# How to protect yourself and your students from Zoom

A comprehensive layperson's guide to the tech ethics of online education for students, instructors, and administrators at all stages of the educational system

3rd Edition

(Last updated Nov 18, 2020)

# Introduction

## What is this document?

So your school or university has moved online because of the COVID-19 pandemic, and you're wondering about best practices for teaching online! Maybe your institution has already told you that you will be teaching class using Zoom, or another video conference software. It's great that your school is taking the COVID-19 pandemic and the need for social distancing seriously, and is trying to find technologies to help you teach your students at a distance. But in many of our conversations about best practices in online education, we haven't been talking much about cybersecurity, data ethics, or non-consensual surveillance. Zoom is a notoriously insecure software made by a privately owned company, and part of its business model involves collecting data on its users and then (very likely) selling that data to other private companies. Zoom's private ownership also has complete control over the platform and what can be hosted on it, giving them virtually unrestricted ability to monitor and censor Zoom classes and events. In this guide, I'll go through some of the major issues and risks of using Zoom (privacy concerns, accessibility, hacks and exploits, data mining, and surveillance) and make some suggestions about how you can protect yourself and your students from these dangers.

This guide is divided into a few sections. The first one, "Why Should I Be Worried About Zoom" explains some of the major issues with Zoom as a software and a company. The second section is aimed mostly at teachers, or anyone hosting online classes. The third section is aimed mostly at students, or anyone participating in online classes. The fourth section, "What Else Can I Do?" discusses some ways to take organized action to put pressure on Zoom to improve their policies. Though this guide is written specifically for people at schools using Zoom, a lot of the principles in it are also relevant to other video call setups.

I don't mean to argue here that no one should use Zoom ever. Online class - let's face it - is just not going to be as good as in person class, all ways of doing remote teaching will have major issues, and you might not be in a position to choose what software you use to teach your classes. But, even if it's the only choice, there are better and worse ways to Zoom, and there are still some things you should definitely not use Zoom for. Rather than tell you not to use Zoom at all, I wrote this guide to help you use Zoom safely, and to assist you in communicating about using Zoom in a way that respects your students' privacy and autonomy over their data.

Please share this document widely with your colleagues or fellow students. While many universities and schools are circulating tutorials about how to use Zoom for online teaching, most of those guides don't touch on cybersecurity, or the technological ethics of video-conferencing software, so it is up to us to make sure this information gets around.

## Who's Writing This?

This document was created by Mehitabel Glenhaber, currently a PhD student in Communications at USC Annenberg, and previously a Media Studies and Science, Technology, and Society researcher at MIT. As someone who's recently played both the student and instructor roles, I hope I can speak to the experiences from both sides of the classroom. Email me at glenhabe@usc.edu if you have questions about or additions to this document.

## Main Takeaways

A quick summary of the main points in this Guide

- Zoom is gaining a worrying monopoly over education - which fits into a standard pattern of "extend, engulf, extinguish" which internet mega-corporations use to create monopolies, eliminate competition, and jack up prices.
- Zoom has a history of censorship - both in service of world governments, and voluntarily - which poses serious threats to intellectual freedom.
- Zoom has a history of shady data practices. One company having access to the data of almost every teacher and student participating in online education during the coronavirus pandemic should scare you.
- Zoom has a history of privacy bugs, and, because the software is so popular, every hacker in the world has their eyes on it now. Even if you trust what Zoom will do with your data, you should not trust them to keep your data safe from other people who you trust even less.
- Remember that alternatives to Zoom exist: Jitsi, Discord, Microsoft Teams, Google Meet, Skype, Bluejeans, Cisco Webex, Slack, and many others. These platforms all have their own strengths and drawbacks, but Zoom is not your only choice!
- If you use Zoom, there is nothing you can do to 100% stop it from collecting data on you. But you can still take steps to control what data you give it, such as: using zoom in

browser rather than downloading it, turning off your camera whenever possible, or calling into Zoom meetings from a phone.

- If you use Zoom, there is nothing you can do to 100% protect your data. But you can take some steps to use Zoom more securely such as: not downloading the zoom app, setting your camera by default to “off” or taping over your webcam.
- Always treat Zoom as if there’s a chance anything you say on it might get out. If you need to have a private conversation or talk about something sensitive, do it across an encrypted communication method, like Signal.
- Both students and teachers should have a right to be informed about and make choices about the software that they need to interact with to do their job or get their education. Make sure your colleagues and fellow students are aware of the privacy and security risks of using Zoom. Let’s set up our classrooms in ways that make it easy for everyone involved to stay safe and take control of what data is collected on them.
- Universities are big clients, and Zoom does care what they think - if we all put pressure on our school administrations to put pressure on Zoom, we can get Zoom to change.
- Flip to the end for a Zoom privacy checklist to remind yourself of when you use Zoom!

Continue on for a more comprehensive explanation of the privacy risks of Zoom, info on what data Zoom does and doesn’t collect, and tutorials for using Zoom or other video call software in a secure way.

# Why Should I Be Worried About Zoom

In a few weeks at the start of the COVID-19 pandemic, pretty much every higher-ed institution in the US, and a large number of other schools, have adopted Zoom as their main tool for online classes.[1] There are a lot of things to be excited about about Zoom — it’s pretty incredible to me how effectively many schools have managed to move entirely online on short notice, with the help of video-call software. But at the same time, **almost every educational institution in the country all at once adopting this single software should worry us.**

## Always Be Wary Of A Monopoly

First off, it’s scary to me that over a three week period last April, **Zoom pretty much gained a monopoly over education.**[2] Many schools are entirely dependent on Zoom. Many schools have only provided resources to teachers about how to teach classes in Zoom. **If Zoom breaks**

---

[1] https://www.washingtonpost.com/technology/2020/04/02/everybody-seems-be-using-zoom-its-security-flaws-could-leave-people-risk/

[2] https://www.nytimes.com/2020/03/17/style/zoom-parties-coronavirus-memes.html https://www.forbes.com/sites/alexkonrad/2020/03/13/zoom-video-coronavirus-eric-yuan-schools/#44793a234e71

**or fails, or is revealed to have some sort of dangerous security bug, or if the CEO decides to jack up prices, we are all screwed.**

**Forming monopolies is how big tech companies get away with exploiting both their customers and their workers**. When companies like Amazon[3] or Facebook[4] have no real competitors, they can get away with things they shouldn't be able to — they can pay their workers starvation wages, exacerbate the spread of fake news, or mine and sell their customers' data to advertisers — because there is no competitor for customers to take their business to if they don't like it. Large tech companies often strategically lower their prices to drive competitors out of business, then raise their prices once they've got a captive market - so we should be suspicious that Zoom has been lowering their prices and pushing their video call software on schools right now.[5]

We don't want to end up in a situation where Zoom is the only way that US teachers are trained to conduct online classes. **We don't want to end up in a situation where we have to be okay with whatever changes to terms and conditions Zoom makes because our teaching infrastructure is entirely dependent on it.**

**Alternative to Zoom do exist!** We used them before the pandemic, and they have not disappeared. (In the Guide for teachers section, I go more in depth into other platform choices you have available to you) Though these platforms all have their own issues, diversifying the platforms we teach on still helps to fight the monopolistic power of Zoom - at least they won't be able to get away with anything too shady while worrying about competitors.

## Zoom Has A History of Censorship

**You have no right to free speech on Zoom**. Zoom is not a public space, it is owned by a private company, and this means that (in the United States), the first amendment does not apply to them. **If Zoom at any time decides that they don't like what you're saying, they can (completely legally) shut down your meeting.**

Historically, Zoom has used this power - and **jumps quickly to the beck and call of world governments which want to restrict your freedom of speech**. In June, Zoom suspended the accounts of two Chinese activists running an event about the Tiananmen Square massacre - even though the activists were currently living in the United States.[6] This September, they shut down an event at San Francisco State University discussing palestinan liberation, after zionist

---

[3] https://www.yalelawjournal.org/note/amazons-antitrust-paradox
[4] https://qz.com/1704143/the-antitrust-case-against-facebook/
[5] https://www.theverge.com/2019/5/13/18563379/amazon-predatory-pricing-antitrust-law
https://www.nytimes.com/2018/12/12/books/review-curse-of-bigness-antitrust-law-tim-wu.html
[6] https://qz.com/1868184/zoom-will-continue-censoring-calls-at-chinas-request/

groups reported the event, because one of the speakers was on the US government's terrorist watchlist.[7] We should not expect this censorship to stop - **Zoom has promised the Chinese government that it will be better and quicker at jumping to censorship requests in the future.**

Zoom has also capricious censored events for its own purposes - in October**, they shut down an event at NYU discussing Zoom's history of censorship.**[8] When Zoom shuts down events, there is no appeals process**.** They do not need to provide an explanation for their actions, and they can change the rules whenever they want. **Especially combined with Zoom's monopolistic control over educational videoconferencing, that gives Zoom a pretty worrying ability to limit academic and educational free speech - which is crucial to the work we do in almost any field.**

## Zoom Has A History of Shady Data Practices

**Zoom does not respect user's privacy**, both from their own bosses and from the Zoom company itself, **and their terms and conditions are not honest or transparent about the data they collect and share.**

As with all tech companies, if you are using an online service for free, *you* are probably the product. **We don't know that Zoom does with data that it collects on you, but it collects a lot of it.** When you sign the Zoom terms and conditions, you give Zoom permission to store **everything that it records through your webcam, microphone**, everything you type into the chat, every attachment you share through the program, as well as information about the computer you're using, and **your exact location in latitude and longitude**.[9] **We don't know exactly what Zoom does with this information.**

**Zoom has already gotten in trouble for lack of transparency in their data practices.** Back in April, several states sued Zoom, forcing the company to remove a feature which shared users' data with Facebook without their consent.[10] In fact, Zoom shared users' data with Facebook even if the user didn't have a Facebook account.[11] When journalists raised the issue with Zoom, officials at Zoom responded that they "didn't know" that Zoom shared the data,

---

[7] https://medium.com/datadriveninvestor/leila-khaled-on-campus-letters-from-zoom-palestine-legal-aaup-fec660c6d57b
https://www.thelawfareproject.org/releases/2020/9/22/victory-lawfare-project-and-endjewhatred-movement-cause-zoom-to-cancel-leila-khaled-webinar

[8] https://www.buzzfeednews.com/article/janelytvynenko/zoom-deleted-events-censorship

[9] https://www.consumerreports.org/video-conferencing-services/zoom-teleconferencing-privacy-concerns/

[10] https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html
https://www.documentcloud.org/documents/6821573-Zoom-Class-Action-Lawsuit.html

[11] https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account

which I can only imagine was supposed to inspire confidence, but mostly just worries me again about negligence. And this is not the only time Zoom has gotten in trouble for lying in their terms and conditions about what data they collect on users and sell to advertisers.[12]

**Zoom is also not interested in protecting marginalized users or political dissidents.** For instance, on June 12th, Zoom terminated the accounts of three Chinese dissidents at the request of the Chinese government.[13] Zoom's CEO, Eric Yuan, also initially refused to provide end-to-end encryption as a feature in order to enable Zoom to "work together with FBI, with local law enforcement".[14] **Earlier this year, Zoom promised to publish a transparent report on what government requests for user data they have received and fulfilled, but they missed their own deadline to deliver and so far no information is available - so we do not know what governments Zoom gives data to.**[15]

## Zoom Is Easy To Hack

Historically, Zoom has not proven that it can keep your data secure. **Cybersecurity experts recommend against using it**.[16] SpaceX and NASA, as well as several companies in the Entertainment industry, have already banned their employees from using Zoom because of security concerns.[17] **Zoom has a history of severe high-profile security bugs, and has not fully fixed all of them.** And now that Zoom has been so widely adopted in industries across the board, and so many people have it on their computers, every hacker will be looking for ways to exploit it.

For instance, in Jan 2019, cybersecurity researchers discovered that if Zoom was installed on a Mac computer, a hacker could create a website which could open a secret video call on that computer without the computer owner's consent.[18] This meant that **a hacker could get access to that computer's webcam** just by sending the user a link to an innocent looking website **-**

---

[12] https://sfist.com/2020/04/01/zoom-video-conferencing-hit-with-privacy-scandal/
[13] https://www.tomsguide.com/news/zoom-china-blocking
[14] https://www.theguardian.com/technology/2020/apr/08/zoom-privacy-video-chat-alternatives
[15]https://techcrunch.com/2020/07/01/zoom-transparency-report-deadline/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAADT9OnEicpGL9NsSEMtXeK8eWalU8keJCknmxFeJRGQ4RdpQAB7Dw6UU8kNFJhLpKOkPXEE5t-0GUtL5s__lodNYQ-S93fD3F0qJQuAUb7Vkm9bg7xIYW8fkkb2EqbLzvj2MwQemIxGUWjc48ob4RQDejpavpTkFg_jWWgRp6Z1v
https://tech.newstatesman.com/security/zoom-government-data-requests
[16] https://theintercept.com/2020/03/31/zoom-meeting-encryption/
[17]https://www.reuters.com/article/us-spacex-zoom-video-commn/elon-musks-spacex-bans-zoom-over-privacy-concerns-memo-idUSKBN21J71H
[18]https://www.vox.com/recode/2019/7/9/20687689/zoom-mac-vulnerability-medium-jonathan-leitschuh-camera
https://www.vice.com/en_us/article/8xzjj4/zoom-video-conferencing-vulnerability-lets-hackers-turn-on-your-webcam
https://www.theverge.com/2019/7/8/20687014/zoom-security-flaw-video-conference-websites-hijack-mac-cameras

**they could see inside the user's house, watch as the user typed in passwords, or eavesdrop on conversations**. Or they could crash the user's computer by opening and closing fake meetings until it overwhelmed the machine. To make matters worse, you couldn't even protect yourself by deleting the app: if Zoom had *ever* been installed on the computer, a hacker could reinstall it remotely. This is, by cybersecurity standards, a really bad bug - super easy for hackers to exploit, super dangerous to the user. The bug went un-patched for several months.

Though Zoom has patched this particular security bug and made significant advances in data security after coming under criticism from data privacy experts at the start of the pandemic, many issues with the program remain. A recent security bug let hackers take over any computer running Windows 7 or earlier if a user opens a file they send them in Zoom.[19] Cybersecurity experts have also found vulnerabilities in Zoom's chat which let a hacker run code on a user's computer just by sending a GIF to the chat.[20] And those are just the bugs that security experts have kept ahead of - hackers might be finding more every month.

**Zoom has also strongly signalled that they care more about making money than they do about their user's data security**. For instance, after they were caught falsely advertising end-to-end encryption (a way of encrypting video calls which means that Zoom itself, or hackers accessing Zoom's databases, can't see the content of your calls) in June, Zoom promised to provide the feature...but only for paying users. **It wasn't until activists campaigned against this decision that Zoom released this necessary privacy feature for all users.**[21] Data security shouldn't just be for those who can afford it, it should be for everybody - but Zoom has shown that they don't think so.

# Data Ethics Principles

**When we bring technology into the classroom, we should always think about the ethical implications of that tech**. Here are a few principles that guide my thinking about tech ethics in schools - in my recommendations in the second half of this paper, I've tried to make suggestions that I believe will help uphold these principles. As technology becomes increasingly integrated into our classes, I hope that you can take these principles forwards, beyond just the case of Zoom and the COVID-19 outbreak.

## Privacy

Classrooms should be safe and private spaces where both students and teachers feel comfortable taking risks and being vulnerable. **People can't learn and be brave in an**

[19] https://www.tomsguide.com/news/zoom-security-flaw-windows
[20] https://talosintelligence.com/vulnerability_reports/TALOS-2020-1055
[21] https://www.theguardian.com/technology/2020/apr/08/zoom-privacy-video-chat-alternatives

**environment where they're worried they're being watched** - this is what free speech scholars call a "chilling effect."

## Security

Storing data is always a risk.Though the GDPR is improving things in terms of how long companies can hold some kinds of data, like location data, on you, there are still lots of sorts of data that they can hold on to for a very long time.[22] **Once a company has collected your data, there is usually no way to take it back.** Even if you trust the company storing your data now, if their leadership changes and you don't trust them anymore, they still have your data. If the company hands your data over to the government or the police, you can be prosecuted based on it. If hackers break into the company's data stores, now criminals have it. If anyone in your classroom ever says anything that they wouldn't want the police, the state, or the world to know about - if you have an undocumneted student, if you have a queer student who's not out to everyone, if you express controverisal beliefs in the classroom - then **you better really trust whoever's storing that data - or make sure as little of it gets collected as possible.**

## Freedom to Protest

Speech on online platforms may not be protected by the first amendment, but that doesn't mean that online platforms shouldn't respect the spirit of freedom of assembly or freedom to protest. **Giving corporations unlimited power to censor what we say online (especially with no input from users about what content should be censored) is a threat to democracy, as well as to academic liberties.**

## Data Autonomy

**Classrooms should be places for learning, not involuntary data factories for advertising companies**. Giving data to a corporation is a political choice - corporations can use data they collect on users to create racist and sexist algorithms, or sell them to entities that a person might not want to support. For instance, Clearview.ai didn't ask permission to use pictures people had posted online to make a creepy face recognition system for police departments, and it's upsetting to me to think that pictures I innocently posted online for my friends were used to make something so sleazy and dystopian.[23] Data collected without user's consent often goes towards the creation of racist, sexist, discriminatory. **Everyone in the education system should get to choose who their data goes to, what projects their data supports, and how much and what sorts of data are collected on them.**

---

[22] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
[23] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

## Anti-Racism

**Surveillance in the classroom is a racial equity issue.** In classrooms with more monitoring and more police presence, BIPOC students are much more likely to be prosecuted than white students, and their education suffers.[24] Simogne Brown's research on digital surveillance shows that the same is true in cyberspace - high tech algorithms based on intrusive data collection techniques are much more likely to discriminate against or falsely incriminate black people.[25] Having big archives of any kind of data on your students is dangerous to anyone, but it's most dangerous and disruptive to your BIPOC students. Let's preemptively take steps against a world where recorded video footage of classes is used by racist police to perpetuate racial injustice.

## Accessibility

Which technologies a student can access, and which technologies will work for a student will vary by a number of factors, including the student's socio-economic status, geographic location, and physical and mental health. **Don't assume that all of your students are rich, are located near the school, or are mentally and physically abled.** Your class needs to work for every student, not just the "average" one.

## Transparency

We all have a right to know what data corporations are collecting on us and what they are doing with it. **When corporations act shady with our data, we can't properly evaluate the risks of giving our data to them.**

## Consent

It's important that everyone - students, teachers, faculty, staff - has a real say in what software they use and what data they give to corporations. And by consent, I mean real, informed consent, freely given. Consent given under duress, like consent given under the unequal power dynamic between a school administration and a student, shouldn't count as consent. **Don't sign terms and conditions for people or volunteer other people's data without consulting with them.**

---

[24] https://www.reuters.com/article/us-health-education-safety/some-school-security-measures-make-kids-feel-less-safe-idUSKCN1M72P5
https://www.aclunc.org/sites/default/files/20161019-the_right_to_remain_a_student-aclu_california_0.pdf

[25] https://nyupress.org/9781479837243/algorithms-of-oppression/
https://read.dukeupress.edu/books/book/147/Dark-MattersOn-the-Surveillance-of-Blackness

# Guide for Teachers

This section of the guide is for instructors who find themself in the position of being asked to teach classes in Zoom. Maybe you're not very familiar with this technology and have lots of questions about how to adapt. Or maybe you're a little more tech savvy, but are concerned about what data Zoom might be collecting on you and your students. Here's some information you should know about what data Zoom collects on you and your students, what information it hands over to your employer, and some recommendations about how to teach online classes which minimally invade your students' privacy.

Tl;dr

- Avoid requiring students to video call if its an option for you - create asynchronous or voice-only options
- Be aware that there are alternative video-conferencing softwares - for instance, Jitsi, which is privacy-respecting and open-source, or Discord, which at least provides an alternative to Zoom's monopoly and more useful UI features - and work with your students to find a software they feel comfortable using.
- Refuse to make recordings of your classes without your students' consent - and if you must make recordings, make sure they're stored securely.
- Reject additional software which subjects your students to surveillance
- Make it easy for students to join in the browser - a more secure way for them to use Zoom
- Allow students to participate in class with their video off
- Use passwords and the waiting room feature to protect your class from trolling and racist "zoombombing"
- Make sure your students understand how zoom collects and stores their data, and what they are agreeing to when they use Zoom
- Be aware that your employer can access recordings you make of classes, and information about the zoom calls you make, as well as the computer you make them on
- Understand how Zoom censors events, and have backup plans for events or classes that may be censored
- Read the Guide For Students section for more best practices about how to use Zoom

## Consider Alternatives

As an instructor of an online class, you have a lot of power to control how students interact with their own computers in their own houses. It might not seem obvious how much power this really is, but it is important that you understand this responsibility. **When you teach an online class using a particular software, you are telling students that in order to continue with their education, they need to consent to all the terms and conditions of that software.** You

might be asking students to change the operating system that they are using to one that can accomodate that software, to allow the company that owns that software access to their own personal data, and perhaps compromise on their own moral principles about data privacy and ethics. Asking students to install software will affect how they interact with their own computer beyond the boundaries of your class - for instance, if a student even so much as installs zoom on their computer, zoom can share data about that computer's location, make, model, operating system, and IP address, *even when zoom is not open.* Most students won't have a separate computer for work and school - so when you ask them to install software, **you're not just asking them to take risks with their school-related data, but the rest of their personal data as well.**

**Not using the software required by a class is not a choice for most students** - abandoning their education to avoid compromising their privacy is just not an option. Especially as more of our life moves online during the COVID-19 outbreak, people often view computers as extensions of the self - and being forced to make a change to your computer's software that you do not want can feel incredibly invasive, like a violation of autonomy in one's own home - especially when a student is faced with a choice between downloading invasive software or failing a class. **Before you decide to teach a class using a certain software, ask yourself "Am I okay with forcing students to agree to the terms and conditions of this software, even if they can't consent?"**

## Not Using Video Chat Or Providing Alternatives

Right now, most schools shut down due to Covid-19 are moving to video-call based classes. There are a lot of advantages to video call based classes - video calls might help your class feel more present, make it easier to read the room, or create a more convincing illusion of face-to-face human interaction.

However, **video calls are also a majorly data intensive form of communication - they take a pretty high speed computer and a lot of bandwidth to work well.** The computer that gets me through grad school - a secondhand 2014 Dell PC that I got secondhand off ebay - majorly struggles to keep a video call going. It will usually crash if I try to both participate in a video call and take notes in another tab. Many of your students will be using even worse computers.

**Video calling also requires a fast and reliable internet connection**. Students in areas with low internet coverage (for instance, college students who've gone back to stay with family in rural areas) will have a hard time keeping up with video calls. Video calling can also be very expensive for students on pay-for-data internet plans.

**Many students, especially students with disabilities, can have a hard time focusing on video chats.** Sitting staring at a screen can make focus very difficult for students with ADHD or

Autism - and, in fact, turning off their video to fidget or walk around can actually help these students focus. Students who get chronic migraines (like me) can have a really rough time looking at a bright screen for hours, especially when the rest of their work is a computer. And students with physical disabilities might suffer from the non-ergonomic setup of sitting watching a screen.

For these reasons, **video calling can be a major accessibility issue for a class.** If you plan to conduct a class mostly through video calls, **make sure that all of your students have a fast computer, reliable internet connection, and won't be paying out of pocket for data**, **and that this is the best method for your students focus and health.** If you have students who don't have these things, consider alternatives - perhaps, you could teach an asynchronous class with posts on discussion boards, or use voice-only conference calls. At the very least, make sure you **create alternative methods of participation for students who video calls won't work for.**

## Using An Alternative Video Conferencing Software

**There are a lot of alternatives to Zoom**: we all used them before the pandemic and, though it can seem like Zoom is everywhere now, they still exist!

Unfortunately, there is no perfectly ethical, perfectly useful, perfectly accessible video call software -I don't unconditionally endorse any of the software listed here. A lot of open-source, privacy-respecting alternatives to Zoom are going to be less sleek and shiny - you'll have to deal with some frustration, lag, and inconvenience. Other softwares might be sleeker, but not necessarily be better than Zoom in terms of data privacy. All the softwares listed here will probably all be better than Zoom in terms of security and censorship. And, **by using one of them, you're helping fight Zoom's monopolistic control over education**. And, it is good to know what your options are. **Here are a few alternatives to Zoom, along with their benefits and drawbacks.**

### Discord

tl;dr the somewhat more ethical, much more convenient choice

**Discord is another large corporate platform with video conference capabilities.** Unlike Zoom, which was created for corporate meetings, Discord was created for gamers to chat on - so it has the upside that many of your Gen-Z students will already have an account. Discord has capabilities for chat, link and image sharing, small video chats, or and voice chat. It also allows you to livestream a presentation with one person screen sharing and other members of the class on voice only. It's got some cool features that Zoom doesn't have that might be helpful for

teaching classes - like the ability to create multiple chat channels for topics. You can also make a persistent digital location, called a “server” for your class, so you won’t need to send out a different link every class, and your class will be able to hang out on the server even when you’re not there.

**Discord also has a rigorous system of permissions management which makes it a good choice for preventing “zoombombing”** and keeping your class secure - for instance, you can make single-use invite links. It also doesn’t have a lot of the issues with hackers that Zoom has.

Unlike Zoom, **Discord won’t tell data about you or your students to your employer. But Discord is still a private corporation and can still collect and sell your data and your students data to advertisers.**

Here’s a tutorial on how to set up a discord server for your class - https://support.discordapp.com/hc/en-us/articles/360040613072-How-to-Use-Discord-for-Your-Classroom
And an experienced online teacher talking about how he structured his class’s discord: https://www.youtube.com/watch?v=UePvbD31ON4
And here’s a bot that you can add to Discord for teaching math classes that will let you type math formulas in Discord chat: https://top.gg/bot/510789298321096704

### Jitsi

tl;dr the much more secure and ethical, but slightly less convenient choice

**Jitsi is the most widespread open-source video chat platform.** That means, there are no secrets about it - anyone can look at the source code to make sure they’re not up to anything sneaky, and it’s not owned by a monopolistic megacorp. Jitsi is totally free for you and your institution to use. And, most importantly, **Jitsi’s business model is not about selling your data.** Jitsi also takes encryption and data privacy very seriously.

**The Jitsi interface basically looks like a copy of Zoom**. You can make meetings, share screens, password protect meetings, do pretty much everything you can do in Zoom. You can use Jitsi online through the official Jitsi servers, or, to be super duper secure, you or your institution can set up your own server.

Jitsi is a pretty loosey-goosey. You don’t even need to make an account to create a meeting. This is good because **Jitsi won’t require your students to download anything or even make an account.** But one drawback is that on Jitsi, no one is the “host” of a meeting - everyone can mess with the settings, which could be a problem if you have an unruly class. **It also doesn’t have great features for protecting against zoombombing.**

Another big downside is that Jitsi can be pretty glitchy, and doesn't have all the features that more polished software like Zoom has. It also doesn't work great on all browsers - chrome and chromium are best.

Here are some tutorials about how to use Jitsi:

A basic guides to creating a JITSI meeting online -
https://www.youtube.com/watch?v=QMnD-47Rquo
https://www.youtube.com/watch?v=IN0Jnwo7eww
More advanced tutorials to make your own server - https://jitsi.org/tutorials/

## Livestreaming

**Another option that's good for large lecture classes,** where students will be mostly participating by listening and occasionally asking questions, **is to livestream class.** In a livestream, you present a lecture through a video broadcast, and students can raise questions of comments through a text chat. You'll need to get used to splitting your attention a bit, but once you get the hang of it, it can be a good option. **You can use a livestreaming platform like Twitch, crowdcast.io, or YouTube. For a very large class, this setup actually makes much more sense than a 150 person video call.**

Many of these platforms also allow you to record class for students who need to participate asynchronously - a good option if you're okay with being recorded, which won't expose your students to too much risk. Most livestreaming platforms should have options for a private livestream that you can give your students access to.

**Livestreaming is not ideal for discussion classes** with a lot of back-and-forth, so you may want to find another setup to pair it with if you have a class with a combination of lectures and discussions.

## Other Alternatives

For small discussion classes, you can also meet using **another video-conference software like Signal, Google Hangouts/Google Meet, Skype, Microsoft Teams, Cisco Webex or BlueJeans.** These programs are at least easier to use in browser or more secure than Zoom, and most of them have fewer issues with censorship.Some of these softwares may not be as able to handle really large calls - They're good options for small classes though.

You also could consider polling your students to see what software they would feel comfortable using to attend class, rather than handing them a top-down choice.

If your employer is requiring teachers to use Zoom, ask them to let you use an alternative to Zoom, or, better yet, for them to institutionally support an alternative to Zoom.

# If You Have To Use Zoom….

There are still some things you can do to use it in a way that is minimally invasive for you and your students.

## Protecting yourself from surveillance

You should know that Zoom collects this information on you when you are teaching class:

- If you are using an institutional Zoom, your employer can see when you have zoom open and running and when you don't - and can see the IP address, location, make, and model of the computer you're running zoom from. They can also see this information for all your students.
- If you make any recordings of a class, your employer will be able to access those recordings (which also means they can copy them and store them indefinitely). They probably hold the intellectual property rights to those videos too, meaning they could reuse them without your consent - check your particular school's policy.
- Someone at your school with an administrator account can enter any of your zoom calls at any time, without needing an invite or a password.
- Zoom has a bug where it might share your email, name, and profile picture with anyone you've been in a call with - so make sure whatever email you use to create a zoom account is one you're okay with students seeing.
- And in general remember - anything you can see or hear on your webcam or microphone, Zoom can see too.

## Protecting Your Students From Surveillance

### Refuse To Make Recordings Without Your Students' Consent

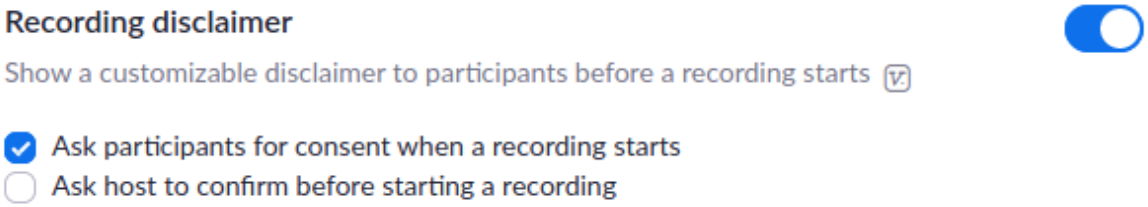
Some schools (such as my institution) are requiring teachers to make recordings of all of the classes they teach, to be handed over to the administration. This means that your school administration, as well as the Zoom company, can hold onto recordings of you and your students for an arbitrary amount of time. Your employer will be able to access these videos to evaluate your performance, judge the choices you make as a teacher, and it is likely that your employer now holds the intellectual property rights to that video as well. **Having video recordings of class exist indefinitely is a security risk to you and your class** - if your

school is served a subpoena, anything in those records will be handed over to the government, and if hackers infiltrate the video database, anything you or your students say in class could be made public.

Having recordings of lecture classes can be nice as a way for students to asynchronously participate in class, especially if they're in different time zones, and especially if you can record class so you're the only one in the recording. **But don't record your students without their permission** - if students ask questions in a lecture video you intend to post, ask their permission to have their questions included in the recording. And don't record discussion classes unless you get every student's permission, even if you don't intend to post the recordings - it's really important to students' learning in discussion classes that they feel comfortable and can be open.

Sometimes, our institution doesn't give us a choice about making recordings though. **If not all of your students consent to being recorded, but your school requires you to make recordings, I encourage you to, if you feel comfortable, advocate for your students to your school administration.**

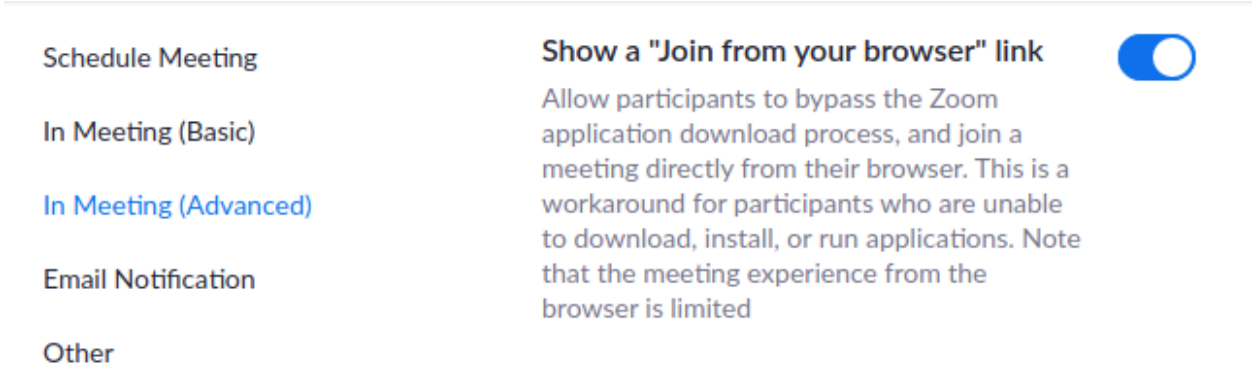
**If you are still required to record classes after raising the issue with your institution, do your best to inform students that they are being recorded and to educate them about the risks.** Make sure that it is clear to your students when they are being recorded by enabling the "ask participant's consent when a recording starts setting." This setting will not allow your students to participate in class without being recorded, but it will make sure that they at least understand clearly when they are being recorded. To make sure this is enabled, **go to the online zoom settings My Settings > Recording > Recording Disclaimer (turn on)**




**Also, if you are required to record classes, store your recordings on an encrypted, removable harddrive.** You can change where Zoom stores recordings in Zoom Settings > Recording > Local Recording. This will ensure that if your computer is hacked, your students' data will still be safe.

## Don't Make Your Students Download Zoom; Encourage Them To Use It In The Browser

You actually don't need to download Zoom to use it - there's a browser option! Zoom tries to keep the browser option a secret though, you have to do a bit of digging in the settings to find it. You can help make it easier to find for students to find it by enabling a "Join From Browser" link, which will give students a clear option to join in the browser when they click the meeting link. You'll want to go to Zoom Account Settings online and go to Personal Settings > Meeting > In Meeting (Advanced) > Show a "Join from your browser" link, and toggle that setting to "on"




**Using Zoom in the browser is a safer and more secure way for your students to use Zoom,** since it means that Zoom can only collect data on them when they've actively got Zoom open, and means they won't have to install a piece of software on their computer that hackers could infiltrate.

Sometimes, students might have trouble accessing a password protected meeting in browser - this is a tricky tradeoff with protecting your class from zoombombing - if that issue comes up, I encourage you to have a discussion with your students about which option they'd rather.

## Always Use End-To-End Encryption

Zoom now provides end-to-end encryption for all users, but you will need to make sure it is turned on. In order to check this:

Navigate to the Zoom browser personal settings again, then navigate to Meeting Settings (Basic) and then check the slider which either says "enable end-to-end encryption"


A popup will come up asking if you want to turn on this feature for all participants - click yes.

End-to-end encryption is a basic security feature which ensures that your data is kept secure and private - privacy experts argue that unless data is end-to-end encrypted, it's not really encrypted.

## Allow Your Students To Turn Their Video Off

Regardless of whether or not you are recording Zoom classes, the Zoom company is recording all of your classes, and potentially mining them for data. Additionally, many security flaws with the program work by giving hackers access to video footage from a webcam on a computer running Zoom. **Turning off their cameras during class is an important way that students can protect themselves from corporate surveillance and from hackers. Let students know that you support them doing what they need to do to stay safe, and tell them it's okay for them to participate in class without video.**

I've seen a lot of advice going around that teachers should require students to have their video on during class - the argument goes that if they don't have video on, students will likely be distractible, or secretly goofing off. However, requiring your students to have video on so that you can be sure that they're paying attention in class is effectively requiring your students to submit to video surveillance to participate in class. **Just because students are trying to protect their privacy from Zoom does not mean that they have something to hide from you** - please extend the same trust to them that you would if classes weren't remote.

**Do not use Zoom's features to forcibly unmute participants or turn on their audio - send the message to students that you respect their autonomy over their own computers.**

## Protect Your Students From Zoombombing and Racist Trolling

Regrettably, because we can't have nice things as a society, a new form of trolling, called Zoombombing, has become a big problem for teachers everywhere in these past few weeks.[26] **In Zoombombing, trolls infiltrate zoom classes and use the screen sharing function to disrupt a class, often with obscene or racist material**. Trolls who organize zoombombings through websites like 4chan often especially target teachers of color, and professors of feminist or queer studies classes. **Most zoombombings happen when class links get posted online and trolls find them, and when meetings aren't password protected.** Regrettably, because some bad actors apparently don't see a global health crisis as a good enough reason to not be terrible people, **we all need to up the security on our online classes** so that these jerks can't barge in and make our students have to listen to hate speech. Honestly though, it's probably good practice to have our Zoom meetings be a little more secure anyways.

---

[26] https://www.buzzfeednews.com/article/salvadorhernandez/zoom-coronavirus-racist-zoombombing
https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html

To prevent zoombombing, you'll want to:

- **Make sure your meetings are password protected.** Zoom's password feature actually isn't great and serious hackers can crack it like nobody's business, but it'll deter most trolls. (You should make sure password protection is on if you're using another video-call software too, like Jitsi)
- **Don't post your meeting links online.** Email them to your students privately.
- **Make sure you have the waiting room feature on** - this means that when new members join the meeting, you'll have to manually approve them to enter, so you can reject anyone you don't recognize as one of your students. (Note that the waiting room feature won't notify you when students are waiting, and if students get kicked from a call due to bad internet connection they'll be put in the waiting room again, so check it frequently. And, if you can, give students another way to contact you that will ping you with a notification, so they can let you know if they're in the waiting room) - here's how to do that: https://support.zoom.us/hc/en-us/articles/115000332726
- **Limit screen sharing** so that trolls who do break into the call at least can't hijack your class with disturbing visuals.
- **Make sure you know how to ban participants** in case you get unwanted trolls and need to kick them from the call.

Here are a few guides about how to do all that:
https://www.adl.org/blog/how-to-prevent-zoombombing
https://security.berkeley.edu/resources/cybersecurity-and-covid-19/settings-preventing-zoom-bombing

## Avoid Zoom Censorship

Zoom has a history of censoring meetings discussing controversial topics, often at the request of oppressive governments. **Based on previous cases of censorship, Zoom may try to censor your meeting if:**

- **Your meeting includes speakers discussing a topic which governments have attempted to silence in *any country* where Zoom is popular** (for instance, Chinese activists discussing Tiananmen Square have been censored even in US based Zoom calls)
- **Your meeting includes speakers who are declared to be enemies of the state (exiled, on terrorist watchlists) by *any country* where Zoom is popular** (for instance, Zoom has censored events with speakers who are members of groups classified as terrorist organizations by the US government)

- **Your meeting will discuss information that makes Zoom look bad** (Zoom has censored meetings discussing Zoom censorship)

Currently, we have no reason to believe that Zoom is surveilling all meetings looking for meetings to censor - **all of the meetings which have been censored so far seem to have come to Zoom's attention when they were reported, either by governments, or by other organizations.** This could change in the future, especially if governments put more pressure on Zoom to be more proactive about censoring meetings. Zoom currently does not censor most events which discuss controversial topics. But **your event is more likely to end up on Zoom's radar if:**

- **The meeting name mentions the controversial speakers or topics** (this would make it easier for Zoom to use an algorithm to find and censor the meeting)
- **The meeting is publicly advertised** (this would make it more likely that groups that want to report it to Zoom will see it)

If you plan on running a meeting which is likely to be censored by Zoom, **I recommend that you have a backup plan (an alternate way to host the meeting) lined up, in case the meeting gets shut down.**

If you want to band together with other faculty to demand that your university administration address the problem of Zoom censoring academic freedom, here's a statement that faculty at Georgetown university wrote which could work as a helpful template.

### Schedule One-On-One Meetings In An Encrypted Medium

If you schedule one-on-one meetings with students, for example, for mentorship or consultation on papers or office hours, try to use a software other than Zoom. For teaching class, Zoom is helpful since you might need screen sharing or the ability to juggle dozens of participants. But for a one-on-one meeting, you shouldn't need anything fancy. Students might need to discuss sensitive topics with you in one-on-one meetings, so it's extra important to protect their privacy. Be especially aware of the needs of your BIPOC, female, international, and immigrant students - don't assume your students aren't carrying heavy stuff that could get them in trouble or that they won't mention it to you in a meeting. **Instead of scheduling one-on-ones on Zoom, try a phone call (especially an encrypted phone call through a program like Signal)**

### Make Sure Your Students Are Informed About How Zoom Collects Their Data

Share this guide with them, or write up a cheat sheet. When designing syllabi for virtual classes, make it a part of the syllabus! If it fits with your class, you might want to even take the time to have a discussion with your students about Zoom and the implications of using it.

## Other Software

As the pandemic drags on and it looks like online teaching is here for the long haul, a number of companies have stepped in promising solutions to the difficulties of online teaching. A lot of these programs can be very helpful, but the same cautions that I want to raise about Zoom go for these programs too - **always look into the data practices of any program you're going to ask your students to use and install, and ask: how is this surveilling my students? What is this doing with the data?**

A category of software to **be especially suspicious of is proctoring software for monitoring students during testing**. Programs like Canvas, Respondus, or ProctorU promise to help solve the potential problem of cheating during remote testing.[27] But these incredibly invasive softwares which might literally seize control of a student's computer for the duration of a test, or require them to submit to video surveillance, are effectively asking your students to install spyware on their computers. Whereas surveillance might be an unfortunate side effect of Zoom, it is literally the point of these softwares.

**Using spyware on your students is unfair to your students, perpetuates bias, and creates an environment hostile to education.[28]** Feeling like your instructor sees you as a criminal who might at any minute cheat on a test is a lousy emotional condition for students to take an exam in, and normalizes to your students that it is okay for authority figures to treat them as criminal until proven otherwise. Students do feel creeped out by these programs, and feeling creeped out distracts from learning.[29] Research by researchers like Ruha Benjamin tells us that invasive programs which use eye tracking, face recognition, and other biometrics to identify suspicious behaviors, are likely to be unfairly biased against BIPOC students[30] - and, even if your software doesn't use any algorithms, students who have had more negative past experiences with surveillance and being treated as criminals will have an even more miserable time with this software.[31] These softwares have often been shown to be buggy, exploitable by hackers, and, at times, expensive for students who need to themselves pay out of pocket to be scrutinized by these programs.[32]

Zoom might be a grey area, but **you owe your students better than spyware software**. Kick and scream if anyone asks you to use this stuff.

---

[27] https://www.forbes.com/sites/seanlawson/2020/04/24/are-schools-forcing-students-to-install-spyware-that-invades-their-privacy-as-a-result-of-the-coronavirus-lockdown/#e8c920c638d8

[28] https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education/

[29] https://www.nytimes.com/2020/05/10/us/online-testing-cheating-universities-coronavirus.html

[30] https://politybooks.com/bookdetail/?isbn=9781509526390

[31] https://www.theverge.com/2020/4/29/21232777/examity-remote-test-proctoring-online-class-education

[32] https://www.chronicle.com/article/will-the-pandemic-usher-in-an-era-of-mass-surveillance-in-higher-education/

## An Afterword

I get that as teachers we're all having to make hard choices right now. We were already overworked before the coronavirus pandemic, and now we're being asked to completely reconfigure our classes with absolutely no time to do so, and we need quick and easy solutions. Often we're not totally free to make decisions about the software we use - our school administrations are handing these things down to us. I wrote this guide to help make ethical remote teaching easier for teachers, not to shame anyone for teaching their class any particular way - we live in a world where access to technology is controlled by a few large, self-interested tech companies, where there often isn't a perfectly ethical option, and every day, we have to make compromises. It is going to be hard to find an option that will 100% respect your students privacy , but will also be useful to you as a teacher. Good cybersecurity practice isn't about always choosing the most secure option, but it is about being aware of the risks that you're taking on every time you choose to use a technology and making an informed evaluation of it it's worth it. Your needs as a teacher are also a valid part of that consideration - be aware of your students needs, but also, make choices that work for you.

Fighting for students' data privacy can be hard right now when so much is going on - I hope that this guide can be a tool that will not only help you structure your own classes, but also help you communicate with your school administration that these issues are important. If you are concerned about these issues, but feel unheard, use this guide to organize within your school or department. Universities do have sway with Zoom - they are big customers who Zoom doesn't want to lose, and Zoom has added features at the request of university administrations before. If you are upset and feeling helpless about any of this, tell your university administration to put pressure on Zoom to shape up its act.

I would also suggest reading the students' section of the guide as well which goes into more in detail about strategies that can minimize how much data on you Zoom collects, stores, and sells.

# Guide for Students

This section of the guide is for students who have had all their classes moved online and are being required to use Zoom or another video conferencing software in order to continue their studies. You likely haven't been given much of a choice about what software to use, or been informed much about how to control the data this software collects on you. Here's a guide to what you should know about Zoom, and what you can do to protect yourself from being spied on, whether by Zoom itself, or by hackers who exploit Zoom.

tl;dr

- Zoom is potentially storing and potentially selling any data it gets from video calls, as well as info about your computer and location. If you install the Zoom app, Zoom is recording info on you always, even when Zoom is off.
- When you use Zoom, your teacher and school administrators might be able to see anything you send in Zoom private chat to your classmates.
- The safest and most secure way to use Zoom is to call into meetings from your phone, or use Zoom in the browser only. Try not to download the Zoom app, if you can avoid it.
- If you do have to download Zoom, make sure you're using the most up to date version, so hackers can't take advantage of old bugs.
- When you're using Zoom, try to have your camera on as little as possible. Make sure your camera is set to "off" by default when you enter meetings. The best strategy is to tape over your webcam when you're not using it.
- Don't talk on Zoom about any information that might endanger you if it was made public. If you have to talk about something sensitive, set up a meeting using an encrypted software, like Signal.

# Things to Know About Zoom

## What Does Zoom Know About Me?

**Zoom is always collecting data about you, even when the app is closed.**

Regardless of whether you've got Zoom open, Zoom knows all the specs of your computer: what operating system you're running, what kind of computer you have, and your computer's exact location in physical space (which means it knows your location too).

When you have the app open, **Zoom can record everything that it can see through your webcam or your microphone.** This includes everything you say in class, but also any background noises your microphone might pick up, any details about your room that the camera catches, etc. It's possible that when you've got the webcam and microphone settings off, Zoom stops recording, but I can't say that for sure. **Zoom also knows everything you write in any chat on Zoom, and if you share any attachments, it knows what's in those attachments too.**

**Zoom stores your data for its own purposes and we don't know who it shares it with**. Though they claim they don't anymore, Zoom has leaked data to other companies without user's permission. We know that Zoom has, on request, given data to the US and Chinese

governments. And we don't know what else they do with your data, because they have not been transparent about it.

### What Data Does Zoom Tell My Teacher About Me?

**For most of your online classes, your teacher will be the meeting "host." This means that they can access a lot of data about everyone in the meeting.**

The host can record meetings if they turn on the "recording" feature. **If a host records a meeting, they'll have a record of everything in that meeting, including everything that was written in chat, *even in private chats that don't include the host.*** So don't use zoom chat to talk about anything you don't want your teacher to see.

### What Data Does Zoom Tell My School Administration About Me?

If your teacher records a meeting, the administrators of the school zoom account will be able to see everything that your teacher can see too.

## How Can I Protect My Privacy While Using Zoom?

Here are a few suggestions about how you can use Zoom in a way that gives you more control over what data is recorded, and better protects you from hackers who might exploit vulnerabilities in Zoom. All of these suggestions are going to be tradeoffs - they'll make using Zoom a little more inconvenient, but they'll give you a bit more control over your data. It's up to you to decide what level of inconvenience is worth what level of privacy.

### Request That Your Teacher Use A Different Software

**The best way to protect yourself from Zoom stealing your data is not to use Zoom**. Suggest an alternative option to your professor, like Jitsi or Discord, or, if you're concerned about all video chat software, ask them to teach class in a different way. Show them the "Guide For Teachers" section of this document!

### Request That Your Teacher Not Record Class

**If you feel uncomfortable with being recorded, ask your teacher not to record class.** Tell them that you don't consent to them using the recording feature.

If your teacher still insists on recording class, you will at least always be able to tell when class is being recorded - a red dot and text saying "recording" should appear at the top left of the screen. **There is no way for the teacher to record class through Zoom secretly without the**

**“recording” symbol appearing.** However, they could still be recording class with another screen recording software.

## Call Into Zoom Meetings on Your Phone Instead Of Computer

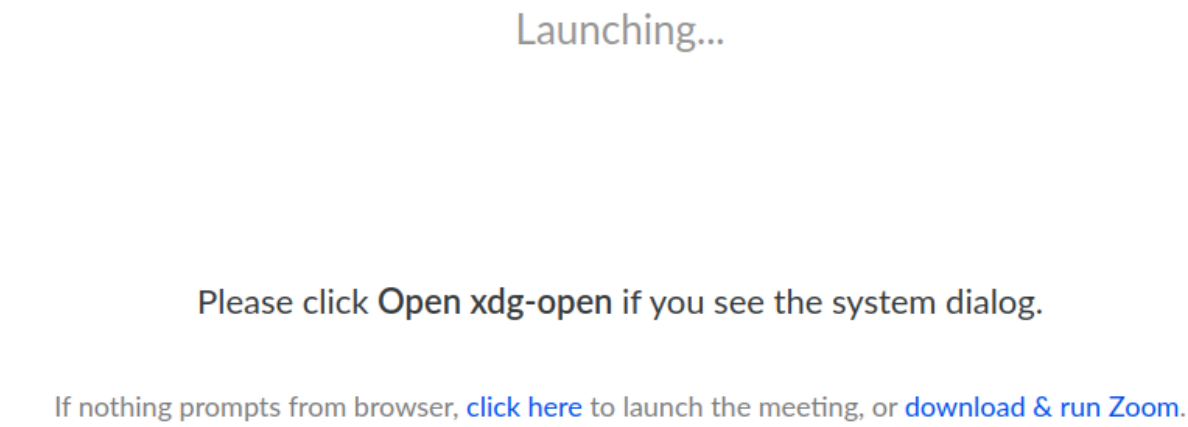
The best way to stop Zoom from spying on your computer is to not use Zoom on your computer. If your professor will let you, and if you can get away with only using audio and no video, **the most secure way to use Zoom is to call into a Zoom meeting using your phone number.** From your phone, you won’t even need to worry about Zoom accessing your webcam or other data on your computer.

When your professor sends out a Zoom link, phone numbers that you can call to join the meeting should be listed under the link. Here is a tutorial about how to call into a Zoom meeting. You’ll need to know your meeting ID #:
https://support.zoom.us/hc/en-us/articles/201362663-Joining-a-meeting-by-phone

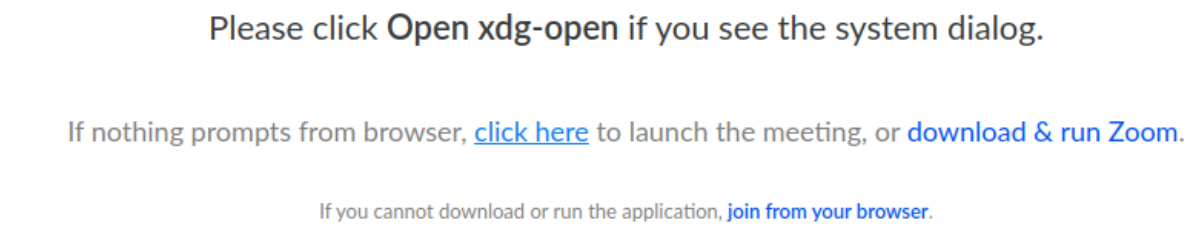
## Use Zoom In The Browser

**The second best way to stop Zoom from spying on your computer is to not download the app, and only use Zoom in the web browser.** A lot of the sneaky stuff that Zoom can do with your data, and a lot of the bugs in Zoom that hackers can exploit to spy on you, really only work when the Zoom app is installed on your computer. If you have the Zoom app installed, Zoom can collect data on you all the time, even when you’re not in the middle of a Zoom call. **If you only use Zoom in your web browser though, Zoom can’t collect data on you or run on your computer when you’re not on a Zoom call - so it’s a much safer option.**

**Zoom really wants you to download the app so it can spy on you, so it tries to hide the fact that the browser-only option exists...But it does!** If you open a Zoom link in your browser, but don’t have Zoom installed on your computer, Zoom will give you a screen that looks something like this (it’ll be a little different depending on your web browser), which prompts you to download Zoom.




Here's the tricky thing. Click that "click here." All of a sudden, a new option should appear:




Click on that "join from your browser." Congrats, you're now using Zoom in your browser!

Sometimes, this doesn't work for me on Firefox. Chrome and Chromium are the best browser choices. If you've already downloaded Zoom, you'll need to uninstall it to use Zoom in the browser - which you should do anyways to protect your computer!

**If the meeting host has the "Join From Browser Link" setting enabled, you won't need to go through that whole clicking through pages process** - the first "Launching…" page will just display the "join from your browser" option. **Ask your teacher to enable that setting** (see, the Guide For Teachers section) to make that link easier for your classmates to find.

You can also use browser extension that automatically converts zoom links into join-in-browser zoom links to accomplish the same thing:
https://chrome.google.com/webstore/detail/zoom-redirector/fmaeeiocbalinknpdkjjfogehkdcbkcd

I've sometimes run into problems accessing password-protected meetings in the browser.

For more info on using Zoom in the browser:
https://techcrunch.com/2020/03/20/psa-yes-you-can-join-a-zoom-meeting-in-the-browser/
https://support.zoom.us/hc/en-us/articles/214629443-Zoom-Web-Client#h_d058aa08-10b5-4c9f-b029-4ce9603bb2d1

## If You Download Zoom, Make Sure It's The Real Deal

Since Zoom has gotten so popular, a lot of hackers have been making fake copies of Zoom, and been trying to get people to download them.[33] These fake copies work like Zoom, but they also let hackers access your account and calls, or even let hackers access data on your computer, so they can steal your personal information and passwords. These hackers have also been registering scam website domain names that look like Zoom, so people will accidentally find those websites.[34]

So if you need to download Zoom, make sure you've got the right url. Legitimate Zoom software should come from https://zoom.us

## Turn Off Video and Microphone

Most cybersecurity expert's recommendation for using Zoom is that you **have your video and microphone off at all times that you don't need them**. That way, you're giving Zoom as little data on you as possible, and minimizing the chance that your camera or mic will accidentally pick something up in the background. **If your teacher will let you participate in class with only audio, no video, that's the most secure.**

## Set Your Camera Default To "Off"

Last year, security experts identified a bug in Zoom that let a hacker spy on you through your webcam by secretly opening a meeting on your computer. You can fight similar security bugs by setting your webcam and microphone defaults to off, so you have to turn them on yourself every time you join a meeting. If you use Zoom only in the browser, you need to worry about this much less. If you have Zoom installed on your computer, you'll need to **go to Settings > Audio > Always Mute The Microphone When Entering A Meeting and Settings > Video > Always Turn Off Video When Joining A Meeting.**

## Tape Over Your Webcam

Turning off video should usually be sufficient, but **the best way to protect against webcam spying is to get a small sticker or piece of opaque tape and put it over your webcam whenever you're not using it.** A sticker or piece of tape is a good failsafe - you can just look to

[33] https://www.tomsguide.com/news/hacked-zoom-installers
[34] https://www.tomsguide.com/news/zoom-malware-attacks

see if the tape is there to know if your webcam is on or off, and even if you forget to turn your webcam off it'll be there. **A piece of tape over your webcam will also protect you from Zoom hackers - even if someone manages to gain access to your webcam and tries to creep on you, they'll just be looking at the back of a piece of tape.** Given Zoom's history of really bad security exploits, it's a good idea, especially if you've got Zoom installed on your computer.

**Try and use a piece of tape that's not too sticky and won't gum up your camera.** Stickers designed for blocking webcams are best, and masking tape or electrical tape is better than duct tape.

## Keep Zoom Updated

If you do install Zoom on your computer, make sure you are frequently checking for updates and have the most recent version. Every hacker in the world is going to have eyes on this thing for the next few months, and Zoom will be racing to try to patch the bugs they find, so **you want to make sure you're using a current version with the holes patched, not on old version that hackers know how to break into.** The safest option is to not download Zoom at all, but if you have to, make sure it's updated. And again, make sure you're getting it from a legitimate url.

## Don't Say Anything On Zoom That You Wouldn't Want The Cops To Know

Bottom line, you should probably assume that no matter what you do in the privacy settings, when Zoom is on, anything you say has a chance of ending up in Zoom's databases....which means that it has a chance of getting watched by your university administration, or getting hacked, or handed over to the police or the government. This doesn't mean you should be totally paranoid - that chance any of those things will happen is still pretty small - but **if you want to say something that would be a big problem for you if someone outside of your class learned about it, don't say it on Zoom.**

This goes for one-on-one meetings too, as well as class. Often, as students, teachers are mentors for us. Or, in order to get accomodations for assignments, we need to disclose dark or personal details to our teachers. But **if you need to tell a teacher or advisor anything really private** - anything dealing with substance abuse or underage drinking, your personal medical situation, pregnancy, abortion, sexual assault, gender or sexuality (if you're in the closet), mental health, or immigration status - **don't do it over Zoom. Set up a phone call on an end-to-end encrypted program like Signal instead.**

## Spreading Education

If you're concerned about the privacy of your data now that classes have gone online, I hope this Guide can be a friendly resource to help you explain your concerns to your teacher or your school administrators. And even if they won't listen, please share this guide around with your fellow students to help them protect their own privacy!

# What Else Can I Do?

Since, as things are going, it does look like a lot of us are going to be stuck with Zoom and kind of at the mercy of whatever privacy policies it choses - and the only way we're going to change that is to work together to put pressure on Zoom to change.

Zoom listens to university administrations: they are big customers, and Zoom does not want to lose them. Zoom has added features at the request of university administrations before, so we know that universities putting pressure on Zoom works. So tell your university or school administration to put pressure on Zoom to shape up its act: demand that Zoom stop censoring meetings, demand more transparency about data practices and security, demand more control over what data Zoom collects!

Here are some academic organizations currently organizing against Zoom censorship:
Statement by Georgetown University Faculty -
https://jimmillward.medium.com/following-zooms-repeated-interference-in-academic-freedom-the-following-resolution-is-going-674716efb702
Statement by the Middle East Studies Association -
https://mesana.org/advocacy/letters-from-the-board/2020/10/29/mesa-statement-on-academic-freedom-and-corporate-control-of-digital-platforms

Zoom can also get away with what it gets away with because in the US (and in many other countries), tech monopolies are extremely poorly regulated. So organize and change that! Call your congresspersons and your representatives and demand that they regulate Zoom better. Call on them to enforce consumer data privacy laws. Call on them to bust Zoom's monopoly over education! Here are some national organizations currently organizing on these issues:

Fight For The Future -
https://www.fightforthefuture.org/news/2020-04-02-new-campaign-calls-for-zoom-to-actually/
Electronic Frontier Foundation -
https://www.eff.org/deeplinks/2020/06/victory-zoom-will-offer-end-end-encryption-all-its-users

# Further Reading

Building Anti-Surveillance Ed-Tech - Audrey Watters: http://hackeducation.com/2020/07/20/surveillance

Against Cop Shit - Jeffrey Moro: https://jeffreymoro.com/blog/2020-02-13-against-cop-shit/

# Zoom Security Checklist

## Zoom Settings

- ❏ End-to-End Encryption is on
- ❏ Join-from-Browser is on
- ❏ Recording Disclaimer is on
- ❏ Waiting Room is on
- ❏ Screen sharing is limited
- ❏ Meetings are password protected
- ❏ Video and Microphone are off by default

## Using Zoom

- ❏ I am calling in on a phone, or if I cannot, using Zoom in the browser, or if I cannot, have downloaded Zoom from a legitimate source
- ❏ My webcam is taped over when not in use

## Scheduling a Zoom Meeting

- ❏ I have determined that Zoom is the best software for this meeting and it would not work to use another program
- ❏ I have asked other participants about their preference for method to meet, and they have given me their explicit consent to use Zoom
- ❏ If this meeting is likely to be censored by Zoom, I have a backup plan ready to go

## Running a Zoom Meeting

- ❏ I have informed participants that it is okay for them to turn their sound/video off and that it will not negatively impact their grade (unless there is a strong reason to require video)
- ❏ (if recording) I have verified that there is no alternative method which would accomplish the same goals as recording this meeting
- ❏ (if recording) I have informed participants that I am recording and asked for their permission to be recorded