2. What two separate harms showed up in these stories - one from the flagging itself, and one from how the data was stored? (2 pts)

Analysis

1. Who benefits from student monitoring, and who bears the risk? Name at least two groups on each side and explain each. (3 pts)

2. From a security standpoint, explain why collecting students' flagged messages creates a new attack surface - and what a breach of that data could expose. (3 pts)

3. A keyword filter can't tell a poem from a threat. Using an example, explain the cost of a false positive here, and why "better safe than sorry" isn't a free choice. (5 pts)

Position

Take a clear position on the resolution below and argue it - this is the required part.

1. Where do you stand on the resolution? Argue your side using evidence from at least two of the

sources you found, then fairly state the single strongest argument against your view and respond to it. (10 pts)

(OPTIONAL) **Prepare Both Sides**

Your teacher may ask you to be ready to argue *either* side. If so, also prepare a short case for each:

1. The strongest case **FOR** the resolution, backed by evidence you found yourself.
2. The strongest case **AGAINST** the resolution, backed by evidence you found yourself.

Step 4 - (OPTIONAL) **Class Debate**

Resolved: *"Schools should be allowed to monitor the contents of students' school accounts."*

If your teacher runs the debate, you'll defend a position on this resolution, and you may be **assigned a side at random** - which is why the optional prep above asks you to be ready for both. You won't have your paper or notes with you, so know your evidence well enough to argue from memory.

Two rules make the debate work:

1. Evidence only. Every claim points to a specific source for evidence, not a feeling.

2. Steelman first. Before you rebut the other side, restate their strongest argument fairly enough that they'd nod along. Then tell your tale.

One More Thing

Security is never just "lock everything down." Every safeguard has a cost - money, time, convenience - and the hardest calls in this field are the ones where the tools that protect people are the very same tools that can surveil them. What separates the two isn't the technology; it's intent, limits, and who is watching the watchers.

READING & WRITING ASSIGNMENT

The Data You Can't Take Back

23andMe, Bankruptcy, and Who Owns Your DNA

The Story That Started This

Millions of people spit into a little tube, mailed it off, and paid **23andMe** to tell them about their ancestry and health. It felt harmless - fun, even - as you could uncover your ethnic makeup or find a long-lost cousin. You can't get more personal than your own genome, but the company promised to keep it safe.

Then, in March 2025, 23andMe filed for bankruptcy. When a company that holds the DNA of **more than 15 million people** goes broke, what happens to the data - the DNA? Well, it became an asset for sale in court. The pharmaceutical company Regeneron won a bankruptcy auction to buy 23andMe for $256 million in May 2025. Then, in July 2025, a nonprofit led by the company's own co-founder ultimately completed the purchase instead. Along the way, several state attorneys general urged customers to delete their genetic data, and a court appointed an overseer just to watch how that data got handled.

You gave a company your entire DNA genome years ago. Now strangers in a courtroom are deciding what happens to it.

The Bigger Idea

Most data you generate is replaceable. Change a leaked password, cancel a stolen credit card, get a new phone number. Your genome is different: it's permanent, it's uniquely yours, and it's partly shared with your relatives - who never consented to anything. That makes genetic data a great test of a principle that lies central to data literacy: **data you hand over doesn't stay where you put it, and it outlives the promises made when you gave it up**.

23andMe's privacy policy always allowed for the possibility that the company - and its data - could change hands. Almost nobody read that far. When the business became the thing being sold, the customers' most permanent information came along with it, governed by whatever the new owner decides and whatever the law happens to require.

Why This Is Tricky

There's a real upside here: a giant genomic database can accelerate medical research and drug discovery in ways that help everyone, and most 23andMe customers actively consented to research use. So you have both the promise of future research breakthroughs and consent - this isn't a simple villain story. The hard questions are about consent and permanence: can you meaningfully agree to how your DNA will be used decades from now, by an owner who didn't exist when you signed up? And should genetic data be sellable in a bankruptcy at all?

Step 1 - Read

The first two report the sale and what it means for customers; the third is the acquiring company's own announcement, including its privacy commitments.

- **The sale (CNN Business)** - a bankrupt DNA firm changes hands for $256M.
  https://www.cnn.com/2025/05/19/business/regeneron-23-and-me
- **What it means (BioPharma Dive)** - the deal and the data behind it.
  https://www.biopharmadive.com/news/regeneron-23andme-acquire-bankruptcy-genetic-testing/748440/
- **The buyer's own words (Regeneron newsroom)** - the purchase agreement and privacy promises.
  https://newsroom.regeneron.com/news-releases/news-release-details/regeneron-enters-asset-purchase-agreement-acquire-23andmer-256

Step 2 - Research on Your Own

Find **at least four more** reputable sources you dig up yourself - news reporting, a state attorney general's guidance on deleting 23andMe data, 23andMe's own privacy policy, or scholarship on genetic privacy. Random social-media posts don't count. You'll need to cite these in your paper (and lean on them if we debate).

Step 3 - Written Response

Turn in a typed paper. Answer in complete sentences. Point values are shown; total is **25 points**.

Comprehension

1. What happened to 23andMe in 2025, and why did its bankruptcy raise alarms about customer DNA? (2 pts)
2. Why is genetic data different from a password or a credit card number when it comes to privacy risk? (2 pts)

Analysis

1. Who benefits from a large genomic database, and who bears the risk? Name at least two groups on each side and explain each. (3 pts)
2. Your DNA is partly shared with relatives who never signed up. What does that fact do to the usual idea of "individual consent"? (3 pts)
3. Should deeply personal data like a genome be allowed to be sold as an asset when a company goes bankrupt? Take a position and support it with evidence. (5 pts)

Position

Take a clear position on the resolution below and argue it - this is the required part.

1. Where do you stand on the resolution? Argue your side using evidence from at least two of the sources you found, then fairly state the single strongest argument against your view and respond to it. (10 pts)

(OPTIONAL) **Prepare Both Sides**

Your teacher may ask you to be ready to argue *either* side. If so, also prepare a short case for each:

1. The strongest case **FOR** the resolution, backed by evidence you found yourself.
2. The strongest case **AGAINST** the resolution, backed by evidence you found yourself.

Step 4 - (OPTIONAL) **Class Debate**

Resolved: *"Companies should be barred from selling customers' genetic data as an asset in bankruptcy."*

If your teacher runs the debate, you'll defend a position on this resolution, and you may be **assigned a side at random** - which is why the optional prep above asks you to be ready for both. You won't have your paper or notes with you, so know your evidence well enough to argue from memory.

Two rules make the debate work:

1. Evidence only. Every claim points to a specific source for evidence, not a feeling.

2. Steelman first. Before you rebut the other side, restate their strongest argument fairly enough that they'd nod along. Then tell your tale.

One More Thing

This is one of those questions that does yet not have a tidy answer. The law is still catching up to the fact that some data is permanent. Embrace the ambuigity and practice your critical thinking - the kind of thinking the world needs.