# Security and Privacy Principles for Virtual Meetings

Version 0.3 July 18, 2020

LINK to live Google doc

## Abstract

The COVID-19 pandemic has rapidly driven individuals and communities worldwide to interact over the Internet in new ways. Consequently, and with a speed rarely seen, virtual conferencing platforms have been pressed into service for new uses by large categories of users to facilitate previously non-virtual aspects of everyday life. These diverse interactions include, for example, religious services, birthday parties, department meetings, weddings, medical appointments, psychotherapist sessions, and high-level government consultations. This document offers specific security and privacy recommendations for virtual conferencing, connecting these recommendations to classic principles in security and privacy.

**Contributors** (in alphabetical order):

Adam Eisgrau, Simson Garfinkel, Jeanna Matthews, Andy Oram, Patrick Traynor, Alec Yasinac

**How to contribute**: Since it surveys a rapidly evolving topic, this guide is based on a live Google document that is periodically versioned. We welcome contributions from readers! We expect to export subsets of the document for a variety of purposes including possibly a US-TPC

statement of general principles, an addition to "Virtual Conferences: A Guide to Best Practices" from ACM and more. Copyright for the entire document will be held by the Executive Editor of this document and all contributions are gratefully accepted with the understanding that making a contribution is understood to include transferring copyright in that contribution. If you make a contribution you are assigning copyright. Feel free to make comments/give feedback at any time, but if you want to make an official contribution of text and add yourself to the contributors list, please first contact the Executive Editor regarding the copyright transfer.

# Introduction

Virtual conferencing platforms are experiencing a sudden burst of use as the COVID-19 pandemic drives communities worldwide to interact over the Internet. In one of the most rapid technical adoption trajectories ever seen, these platforms are suddenly being pressed into service for new uses throughout everyday life: university classes, virtual conferences, religious services, birthday parties, department meetings, weddings, medical appointments, psychotherapist appointments, and even high-level government consultations.

All kinds of people, including students, workers, and even attendees at religious services are being encouraged to use these technologies, despite significant security and privacy failings that many of these platforms share. Many of these systems have limited security and privacy controls that might have been sufficient when they were only used for the occasional public-facing webinar, but are insufficient for use in more sensitive applications.

As a result, virtual conferencing tools are suddenly drawing scrutiny, sometimes for flaws in security or privacy that had already been noticed by researchers in the past. Any platform that enjoys substantial usage can become a target for attack, trolling, disruption, and surveillance. Numerous examples of such abuses were documented in March 2020, fueling a sudden concern over the problem and the coinage of the word “zoombombing” (which occurs when miscreants take over and misuse a publicly accessible video conference—for example, by projecting a desktop containing objectionable material) [2, 5, 7].

Many new videoconferencing users are not trained in using these technologies or in underlying principles of online security and privacy [36]. In most cases, adoption is taking place quickly and out of necessity, without much opportunity to consider important issues such as security training, threats to privacy, impacts on vulnerable communities, or laws such as the European Union's General Data Protection Regulation (GDPR) and the US Family Educational Rights and Privacy Act (FERPA).

There are many video conferencing platforms, including Zoom, WebEx, GoToMeeting, Skype, Google Meet, Uberconference, Blue Jeans Meetings, HouseParty, and others. Zoom in particular increased dramatically and unexpectedly from 10 million users in December 2019 to 200 million users in March 2020 as a result of the COVID-19 pandemic [Z1].

In this document, we survey the security, privacy, legal, and compliance issues that arise with the use of virtual meeting platforms to replace in-person interactions. We offer basic principles and summarize the remedies that have been proposed.

# Virtual Meetings Present Unique Needs and Problems

This document focuses on security and privacy principles that are especially relevant to virtual meetings. We focus less on general principles, such as classic coding bugs and best practices for regular patching. While these can be equally important, because the principles there are the same as in many other computing environments, we do not focus on them in this document.

Virtual meetings differ from many other forms of Internet communications, as well as face-to-face meetings or phone teleconferences, in fundamental ways:

- Virtual conferencing is meant to reproduce as much as possible the warmth and conviviality of face-to-face meetings and as a result, often encourages audio and video connections that can reveal details of participants, their homes and their families. Virtual backgrounds can lure attendees into using them to hide details in their environment, but technical limitations (such as an warping of the background image as a participant moves) or sudden events (such as the entrance of a child or a pet) can reveal those details.
- Simple user errors may violate the user's privacy or the confidentiality of others, such as forgetting to turn off automatic recording, or sharing one's screen when a sensitive email message is displayed on it. Something displayed even momentarily could be isolated in a recording and revealed in detail, unlike a quick look at someone's screen that might occur in person.
- Platforms tend to provide recording capabilities, which hold the risk that information shared privately in the meeting may be seen later by people who were not invited. Even platforms that do not offer recording are susceptible to recording using screen-capture software. Especially when third-party programs are used, participants will typically not be notified that they are being recorded.
- Because the richness of information collected by these systems can be vast, the collection, use, and potentially selling of personal data to third parties by these platforms can have broader impacts than similar practices performed by other services.

- Some meetings draw people from many organizations and even members of the general public who choose to join. Connection information is often shared in an insecure manner, leaving open the risk of intrusions and zoombombing.
- It is often difficult to vet the identity of participants as attendees. Attendees in many cases can set any name they want and the list of participants often changes from one meeting to the next even in a series of related meetings. Controls for vetting the participants are often insufficient for the task.
- Partly to compensate for the loose definition of who is authorized to join, platforms may allow potential participants to view personal information of other participants.

In this document, we use the term *virtual meeting* to refer to a broad range of meetings conducted virtually. We use the term *virtual conferencing* to refer to the technology (e.g. virtual conferencing software or a virtual conference platform). The term virtual conferencing may not apply to a family meeting or a medical appointment held online.

### Attendee Expectations

People use virtual meetings to achieve as much of the visual and auditory richness of face-to-face meetings as possible. They bring to this online medium the cultural expectations they have built up for face-to-face meetings, which have always been part of human experience. They expect that:

- People will not record information about the meeting, or even the existence of the meeting.
- Information they don't choose to reveal cannot be revealed by the medium, and steps they take to disguise themselves will be successful.
- People will not be able to zero in on private details displayed only momentarily.
- People not invited to the meeting cannot snoop on it.
- No stranger will intrude or dominate the meeting.

This document describes how to help uphold these expectations.

### Categories of Problems

The recommendations in this document build on fundamental, frequently cited principles in security and privacy: the need to assess risk and create realistic threat models; defense in depth; ease of use for the security controls and features; fine-grained access control; individuals' control over sharing and archival or their personal data; information privacy and integrity; least privilege; minimization of data collection and sharing; security by design; security through obscurity; sensitive information should be short-lived; situational awareness; support for anonymity; transparency; user control over sharing of personal data; and zero trust.

# Target Audience

The security, privacy, legal, compliance issues inherent in virtual meetings affect a wide variety of stakeholders, including:

- **Developers** of virtual meeting software and platforms
- **Hosts** of virtual meetings
- **Attendees** of virtual meetings
- **Companies/Organizations** that set policies for some virtual meetings
- **Governments** that pass laws that have impacts on some types of virtual meetings

The principles and solutions we are recommending focus on features and safeguards that software developers should be designing into their platforms. In some cases, our focus is on steps hosts can take to configure their meetings and to set ground rules for participation. In other cases, our focus is on steps participants should take to protect themselves.

It is important for schools, universities, companies, and others to establish rules and policies for correct and legal use of these technologies in any given use case.

# Security Principles

In this section, we provide a set of recommendations and principles for dealing with security vulnerabilities in video conferencing platforms. As in any software system, security vulnerabilities are introduced when developers fail to sanitize inputs they receive from untrusted sources, fail to secure channels of communications, enable attackers to guess access credentials without authentication, or for other reasons . Recommendations and principles for dealing with these technical vulnerabilities are for the most part well-explored advice for general secure software development.  We focus on recommendations and principles that are specific to video conferencing rather than recommendations and principles that apply widely to any type of software system.

**S1. Platforms should be constructed initially, and evaluated and refined throughout their life cycles, to minimize or prevent both intentional and inadvertent disruption.**

> Developers should anticipate and address the impact of participants who might be unknowingly or intentionally disruptive. Meeting hosts should be familiar with the controls that their platform makes available and test the use of these controls prior to using a system for a live presentation.

There are many ways that a participant might inadvertently or intentionally disrupt a meeting, as simple as leaving a microphone on while having a side conversation, to sharing a text message, image, or computer desktop with objectionable content (recently coined “zoombombing”).

Platforms should provide hosts and moderators with straightforward, consistent, understandable, and easy-to-use tools for addressing such disruption, such as the ability to forcibly mute an attendee's microphone, to mute all microphones, to delete messages from chat, to delete files that have been shared as attachments, to forcibly remove an individual from a meeting, to block an individual from rejoining a meeting, and to ban an individual from attending meetings hosted by an organization.

Both platform developers and the hosts of meetings, especially large public-facing meetings, should proactively test their configurations with actions that a disruptive participant might take. Hosts should understand the features of the system at their disposal to shut down disruption, including disabling screen sharing for others and muting all participants.

Unfortunately, the abuse of electronic communications has been a characteristic since their inception. Unwanted and inappropriate email predates the commercial Internet, and today “spam” messages represent a considerable cost to both service providers and Internet infrastructure. Companies developing software and systems for hosting virtual meetings should expect that they will be equally targeted. Citron and Frank discuss the impact of these technologies on civil rights, equal access to public spaces and the need to address harassment, discrimination and abuse [E4]. They emphasize that caretakers of crucial spaces have affirmative obligations to maintain them in ways that promote equal access, and that they can and should be held accountable when they fail to do so.

**S2. Platform architecture should incorporate end-to-end encryption of meeting data, both in transit and in archival form.**

By definition, participants in virtual meetings are sharing a rich set of personal data including their voice, video of themselves, the inside of their homes or offices, at times video of their family or coworkers who may find themselves inadvertently captured. This is not data that should be sent in unencrypted format across the public Internet. [E2]

Because recordings can be passed around or stored in insecure ways, the option of encrypting the file storing the recording is a valuable option.

**S3. Recordings should be stored in a protected location. Default options for recordings should include encryption, sharing only with designated individuals, and a limited retention period.**

It is important that the default options for recordings make it straightforward for users to protect the recordings. It should take extra steps to make a recording publicly accessible and available in an unencrypted form. We also recommend that the default settings for recordings be for a specific and limited period of time.

**S4. Platform design should permit hosts and other administrators to:**

**a) specify access control on several levels, per session, and per participant, as well as to provide useful default settings**

When video conferencing is used in a wide range of meetings from family gatherings to public religious services, the hosts as well as the individual attendees need to be able to change settings without going back to the defaults each time and switching them back and forth.

Platforms can improve the usability of their security and privacy controls by having predefined default settings for different kinds of meetings: a small trusted group, a small but public meeting, a classroom, and a large public meeting.

**b) determine the level of trust among participants (rather than the software making assumptions of trust based on shared characteristics such as a common domain name)**

Some virtual meeting systems have assumed that all users from the same domain name belong to the same organization. This is an incorrect assumption and has the potential to result in both privacy and security breaches. [10, 14, 17, 19, 25, 26]

More broadly, platforms should not assume that shared characteristics between users implies a degree of trust or that the users are from the same organization.

**c) make detailed access control choices for a meeting once and then easily reuse them as a template for other similar meetings**

Platforms offer a wide variety of host controls, including muting participants, designating co-hosts, allow screensharing, recording the meeting (video, audio,

chat), enabling a waiting room and many others. Unfortunately, in some platforms, these settings may be scattered through a web interface and in-meeting controls, and each setting applies to all of a host's meetings. The more it is difficult to find, set, and save these controls appropriately, the more problems hosts and users will have. Forcing hosts to find and set a wide variety of fine-grained control for each new meeting is a recipe for error and an invitation for attack. Individuals may host a wide variety of different kinds of meetings and they shouldn't need to change a large number of settings in between meetings of different kinds.

**d) generate fresh contact information for each authorized participant without forcing a reset of all access controls for each meeting**

Persistent URLs are popular for regularly held meetings because they simplify administration and publication of meetings; participants can simply return to the same URL each time. However, they are a central contributor to the abuse of "zoombombing," because they tend to spread beyond the people whom the host has invited, and may be detected by malicious actors. Do not assume that the "secret" URL will remain so. Platforms should offer an option to generate fresh contact information (such as the URL for joining a meeting) or fresh keys for each new session.

Convenience needs to be balanced with security on this issue. Stable URLs for meetings that are always shared only with trusted parties can still be useful in some contexts. But offering fresh URLs, while still maintaining all the access control and security/privacy settings, is important for meetings where the URL is announced publicly.

A password can provide additional security, if it is not shared publicly. Be aware that neither email nor SMS text messaging is normally secure. Moreover, SMS text messages are stored by the cellular provider and can be viewed by other people who share your cellular account.

**e) employ robust vetting functions to control meeting access**

Carefully consider the ways in which an attendee could misrepresent themselves when attempting to gain access to a meeting. Offer hosts a range of options from a list of pre-approved attendees with individual access credentials to mechanisms for vetting unknown participants (e.g. allowing participants to leave a message describing their reason for joining).

**f) designate and enable additional individuals to assist with discrete conference functions, including specifically attendee vetting and disruptive attendee management**

Virtual meeting platforms should have the capability to have a meeting managed by more than one person at a time. Ideally, this should be done by having multiple accounts designated with some degree of administrative capability over the meeting, and *not* by having more than one person log in simultaneously to the meeting using the same account.

Face-to-face meetings often have a co-host or a moderator, allowing one person to chair the meeting, while another takes minutes and perhaps a third acts in the role of facilitator. In conferences, while the speaker concentrates on making a presentation, other hosts or designees often check for audience questions and comments or deal with the registration of new attendees. Such approaches also work well in virtual meetings: although intelligent software can serve some of these functions, complex meetings  create many tasks, both technical and organizational.

Co-hosts may be able to notice inappropriate and disruptive behavior before the host, if the host is busy facilitating and leading the meeting.If there is a waiting room, a trusted person should be asked to greet participants and authorize their entry, so that the host can concentrate on leading the meeting. It is also useful to have someone check screens to catch any improper behavior by a participant, and for someone to check for raised hands or important chat messages.

# Privacy Principles

In this section, we provide a set of recommendations and principles for dealing with privacy vulnerabilities in video conferencing platforms.  As in any software system, privacy vulnerabilities are introduced when platforms collect and sell information about users to third parties. (This vulnerability is caught by the common observation, “If you are not paying for the product, you are the product”--and even if you are paying, you are likely the product.) This is a serious problem, but far from unique to virtual conferencing. We focus especially on privacy vulnerabilities that are more specific to virtual conferencing. In order to break out of the one-dimensional emotional connection to which many digital technologies are restricted, virtual conferencing encourages audio and video connections that may reveal details of participants and details from their personal spaces including private data of family and co-workers. In this way, virtual conferencing can present unique privacy vulnerabilities in the way it leaks private

information between attendees and to the host, or the way in which recordings of this information could be leaked to the wider world.

**P1. Platform users should be clearly and completely able to determine:**

**a) whether the meeting is being recorded, by means of a clear and accessible indicator**

**b) what information about them is visible to other conference participants**

Make it clear when information provided by a participant will be visible to others, including the host. Avoid features that imply a level of privacy that is not fully supported. Features that allow “attention tracking,” or that give hosts access to the contents of person-to-person chat marked “Private,” violate participants’ assumptions about the visibility of their information. Platforms should never implement a feature that supports surveillance of participants in a manner that is unknown to the participants. The platforms should also be careful not to offer or advertise features that imply a level of privacy that is not enforced or supported by the platform.

Violations of this principle are unfortunately common. Many web sites include icons that encourage visitors to “like” the site on social media platforms (https://www.engadget.com/2019-07-29-facebook-like-button-data-liability-websites-eu.html). Even if the visitor doesn’t touch the icon, information collected by site on the visitor is automatically sent to the social media platform. Another violation is sending information about the participant, which may include search terms containing sensitive information, to data brokers (https://www.vice.com/en_us/article/539qzk/looking-up-symptoms-online-these-companies-are-collecting-your-data).[11, 26]

Following the general understanding that all personal data can be used to classify or discriminate against people, including data about the use of the platform and the connections made, platforms should be careful to collect only data that the individual has explicitly offered, and to share it with third parties only after obtaining consent from the individual.

**c) who is hosting the conference and what controls the host is applying to the meeting**

Hosts are given controls to help a meeting run smoothly and to mute or eject intruders. The host should explain, before the meeting or at the beginning of the meeting, how these controls will be used--for instance, whether everyone starts

off muted and cannot talk until unmuted by the host. Transparency will establish that the controls are used fairly and will help everyone participate successfully.

If the host is recording, that should be clear to participants. The person who is recording should announce that it's in effect and should ask whether anyone objects, and should explain the purpose of recording, who will see it, how long it will be preserved, and other relevant parameters. A platform should also display the parameters--what is being saved, how it will be shared, etc.--in ways that are clearly noticeable by all attendees. People should be able to drop out before recording starts, leaving a record of them being in the meeting.

Any rules regarding the meeting, including non-disclosure agreements and regulatory requirements, should be disclosed to all participants before the meeting gets underway, just as in face-to-face meetings or phone calls. For instance, investment bankers may be required to record conversations that could be construed as investment advice.

**P2. Platforms should enable users with:**

**a) opt-in or, at minimum, opt-out, controls for attendees;**

Platforms should offer attendees simple ways to control information displayed or shared about themselves. Hosts and other attendees may be able to capture these inputs through the "analog hole" (e.g. taking a recording with their cell phone of everything displayed), but the platform should not make that process easy or high quality by allowing hosts or others to record information outside the knowledge or control of the attendees [E3]. Participants could and should be asked to abide by a set of rules for recording other participants through screenshots or other means of capture.

**b) support for post-meeting editing (including "undo" functionality);**

Consider the ease with which participants might accidentally and momentarily unmute or share their whole desktop. There needs to be some kind of undo operation for striking that from the permanent record. However, to mitigate against editors abusing the undo feature to remove material they don't want to preserve, the edited video should be marked as changed.

**c) anonymous or pseudonymous participation options,**

Hosts will need to balance the use of these features with their ability to deal with disruptive participants. The ability to join group discussions without identifying oneself has made the Internet a powerful draw, almost from its start, for people

with stigmatized or marginalized traits such child abuse, addiction, and homosexual behavior.

Many meetings require careful vetting of participants, of course, but other meetings such as 12-step addiction programs should permit people to participate without identifying themselves. A host or designee could still talk to the participant to vet their attendance before they join. For some meetings, participant may need to be allowed to use pseudonyms or no name at all, allowed to turn off video, and even use software to disguise their voice. Meetings of this type may be more vulnerable to disruption given the lack of vetting and may need an actively engaged co-host to intervene in case of disruption.

**P3. Platforms should not:**

**a) collect user information not needed to provide the platform's service;**

**b) provide a user's information to third parties unless individual users make a clearly presented choice to opt-in to such data sharing.**

Obeying these principles means choosing a business strategy at the founding of the company that is not dependent on payments for data from third parties, whose goals may not be benign, as shown in cases such as Cambridge Analytica (https://epic.org/privacy/facebook/cambridge-analytica/).

Surveillance is a lamentable tendency throughout our digital lives, extending from governments to retail institutions, web sites, and employers. These intrusions into personal privacy not only produce resentment and anxiety (if the targets even know that the surveillance is happening); they are also usually discriminatory and ineffective. Normally, something that can be measured--such as the time spent looking at a place on the screen (https://www.tobii.com/group/about/this-is-eye-tracking/)--is taken as a proxy for some desired trait, such as paying attention. Such crude measures ignore perfectly good reasons for people to fail the test; for instance, they may be paying attention while looking at a document related to the meeting. They may even be blind. [9]

**P4. Hosts should designate, and attendees should be encouraged to follow, a code of conduct for the meeting which includes:**

**a) notification by participants to other attendees when non-participants nearby may be able to hear or see the meeting; and**

Physical meetings offer opportunities to record audio, video or other information on other participants, but virtual meetings offer many more and make it even easier to do so without the knowledge of participants. Virtual meetings also offer the opportunity for others to be “present” in the meeting without the knowledge of others participants. Privacy in virtual meetings is not just the job of the platform, but also the job of the hosts and other attendees. Hosts should set clear expectations and codes of conduct for attendees and ask those attendees to agree to and abide by them. We especially encourage hosts to specify expectations around non-participants who may be able to hear or see the meeting and specifically asking that attendees notify other participants when others are listening/watching.

**b) limits on capturing and/or sharing screenshots and other meeting information.**

Virtual conferencing platforms can enable recording of a meeting, but recordings of various kinds are also possible using other tools. We encourage hosts to specify what is acceptable for attendees to capture for their personal use and to set clear limits on further distribution where appropriate.

# Legal and Compliance Issues

Organizations that adhere to regulations such as HIPAA or FERPA must use platforms that have passed certifications in the relevant areas. The organizations must then ensure that the participants employ features such as encryption that conform to those regulations.

Just as other new media create new legal problems (for instance, "sexting" after mobile phones allowed pictures to be included in text messages), virtual conferencing may cast a new light on old problems and create unprecedented problems of its own, which may or may not be addressed by legislatures. [8, 35, G4]

# References

**General news reports**
[1] Zoom admits user data ‘mistakenly’ routed through China
https://www.ft.com/content/2fc518e0-26cd-4d5f-8419-fe71f5c55c98

[2] ‘Zoombombing’ Attacks Disrupt Classes
Online Zoom classes were disrupted by individuals spewing racist, misogynistic or vulgar content. Experts say professors using Zoom should familiarize themselves with the program's settings.

By Elizabeth Redden
March 26, 2020
https://insidehighered.com/news/2020/03/26/zoombombers-disrupt-online-classes-racist-pornographic-content

[3] Do you know how Zoom is using your data? Here's why you should
Arwa Mahdawi
April 1 2020
https://www.theguardian.com/commentisfree/2020/apr/01/do-you-know-how-zoom-is-using-your-data-heres-why-you-should

[4] ‘Zoom is malware’: why experts worry about the video conferencing platform
https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing
“In 2019, it was revealed Zoom had quietly installed a hidden web server on user devices that could allow the user to be added to a call without their permission. And a bug discovered this week would enable hackers to take over a Zoom user’s Mac, including tapping into the webcam and hacking the microphone.”

[5] A Must For Millions, Zoom Has A Dark Side — And An FBI Warning
April 3, 20205:00 AM ET
Shannon Bond
https://www.npr.org/2020/04/03/826129520/a-must-for-millions-zoom-has-a-dark-side-and-an-fbi-warning

[6]Zoom is Leaking Peoples' Email Addresses and Photos to Strangers
Joseph Cox
April 1 2020
https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos

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

[7] ‘Zoombombing’: When Video Conferences Go Wrong
By Taylor Lorenz
Published March 20, 2020
https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html

[8] New York Attorney General Looks Into Zoom’s Privacy Practices
By Danny Hakim and Natasha Singer
March 30, 2020
https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html

[9] People are skipping Zoom meetings by looping videos of themselves paying attention
by BRYAN CLARK
https://thenextweb.com/corona/2020/03/23/adapt-evolve-overcome/

https://thenextweb.com/security/2020/04/03/zoom-is-a-godforsaken-mess-but-it-can-be-fixed/
[10] Zoom found leaking personal user data, could also facilitate stealing your Windows sign-in credentials (updated)

You could potentially be video-called by strangers
By Humza Aamir, Today 5:10 PM
https://www.techspot.com/news/84641-zoom-found-leaking-personal-user-data-owing-how.html

[11] Zoom updates iOS app so that it stops sending user information to Facebook
By team91 -March 31, 2020
https://www.91mobiles.com/hub/zoom-ios-app-update-stop-sending-user-data-to-facebook

[12] Ex-NSA hacker drops new zero-day doom for Zoom
Zack Whittaker@zackwhittaker / 10:00 am EDT • April 1, 2020
https://techcrunch.com/2020/04/01/zoom-doom
“Zoom uses a “shady” technique — one that’s also used by Mac malware — to install the Mac app without user interaction. Wardle found that a local attacker with low-level user privileges can inject the Zoom installer with malicious code to obtain the highest level of user privileges, known as “root.”

[13]Zoom freezes feature development to fix security and privacy issues
Romain Dillet@romaindillet / 5:34 am EDT • April 2, 2020
https://techcrunch.com/2020/04/02/zoom-freezes-feature-development-to-fix-security-and-privacy-issues/

[14]
https://arstechnica.com/information-technology/2020/04/unpatched-zoom-bug-lets-attackers-steal-windows-credentials-with-no-warning/

[15] Privacy, security concerns for Zoom users, official says
March 31, 2020
https://abc7chicago.com/zoom-video-conferencing-teleconferencing-meeting/6065240/

[16] Hackers Take Advantage of Zoom's Popularity to Push Malware
By Sergiu Gatlan
March 30, 2020
https://www.bleepingcomputer.com/news/security/hackers-take-advantage-of-zooms-popularity-to-push-malware/

[17] Zoom Lets Attackers Steal Windows Credentials via UNC Links
By Lawrence Abrams
March 31, 2020
https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-via-unc-links/

[18]
https://www.zdnet.com/article/zoom-defends-use-of-local-web-server-on-macs-after-security-report/
Zoom is leaking some user information because of an issue with how the app groups contacts.

[19] Another security issue for Zoom
By Jay Peters@jaypeters  Mar 31, 2020, 6:11pm EDT
https://www.theverge.com/2020/3/31/21201956/zoom-leak-user-information-email-addresses-photos-contacts-directory

[20]
https://www.theverge.com/2019/7/8/20687014/zoom-security-flaw-video-conference-websites-hijack-mac-cameras

[21]https://www.macrumors.com/2019/07/09/zoom-videoconferencing-app-vulnerability/

[22]Employees at home are being photographed every 5 minutes by an always-on video service to ensure they're actually working — and the service is seeing a rapid expansion since the coronavirus outbreak
Aaron Holmes Mar 23, 2020
https://www.businessinsider.com/work-from-home-sneek-webcam-picture-5-minutes-monitor-video-2020-3

[23]Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing
Micah Lee, Yael Grauer
March 31 2020,
https://theintercept.com/2020/03/31/zoom-meeting-encryption/

[24]
https://theintercept.com/2020/04/03/zooms-encryption-is-not-suited-for-secrets-and-has-surprising-links-to-china-researchers-discover/

[25] https://www.cnn.com/2020/04/04/us/nyc-schools-zoom-online-security/index.html

[26] A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles
New York Times
April 2, 2020

By Aaron Krolik and Natasha Singer
https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html

[27] Zoom 'unsuitable' for government secrets, researchers say
BBC
April 3, 2020
By David Molloy & Joe Tidy, BBC News
https://www.bbc.com/news/technology-52152025

[28] Three Attorneys General Raise Zoom Security Concerns
Law Street Media
April 7, 2020
by Kirsten Errick
https://lawstreetmedia.com/tech/three-attorneys-general-question-zoom-about-security/

[29] Zoom's Data Sailing Into China: FBI Issues Warning of Counterintelligence Threat
April 6, 2020
by Christopher Burgess
https://news.clearancejobs.com/2020/04/06/zooms-data-sailing-into-china-fbi-issues-warning-of-counterintelligence-threat/

[30] Letter by U.S. Senator Richard Blumenthal to Eric S. Yuan,CEO and Chairman, Zoom Video Communications
March 31, 2020
https://www.blumenthal.senate.gov/imo/media/doc/2020.03.31%20-%20Zoom%20-%20Privacy%20.pdf

[31] U.S. Senate tells members to avoid Zoom over data security concerns: FT
April 9, 2020
by Philip George
https://www.reuters.com/article/us-zoom-video-commn-privacy-senate-idUSKCN21R0VU

[32] Taiwan tells agencies not to use Zoom on security grounds
April 7, 2020
by Supantha Mukherjee, Ben Blanchard
https://www.reuters.com/article/us-zoom-video-commn-privacy-taiwan-idUSKBN21P1MK

[33] Google Told Its Workers That They Can't Use Zoom On Their Laptops Anymore
April 8, 2020
Pranav Dixit
https://www.buzzfeednews.com/article/pranavdixit/google-bans-zoom

[34] Thousands of Zoom video calls left exposed on open Web
April 3 2020
https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/

[35] Attorney General Says His Call Was Zoombombed, Urges Safe Video Conferencing
April 3 2020
https://www.nbcconnecticut.com/news/local/attorney-general-says-his-call-was-zoombombed-urges-safe-video-conferencing/2249848/

[36] How Americans see digital privacy issues amid the COVID-19 outbreak
May 4, 2020
Brook Auxier
https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/

**Expert analysis**

[E1] Security and Privacy Implications of Zoom
Bruce Schneier, April 3, 2020
https://www.schneier.com/blog/archives/2020/04/security_and_pr_1.html

[E2]Trusting Zoom?
Steven Bellovin, April 6, 2020
https://www.cs.columbia.edu/~smb/blog/2020-04/2020-04-06.html

[E3] More on Zoom and privacy
Includes dive into Zoom's user options for privacy
Doc Searls
https://blogs.harvard.edu/doc/2020/03/28/more-zoom/

[E4] Cyber Civil Rights in the Time of COVID-19
Danielle Citron and Mary Anne Franks, May 14, 2020
https://blog.harvardlawreview.org/cyber-civil-rights-in-the-time-of-covid-19/

**Lawsuits**

[L1] Michael Drieu, Individually and On Behalf of All Others Similarly Situated, v. Zoom Video Communications, inc., Eric S. Yuan, and Kelly Steckelberg: Class Action Complaint for Violations of the Federal Securities Laws
https://drive.google.com/file/d/1js5_XZdA7-uOemikUhRzekPWVBtB5heL/

[L2] Samuel Taylor, On Behalf of Himself and All Others Similarly Situated, Plaintiff, v. Zoom Video Communications, Inc.: Class Action Complaint

https://drive.google.com/file/d/1utrCNVLLNRcwIHrpTmFr88lt3F2vkYQ9/

**Zoom announcements**

[Z1] CEO Eric S. Yuan
https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

[Z2]
https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/

[Z3]
https://support.zoom.us/hc/en-us/articles/360041591671-March-2020-Update-to-sharing-settings-for-Education-accounts

**Practical guidelines**

[G1] “Virtual Conferences: A Guide to Best Practices”
ACM Presidential Task Force on on What Conferences Can Do to Replace Face-to-Face Meetings
http://www.acm.org/virtual-conferences

[G2] “How to Keep Uninvited Guests Out of Your Zoom Event”
March 20, 2020
https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/

[G3] “Zoom-bombing: How to keep trolls out of your Zoom meetings”
March 24, 2020
https://www.tomsguide.com/news/stop-zoom-bombing

[G4] “FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic”
March 30, 2020
https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

[G5] “How to Secure Your Zoom Meetings from Zoom-Bombing Attack”
March 31, 2020
https://www.bleepingcomputer.com/news/software/how-to-secure-your-zoom-meetings-from-zoom-bombing-attacks/

[G6] “Who’s Zooming Who? Guidelines on How to Use Zoom Safely”

Omri Herscovic
https://blog.checkpoint.com/2020/03/26/whos-zooming-who-guidelines-on-how-to-use-zoom-safely/

[G7] “How to Prevent "Zoombombing"”
March 30, 2020
https://www.adl.org/blog/how-to-prevent-zoombombing

[G8] “Neuromatch anti zoombombing script”,
Konrad Kording, April 1 2020.
https://medium.com/@kording/neuromatch-anti-zoombombing-script-842eabf160dc

[G9] “Privacy not included: video call apps”
Mozilla Foundation
https://foundation.mozilla.org/en/privacynotincluded/categories/video-call-apps/

**Related Policy Documents**

[P1] ACM Code of Ethics
https://www.acm.org/code-of-ethics

[P2] USACM STATEMENT ON THE IMPORTANCE OF PRESERVING PERSONAL PRIVACY, March 2018
https://www.acm.org/articles/bulletins/2018/march/usacm-statement-on-data-privacy
https://www.acm.org/binaries/content/assets/public-policy/2018_usacm_statement_preservingpersonalprivacy.pdf

[P3] USACM Statement on Computing and Network, May 2017
Securityhttps://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_computingandnetworksecurity.pdf
https://www.acm.org/media-center/2017/may/usacm-statement-on-network-security

[P4] USACM Statement on Accessibility, Usability, and Digital Inclusiveness, September 2017
https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_accessibility.pdf