New Internet - Papers, Please!

Table of Contents

New Internet – Papers Please

Video Length: 19:38

Lesson Description

What if you needed to show your ID just to watch a video or join an online discussion? This video reveals how new laws and tech policies are transforming the internet from a place of openness into one of surveillance and control, and asks whether decentralized systems could protect privacy and freedom in the future.

Objectives

Students will be able to:

- identify examples from the video that show how governments and platforms are increasing online ID requirements.
- compare the stated goals of age verification laws with their potential risks to privacy and security.
- construct an argument about whether mandatory ID checks strengthen or weaken a free society.
- propose alternative models for the internet that could balance safety with personal freedom.

Concepts & Key Terms

Authoritarian: describing a system of government or control where power is concentrated in the hands of a few, and individual freedoms are limited.

Decentralization: the distribution of power and control across many independent users or systems instead of one central authority.

Jawboning: informal pressure from government officials on companies to act a certain way without passing a law.

KYC (Know Your Customer): rules that require companies to collect and verify personal information, such as IDs or addresses, from their users.

Surveillance: the monitoring of people’s actions, communications, or data, often by governments or large organizations.

Preview Activity

Use Think, Pair, Share to have students answer and discuss these preview questions: Have you ever had to show an ID or share personal information online? What do you think are the risks and benefits of giving personal data to websites or apps? Should people be allowed to use the internet anonymously, or should everyone have to prove who they are?

OR

Distribute copies of the K-W-L worksheet to the class. Have students fill in the K and W sections. After showing the video, have students complete the L section and answer the questions at the bottom of the worksheet.

Viewing Guide Instructions

We recommend that teachers show the video twice: first to allow students to view the video and focus on the issues presented, and second to allow them time to complete the viewing guide. After they complete the viewing guide, allow students a few minutes to work in pairs to share and verify answers.

Answers to Viewing Guide

1. different
2. private
3. safety
4. breached
5. IRS
6. minimize

New Internet – Papers Please

Viewing Guide

Name ___________________________ Date ________________________

Class ________________Period _____ Teacher ______________________

Directions: As you watch the video, fill in the blanks with the correct words.

1. If we want a ______________________ future, we have to move fast and start building on the version of the internet that puts people back in control.
2. It would require platforms to automatically scan all ______________________ messages, emails, and stored files.
3. Sometimes these changes are framed as anti-fraud measures or ______________________ features.
4. These databases are ______________________ constantly, and when they are, they don't just expose financial information.
5. Even the ______________________ has been hacked many times.
6. So, what is the path to safety? Well, we need to ______________________ what gets collected in the first place.

Take a few moments to reflect on the video and answer these questions.

1. What does the government gain by requiring ID for using apps and websites?

____

____

____

2. What rules would you design for the internet? Explain your reasoning.

____

____

____

____

Discussion & Analysis

1. What are some examples of ID checks on websites mentioned in the video?
2. What does KYC mean in the video?
3. How is today's internet different from the early internet?
4. Why might governments say they need age checks or ID rules?
5. How could data leaks from ID checks harm people?
6. What risks come with storing large amounts of personal information?
7. How does "jawboning" change the way companies make rules?
8. What are some similarities between surveillance laws in different countries?
9. Why might some people accept ID rules without protest?
10. How do these rules affect personal freedom online?
11. What is the video's main claim about privacy and safety?
12. What are the strongest arguments for and against mandatory ID checks?
13. How might decentralized systems make censorship harder? Is that a good thing or a bad thing? Explain your reasoning.
14. What kind of internet do you think would best balance safety and freedom?

Discuss These Lines from the Video

Show your papers is not a healthy default for a free society, especially not on a network that was originally designed for openness, collaboration, and the free exchange of information without gatekeepers.

This isn't really about protecting children. That's just the justification.

KYC isn't protection, it's exposure.

The safest database is the one that never existed.

Our greatest platform for free expression has become our greatest instrument of control.

Privacy isn't suspicious or criminal. It's normal.

Maybe we need to rethink the architecture of the internet itself and build something that doesn't rely on permission at all.

Quotes for Discussion

Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect. It is about choice, and having the power to control how you present yourself to the world. – Bruce Schneier

Anonymity is a shield from the tyranny of the majority.... It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation and their ideas from suppression at the hand of an intolerant society.
– U.S. Supreme Court, *McIntyre v. Ohio Elections*

Our Constitution does not guarantee us against search and seizure, only unreasonable search and seizure. And what's reasonable is a product of the totality of the circumstances in which we find ourselves. Privacy is the line we continually negotiate… – Michael Hayden

A world without privacy is less imaginative, less empathetic, less innovative, less human. At Apple, that is not the world we want to live in. We believe that privacy is a fundamental human right... – Tim Cook

I guess I think that this debate in the end is between the people who would rather have some kind of an automatic technological guarantee against the government misusing their authority and people who are prepared to trust our institutions to prevent abuse. – Stewart Baker

When we see governments and corporations working in concert, we begin to see the birth of a complex between the two where neither truly act independently, or adversarially, but rather they become the left and the right hand of the same body.
– Edward Snowden

By requiring users to upload their government-issued ID, bank account information, or credit card number to prove their age, these bills compromise our online privacy undermine the First Amendment's fundamental right to free expression and represent government overreach into our private lives.
– ACLU

Activities

1. Have students complete the K-W-L chart in class or for homework. (Recall that the K and W sections are to be completed before watching the video and the L section after watching the video.)

2. Have students complete the political cartoon activity in class or for homework.

3. Have students complete the PMI chart in class or for homework.

4. Have students complete and submit the Exit Ticket as they leave class.

5. Students make a simple chart showing examples from the video of platforms that require ID and the type of data they collect. This helps them identify details clearly.

6. In small groups, students create posters comparing the reasons governments give for ID checks with the risks to privacy mentioned in the video. Each group presents their poster.

7. Students write a one-page response about whether they think anonymity online is a right or a privilege, backing up their answer with at least two examples.

8. Pairs role-play a conversation: one is a government official arguing for ID checks, the other is a student concerned about privacy. Afterward, they switch sides.

9. Students research a recent real-world data breach and write a short news-style summary describing what happened and who was harmed.

10. Groups design a class debate on the statement: "Mandatory ID checks make society safer." Half argue for it, half argue against it.

11. Individually, students draw a cartoon or comic strip showing the dangers of personal data being stored online.

12. Each student writes a short persuasive paragraph on whether they would use a decentralized social media platform instead of a mainstream one, giving reasons.

13. Groups make a flowchart of the steps from small ID checks (like phone numbers) to today's larger ID demands, showing how normalization works.

14. Some students write a creative short story imagining a future internet where every action requires ID, some write a creative short story where the internet is decentralized. In class, read and compare the stories.

15. In groups, students design a new "Bill of Rights for the Internet" that includes protections for privacy, anonymity, and freedom of speech. Compare the results. What things did each group decide were important? What were unique ideas? Do the other groups think they should have included those unique ideas as well? Come up with one Bill of Rights for the Internet for the class. Is it hard to get consensus? Do groups compromise?

Name ___________________________ Date _____________________

Class ______________Period ______ Teacher ___________________

Quiz: New Internet – Papers Please

Directions: Select the answer that best completes the sentence.

1. The term jawboning describes ___________.
   - A. formal new laws
   - B. quiet government pressure
   - C. court decisions
   - D. election campaigns

2. The EU's "chat control" proposal would ___________.
   - A. block online ads
   - B. scan private messages
   - C. limit video length
   - D. remove search engines

3. A major risk of KYC databases is ___________.
   - A. faster fraud detection
   - B. loss of personal freedom
   - C. increased hacking threats
   - D. cheaper online services

4. Decentralized systems resist surveillance because ___________.
   - A. they rely on one server
   - B. they erase all data
   - C. control is widely shared
   - D. they ban encryption

5. The main idea of the video is ________________.
   - A. ID checks protect the web
   - B. surveillance threatens freedom
   - C. children need stronger filters
   - D. open internet is outdated

Answer Key:

1. B
2. B
3. C
4. C
5. B

Name ______________________ Date ______________________

Class _____________ Period _____ Teacher ______________________

New Internet – Papers Please

Political Cartoon Activity

Directions: Use the political cartoon to answer the questions.

What message does the cartoon send about the future of using the internet?

____

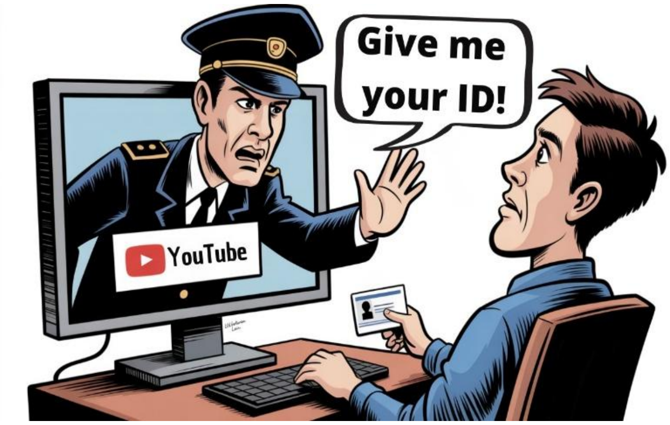
____

____

____

____

____



Why might the cartoonist choose a uniformed guard to represent online ID checks?

____

____

____

How could requiring ID for everyday internet use affect freedom of speech?

____

____

____

____

What are the pros and cons of websites collecting IDs and personal data?

____

____

____

____

____

Do you think the internet will be safer if everyone must provide ID to use it? Why or why not? ____

____

____

____

Name ______________________________ Date ________________________

Class __________________ Period _____ Teacher ____________________

New Internet – Papers Please

PMI Chart

P = Plus: What might be some positive effects of requiring ID to use websites and apps?
M = Minus: What might be some negative effects of requiring ID to use websites and apps?
I = Interesting: What is interesting or surprising about requiring ID to use websites and apps?

+ Plusses +	- Minuses -	I

How might data breaches be more dangerous when IDs and selfies are stored online? ______________________________________

____

____

____

Why might governments want to limit online anonymity, and what risks could that create for citizens? ________________________

____

____

____

Name ________________________________ Date __________________________

Class ___________________ Period ______ Teacher ______________________

New Internet – Papers Please

K-W-L Chart

Directions: Complete the **K** and **W** sections prior to watching the video. After you have seen the video, complete the **L** section and answer the questions below the K-W-L chart.

K	W	L
What I know about needing ID to use the internet…	What I want to know about needing ID to use the internet…	What I've learned about needing ID to use the internet…

How could requiring ID for every online action affect young people? ____

____

____

____

Do you agree or disagree with the idea of ID being required to use apps or websites? Explain your reasoning.

____

____

____

____

Exit Ticket

Name

Admit One

If the internet required ID for every action, would you feel more safe, less safe, or about the same? Why?

Admit One

EXIT TICKET

Name

Admit One

If the internet required ID for every action, would you feel more safe, less safe, or about the same? Why?

Admit One

EXIT TICKET

Name

Admit One

If the internet required ID for every action, would you feel more safe, less safe, or about the same? Why?

(Ctrl)

Admit One

EXIT TICKET

Transcript

Naomi Brockwell

I'm not sure if you've seen it, but over the past few weeks, one by one, platforms started rolling out mandatory age verification. Now, to listen to certain music on Spotify, you have to provide your government ID or biometric verification to a third party. To access certain Reddit communities, users must also verify their age through a third party, which involves submitting either a government ID, a selfie, or both, even for long-time users. To watch videos on YouTube, they'll be using AI systems that will calculate your age based on your behavior, viewing habits, and engagement history, and then restrict content based on what they deem suitable for you.

This sudden wave of ID checks across major platforms wasn't a coincidence. It was the result of a global wave of government mandates that just came to a head, marking the start of a new era for the internet. This isn't just a new login screen or a more annoying sign-up flow. It's a fundamental shift in how the internet works, transforming it from a system built on openness to one built on surveillance and control. We've quietly rewritten the terms under which people are allowed to access the digital world, and most people haven't even noticed it's happening.

In this video, we're going to look at the attack on privacy going on right now all over the world. We're going to look at how we got here and how we can change course quickly. Because the more these systems become normalized, the harder they'll be to undo. If we want a different future, we have to move fast and start building on the version of the internet that puts people back in control.

Let's start with the UK, where the Online Safety Act quietly changed the rules for what the internet is allowed to be. The law marks a fundamental shift. You now need to verify your identity simply to watch a video, share a website, or share your thoughts. It mandates strict age checks for any platform deemed to host harmful or adult content. But that definition is deliberately broad. It includes anything with user-generated content, which basically means every social media site, forum, messaging app, and video platform. Under this system, users are now being asked to submit government ID or facial scans just to browse, communicate, or participate online. The law passed in late 2023, but Ofcom, the UK's communications regulator, gave platforms until mid-2025 to implement these systems.

That's why we're seeing everything change now. A huge chunk of the internet has just been seized under the guise of safety, and the implications are enormous. We're normalizing identity checks just to participate online.

This isn't really about protecting children. That's just the justification. But what's being built is a system a system where anonymity is treated as a threat, and participation requires permission.

It's not just happening in the UK. In the past few weeks, governments around the world have begun moving in lockstep, each advancing their own surveillance regime in what feels like a sudden, synchronized wave. In Canada, Bill C2 was introduced. It expands surveillance powers to allow police warrantless access to your identity, login history, and online activity. It mandates backdoors in apps and platforms, giving authorities real-time access to user data and communications. In Australia, access to YouTube and social media is now banned for anyone under 16. The government mandated that you submit face scans and government IDs to use them, and they plan to expand these controls to search engines too, embedding identity checks into everyday browsing. In the European Union, a law known as chat control has been quietly advancing for years.

It would require platforms to automatically scan all private messages, emails, and stored files. This includes encrypted messages, which would effectively eliminate to end encryption across Europe. The proposal was first introduced in 2022, but the majority of EU member states opposed it and progress stalled. But then in 2024, Hungary took over the rotating presidency of the Council of the EU and used that position to bring the law back. A new version was introduced, and this time, Denmark backed it. Now, the law is headed for a final vote in October 2025. If it passes, it will enable mass surveillance across every major messaging platform in Europe.

In addition, the Digital Services Act in the EU requires certain platforms hosting user-generated content to implement strict age verification, giving companies a 12-month window to comply. In Switzerland, a new surveillance law would force VPNs, messaging apps, and online platforms to log user identities, IP addresses, and metadata for government access. Companies like Proton have announced that they will relocate if the law is passed. But to where?

In the US, dozens of states are pushing new laws that mirror these restrictions, forcing people to verify their identity, proof their age, and give their real name just to use basic online services.
That's why Spotify suddenly asking for your ID, and why YouTube is experimenting with AI-driven age enforcement, and why Reddit, Meta, Discord, and others are quietly preparing to roll out similar ID collection. Even in countries that don't legally require these measures, platforms are rolling out global policies anyway because it's simpler and cheaper to have a single policy everywhere. This forces every country into the same authoritarian policies, whether they wanted them or not.

This is the moment the internet changed forever, and it's chilling. We're yet to fully grasp what's ahead.

How did we get to a point where suddenly it became acceptable for governments to implement policies like these? None of it happened overnight. It required years of laying groundwork. Over time, we've seen platforms gradually introduce more identity checks. First, it's phone number verification, then it's government ID, then biometric metric scans. Sometimes these changes are framed as anti-fraud measures or safety features. But one reason they've become so common is quiet pressure from governments. They might tell the platform, we're worried about disinformation on your platform, or this app poses national security risks. You might want to address that before we're forced to take action.

This tactic is known as jawboning. It's informal, behind-the-scenes pressure from lawmakers and regulators. No new legislation is needed. A strong suggestion is often enough. What looks like voluntary compliance is often something else entirely.

Some people suggest that this sudden global crackdown on privacy must have been a coordinated and deliberate strike. Maybe. But a simple explanation is that the time was right. For years, platforms have slowly adopted these changes, which normalized the idea. Each small change felt minor and tolerable. So by the time governments introduce a legal mandate, almost no one pushes back. The norms have already shifted. The world was primed, and now a wave of regulation has swept in almost unopposed.

So what now? What does this shift actually mean for us? I mean, *show your papers* is not a healthy default for a free society, especially not on a network that was originally designed for openness, collaboration, and the free exchange of information without gatekeepers. But there's even more to be concerned about.

KYC is actually dangerous. KYC stands for know your customer. It was formalized in the Patriot Act as a standard for verifying financial accounts. Whenever people talk about KYC, we're always told it's essential to prevent fraud and keep us safe.

But we rarely talk about the other side of it, the liability that comes with collecting and storing this sensitive data. These databases are breached constantly, and when they are, they don't just expose financial information. They make people targets for harassment, extortion, or worse. KYC isn't protection, it's exposure.

Last month, we got a stark reminder of just how dangerous that exposure can be. There was a massive breach that the entire Internet was talking about.

NBC News
The Tea app announcing a massive data breach to their systems last week. Roughly 72,000 images, including verification selfies and images of government IDs, have been leaked online.

Naomi Brockwell
Tea was marketed as a dating safety app for women. In order to use the app, women were asked to verify their identity by uploading selfies and government IDs. It turns out that these files weren't properly secured. When the database was discovered, people all over the world began downloading and sharing its contents. Now, this was a controversial app. It was an information sharing site where women could warn other women about men that they dated, disclose abuse, protect others from catfish. But critics argued that the accusations blurred the line between caution and public shaming.

So when this data was breached, some saw the breach as ironic, even deserved.

Asmongold TV
That's 100% karma.

Naomi Brockwell
Many people started sharing the leaked documents as a form of retribution. But in the data were also the IP addresses of users, and these started to become shared also. And then people started to make maps showing exactly where these women lived. You might never have said anything nasty on the app and were simply using it because you worried about your safety. Now your face, government ID, and home address were all being eagerly shared.

Now, how you feel about the app isn't the takeaway here. It's that this data never should have been collected in the first place. What happened with Tea reflects a much larger issue that everyone is collecting this information without a second thought, even though none of them can keep it safe. It's putting people in danger. We've seen countless crypto related businesses get their databases hacked. As a result, there's been a surge in related kidnappings and extortion attempts across the world, as criminals now have the home addresses of those who own Bitcoin. There have been dating websites that collect real names and billing information that were hacked, and the user data leaked online.

People have been blackmailed and publicly outed because of this data. People have even taken their own lives in the aftermath of such breaches. Even the IRS has been hacked many times. And in one data breach, hundreds of thousands of taxpayers had their full financial history exposed, including income, employment records, home addresses, and family details.

This kind of information leads to devastating identity theft and fraud that can financially ruin people.

If we want a safer internet, we need to stop equating surveillance with security. Companies and government agencies claim that they're protecting you, but in reality, they're collecting sensitive data with almost no accountability. It's marketed as protection, but what it delivers is exposure. Users are rarely told where their data goes, how long it's kept, or who has access to it. Tea's own privacy policy stated in black and white, “selfies and government ID images will be deleted immediately following the completion of the verification process.” Yet here we are. Over 72,000 images are now circulating online, scraped from an open firebase bucket. This kind of betrayal is disturbingly common. Companies collect high-risk personal data and reassure users with vague promises. *We only keep it temporarily. We delete it right after verification. It's stored securely.*

These phrases are repeated often to make us feel better about handing over our most private information. But there's rarely any oversight and almost never any enforcement. At TSA checkpoints in the US, travelers are now being asked to scan their faces. The official line is that the images are deleted immediately. But how do we know? Who verifies that? There's no public access to these systems. No independent audit, no transparency. We're simply asked to trust. The truth is, we usually don't know where our data goes. Just for verification has become an excuse for massive data collection. Even if a company intends to delete your data, it still exists long enough to be copied, leaked, or stolen. Temporary storage is still storage. These breaches show how fragile these assurances really are.

These KYC pipelines now being mandated around the world are a perfect storm of risk. They collect extremely sensitive data, normalize handing it over, and operate behind a curtain of unverified claims. It's time to stop accepting, “Don't worry, it's safe,” as a substitute for actual security. If your platform requires storing sensitive personal data, that data becomes a liability the moment it's collected. The safest database is the one that never existed.

So what is the path to safety? Well, we need to minimize what gets collected in the first place. The internet was conceived as a tool for freedom and connection, but because of these choke points, it has rapidly descended into a surveillance dystopia where every click, view, and conversation is gated by ID checkpoints. Our greatest platform for free expression has become our greatest instrument of control.

We can't accept this shift passively. The normalization of mandatory identity verification is deeply harmful. Privacy isn't suspicious or criminal. It's normal, and we have to push back forcefully and unapologetically against this cultural change. On many platforms, we can still use pseudonyms. We can still fight to protect those rights, and we should. We should also challenge laws that mandate identity systems and challenge platforms that collect unnecessary identification data.

But ultimately, centrally controlled gatekeepers will always be weak points. They could be pressured by governments, regulators, and others to implement systems of censorship and control. Maybe the real solution is not to keep patching this system. Maybe we need to rethink the architecture of the internet itself and build something that doesn't rely on permission at all.

This means designing decentralized systems. Checkpoints only work when there's a central place to do the checking. They rely on platforms that can act as gatekeepers to content. These platforms become easy targets for governments to enforce identity checks, surveillance, and control. Decentralized infrastructure breaks that model. It distributes control across many independent participants, which makes it inherently resistant to coercion and significantly harder for governments to impose censorship.

This is why decentralization is not a fringe idea. It is a critical piece of the fight for online freedom. There are already some cool decentralized tools that you can explore, and we'll dive further into them in future videos. But just to name a few that are already gaining traction. Bitchat is a Bluetooth mesh messaging network that enables peer-to-peer communication among nearby devices without requiring internet access. Meshtastic uses small radio devices to create local mesh networks independent from the internet. Simplex is a serverless peer-to-peer messaging app with no identifiers or phone numbers required. IPFS is a distributed file storage system where instead of relying on centralized servers, files are split and stored across independent nodes, so there's no single point of failure. There are many decentralized social media platforms already out there, like Mastodon, Nostra, Blue sky, and Matrix.

These services don't yet have the reach of the major social media giants. In practice, most users still gather around a few popular nodes or relays. That can create new points of vulnerability. But even with these limitations, these platforms represent meaningful progress. I am genuinely optimistic about the future of decentralized social media. As more people learn to run their own servers and nodes, these networks will become stronger, more resilient, and much harder to censor.

So yes, the past few weeks have been scary. And yes, we've reached a major inflection point in the evolution of the internet. Control, surveillance, and censorship are now part of the infrastructure itself. Identification is the default. No ID, no entry. No selfie, no account.

KYC culture has spread far beyond finance into social platforms, community forums, and dating apps. But that doesn't mean we've lost. It means that a new fight has just begun. Decentralization and encryption disrupt the core mechanics of surveillance. They make it harder to monitor users, inject back doors, and enforce ID checkpoints. These tools are still growing, but we need them now. The more people who use them, the stronger they become, and the harder they are to shut down.

We need to build, support, and spread these alternatives. This is a landslide of lost freedoms, and it happened in mere weeks. This This transformation wasn't an accident. It was the inevitable result of complacency and quiet normalization. But it will become permanent if we don't resist. The best path forward is to re-imagine the internet, not as a landscape of check points and control, but as the free and open network it was always meant to be. It's time to move full speed into Internet 3. 0. The future is decentralized.

NBTV is a project of the Ludlow Institute, a nonprofit research and media institute dedicated to helping people reclaim ownership of their digital lives. If you found this video helpful, and if you want to see more content like this, or if you believe that privacy is worth fighting for, consider supporting our work. You can visit LudlowInstitute.org/donate to set up a monthly tax deductible donation. Your contributions help keep our content free, independent, and accessible to everyone. And if you want to support us in style, check out our merch shop. Every T-shirt, sticker, hoodie, helps fund our mission and lets the world know where you stand.