



Protecting the Privacy of Your Video Conversations

Understanding the differences between Zoom and Signal App

By Jeff Reifman

Preface

If you're not interested in understanding how to protect your private conversations but you just want to have the most secure messaging and one-to-one video calling software application, use the [Signal app](#) and do not hold conversations on Zoom that you require to remain private. Currently, Signal's video encryption is only available on its Android and iOS apps. Signal's secure text messaging is available on additional platforms.

If you need video conferencing for up to four people or phone calls with up to ten and you want the flexibility for desktop video conferencing, consider [Wire](#). There are no strongly secured solutions for larger group conversations at this time.

Introduction

Certainly, the COVID-19 outbreak has mainstreamed video conferencing and Zoom has been the biggest beneficiary. It's not just being used in professional settings but also for organizing, socializing, interpersonal communication and telehealth. In fact, telehealth and mental health conversations hosted on Zoom may make up some of virtual conferencing's most intimate and sensitive content. But Zoom is not a fully private service. Fortunately, there's a more private alternative for one on one conferencing needs, [Signal](#).

Until Congress enacts a privacy Bill of Rights for Internet consumers, it's up to us to protect ourselves online. We must learn as much as we can about how our data is used and protected during all of our internet-based activity. And, it's important we consider how the unsuspected, unanticipated and unwanted distribution of our data may negatively impact our life.



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).
www.aspirationtech.org • info@aspirationtech.org

What would happen if strangers obtain our phone number, our home address, our banking password, private or intimate photos, a health diagnosis or audio and video of a deeply personal mental health conversation?

This process of consideration is called threat modeling. Learning to threat model the use of common video chat and conferencing solutions such as Zoom and Signal can help you understand and prepare for how your data may or may not be compromised or shared.

First, we'll review why Zoom video conferencing is not safe for private conversations and ill-advised for telehealth. Then, we'll talk about Signal and how it's been designed specifically to maximize privacy. Lastly, we'll review the state of telehealth privacy and discuss how to interpret frequently vague claims of privacy by corporations in the media.

Problems at Zoom

Zoom has had a lot of problems since 2019. Apple had to push a silent update to block hackers from surreptitiously accessing Zoom's users' Macbook cameras¹. In 2020, Zoom confirmed allegations from a class action lawsuit that it was sharing its meeting participants' personal data with Facebook². The lawsuit alleged Facebook could use this data to target advertising at Zoom users. During the 2020 pandemic, Zoom's service has been hit by a rash of "Zoombombings"³ in which intruders gain illicit access to meetings and post pornographic or white supremacist audio and imagery. But still worse - Zoom's misled users about the safety and security of their video calls.

The company did not encrypt the video of calls made at the free account level at all until it says it began doing so May 30th, 2020⁴. And, on June 3rd, USA Today reported⁵, Zoom's CEO said, "the company has no plans to offer end-to-end encryption to users of its free version so it can continue working with law enforcement." But even that comment is misleading.

The term "end-to-end encryption" specifies that only the parties of communication (text message, phone call, video conference, et al.) hold security keys for the encrypted data and no other party can access the content.

¹ [Apple pushes new silent updates to address vulnerable Zoom software \(Macworld\)](#)

² [Lawsuit: Zoom illegally sold users' personal data \(CBS News\)](#)

³ [Zoombomber crashes court hearing on Twitter hack with Pornhub video \(Ars Technica\)](#)

⁴ [It's Here! 5 Things to Know About Zoom 5.0 \(Zoom Blog\)](#)

⁵ [Zoom CEO: No end-to-end encryption for free users so company can work with law enforcement \(USA Today\)](#)



Zoom does not currently use true end-to-end encryption on its free or paid accounts. Thus, whether a Zoom account is free or paid is not a barrier to them sharing meeting calls with law enforcement.

Since Zoom's servers issue and control the encryption keys for its paid users' meetings, the company can share those keys with law enforcement or anyone, thus exposing your private calls.

The lack of true end-to-end encryption leaves even Zoom's paid account's video calls vulnerable to surveillance. And, this includes telehealth calls. How does all of this impact you?

Your threat model for Zoom's current service should include the possibility that any of the following entities could surveil your video calls and conferences and gain access to your call recordings or metadata about your conversations:

- Zoom and its employees
- IT staff or other employees assigned to administer Zoom business accounts which may encompass telehealth accounts at a medical facility.
- Lawful government actors and police through warrants and national security requests
- Third party companies Zoom might privately sell data to or share data with
- Potentially, any third party contractors Zoom hires to review audio and improve its transcription or general knowledge about its users' activities. Both Apple and Amazon have used contractors to listen to Siri and Alexa users without their knowledge⁶.
- A disgruntled, malevolent, voyeuristic or financially compromised Zoom employee who seeks blackmail or financial gain by selling or publishing your data
- Unlawful government actors through sophisticated technological penetration and surveillance of the Zoom network
- Unlawful government actors or a highly sophisticated hacker that gains control of your laptop or smartphone to monitor video and audio directly — independent of Zoom or Signal. No conferencing software can protect you from this attack.

Let's examine Zoom's claims of end-to-end encryption and its importance.

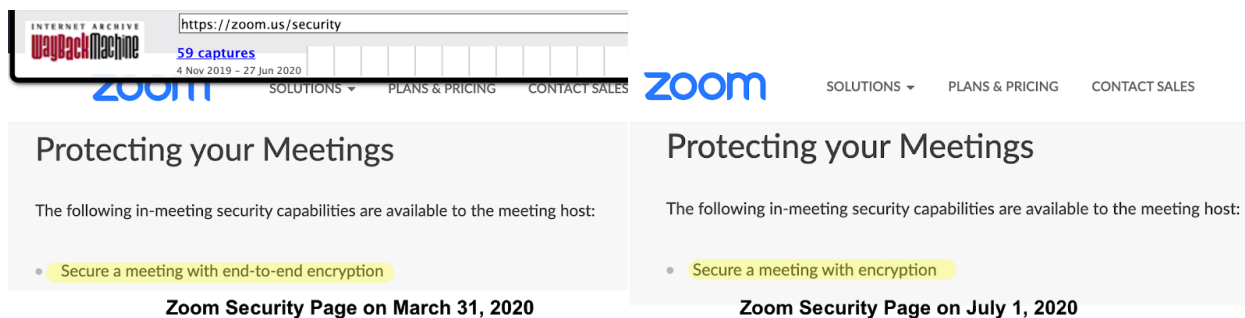
⁶ [Thousands of Amazon Workers Listen to Alexa Users' Conversations \(Time\)](#)



Zoom Lacks End-to-End Encryption

Zoom documentation misled consumers about encryption. Its encryption is insecure because it does not use end-to-end encryption, and the encryption it deployed prior to May 30th had proven vulnerabilities.

On the left below, you can see the [Zoom website Security page from March 31st](#) in the Wayback Machine claiming “end-to-end encryption”. On the right, you can see the page [June 27th](#) below saying just “encryption”:



And, Zoom’s Chief Product Officer Oded Gal confirmed this on April 1st, “...we want to start by apologizing for the confusion we have caused by incorrectly suggesting that Zoom meetings were capable of using end-to-end encryption.”

The term end-to-end encryption means that only the parties involved in a conversation (e.g. texting, email, audio or video) have the means to access the content of the conversation. Signal provides this service but Zoom does not.

For example, Zoom offers a cloud-based [audio transcription service](#), such a service would be impossible to offer in the cloud if the conversation was encrypted end-to-end. No service at Zoom would be able to decrypt an end-to-end encrypted conversation.

Citizen Lab Assesses Zoom’s Security

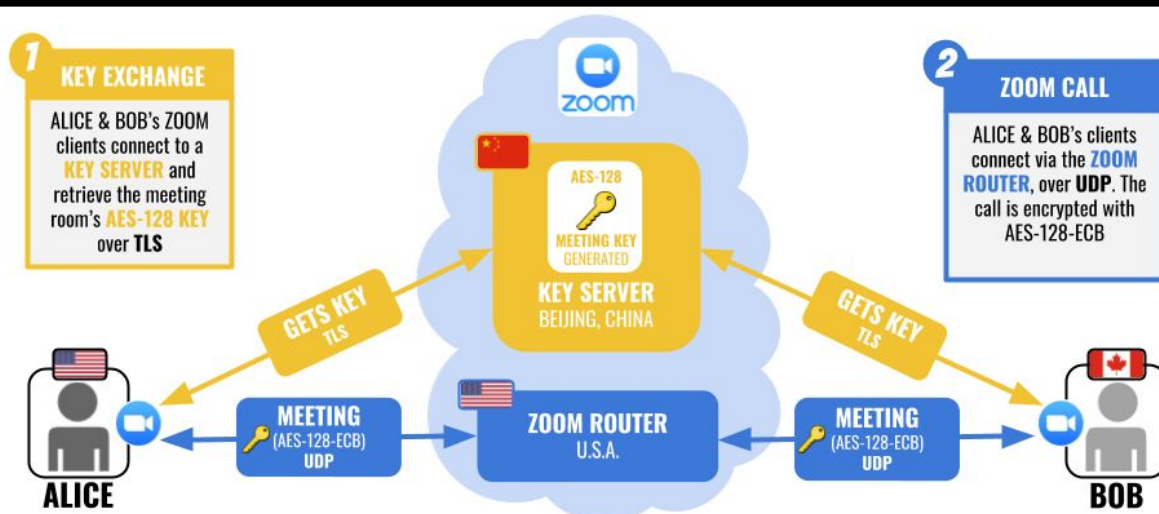
On April 3rd, Citizen Lab, a highly respected University of Toronto research lab, published [an analysis of Zoom security](#) which reported that Zoom software is developed by 700 employees in three Chinese subsidiaries and that Zoom’s encryption keys for meeting participants are sometimes distributed by servers in China.

“the mainline Zoom app appears to be developed by three companies in China, which all have the name 软视软件 (‘Ruanshi Software’). Two of the three



companies are owned by Zoom, whereas one is owned by an entity called 美国云视频软件技术有限公司 ('American Cloud Video Software Technology Co., Ltd.')

OBSERVING A TEST ZOOM CALL



NOTE: Citizen Lab observed these server locations during a test call. Other ZOOM calls may use servers and call routers in other locations.

During a test of a Zoom meeting with two users, one in the United States and one in Canada, we found that the [encryption] key for conference encryption and decryption was sent to one of the participants ... from a Zoom server apparently located in Beijing...A scan shows a total of five servers in China and 68 in the United States that apparently run the same Zoom server software as the Beijing server. ... A company primarily catering to North American clients that sometimes distributes encryption keys through servers in China is potentially concerning, given that Zoom may be legally obligated to disclose these keys to authorities in China.” - [Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings \(Citizen Lab\)](#)

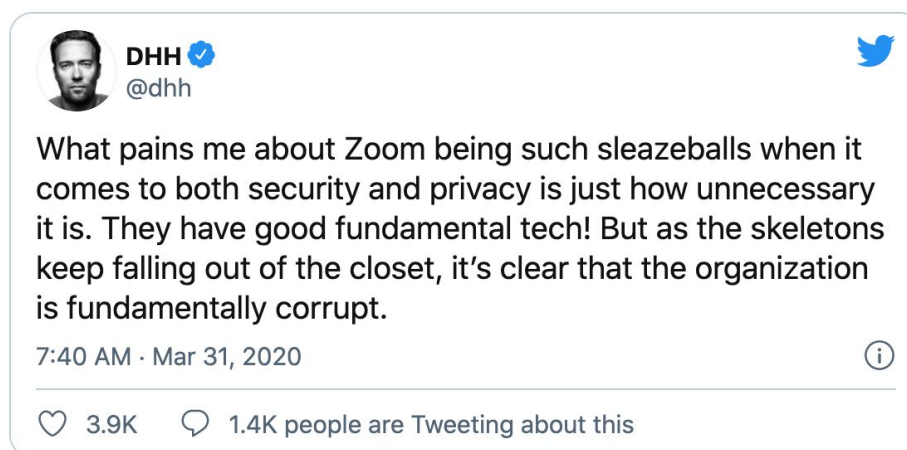
Certainly, this raises concerns in our threat model for China's role in Zoom's operations and meetings conducted in the United States et al.

Mathew Green, a cryptography professor at John Hopkins, tells Wired, "If you build a system where everything comes down to trusting the server, you might as well dispense with all the complexity and forget about end-to-end encryption."⁷

⁷ [WhatsApp Flaws Could Allow Snoops to Slide Into Group Chats \(Wired\)](#)



David Heinemeier Hansson, co-founder of HEY, BaseCamp and creator of programming language Ruby on Rails tweets that Zoom is “fundamentally corrupt”⁸.



It's important to threat model China's involvement in our online activities. Zoom isn't the only application developed in China and subject to government surveillance. Recently it was revealed that another Chinese-made app, TikTok, copies the contents of the users clipboard regularly while they are typing and this can include passwords and sensitive information. Here's Daring Fireball blogger, John Gruber⁹:

"TikTok ... is a Chinese company whose popularity algorithm is a black box. If you use TikTok you should assume they've stored a copy of anything and everything you've had on your clipboard while using the app. Their slogan might as well be 'Chinese state-sanctioned social media' — which to me says don't use them, but maybe that's just me."

When a nation state can access our personal data and conversations, it can use this information for blackmail, targeting voters (as Russia does), selling to third parties for profit, et al.

On July 27th, the Biden US Presidential campaign ordered its staffers to delete TikTok from their devices due to security concerns¹⁰.

It's reasonable to have similar concerns for Zoom's development in China as we do for TikTok.

Ultimately, the involvement of Zoom's servers in encryption key distribution undermines its claims of end-to-end encryption. By distributing keys itself, Zoom exposes its video

⁸ [David Heinemeier Hansson Tweets on Zoom's Fundamental Corruption](#)

⁹ ['Repetitive, Spammy Behavior' Indeed \(Daring Fireball\)](#)

¹⁰ [Biden's staff must delete TikTok from their personal and work phones \(The Verge\)](#)



conversations to additional threats e.g. possibly undisclosed use of our data, disgruntled employees, government surveillance such as China, hackers targeting Zoom's servers, et al.

On May 7th, Zoom acquired Keybase¹¹ with the goal of building true end-to-end encryption into its services but there is no clear timeline on when this will be completed. True end-to-end encryption would also conflict with Zoom's prior claims that it needs to be able to provide the content of calls to law enforcement.

Zoom's Actual Encryption Had an Inherent Weakness

To understand the strength of any encryption process, you'll often hear that the length of the encryption key plays an important role. The longer the key, the stronger the encryption and longer key encryption dramatically increases the number of days, months or years that an attacker's computer might require to decrypt your conversations.

The NSA previously recommended¹² 256-bits for top secret documents, approximately equivalent to a 36 character password, before removing the document from public view. Security journalist Patrick Nohe says, even if you use "...the fastest supercomputer in the world, it will take millions of years to crack 256-bit AES encryption."

Certainly key length matters; however, one security expert we consulted suggested that algorithms used in encrypted communication play more of a role.

CitizenLab found that Zoom deceived users about its encryption key length and it used an unfavored algorithm with a known weakness.

Zoom's Security web page has consistently [reported](#) that it uses 256-bit encryption, that wasn't the case in April 2020 and Zoom has now admitted that it wasn't the case prior to May 30th, 2020 with the update of Zoom 5.0 and enforcement of its use¹³.

¹¹ [Zoom Acquires Keybase and Announces Goal of Developing the Most Broadly Used Enterprise End-to-End Encryption Offering \(Zoom Blog\)](#)

¹² [NSA Suite B Cryptography NSA/CSS](#)

¹³ [It's Here! 5 Things to Know About Zoom 5.0 \(Zoom\)](#)

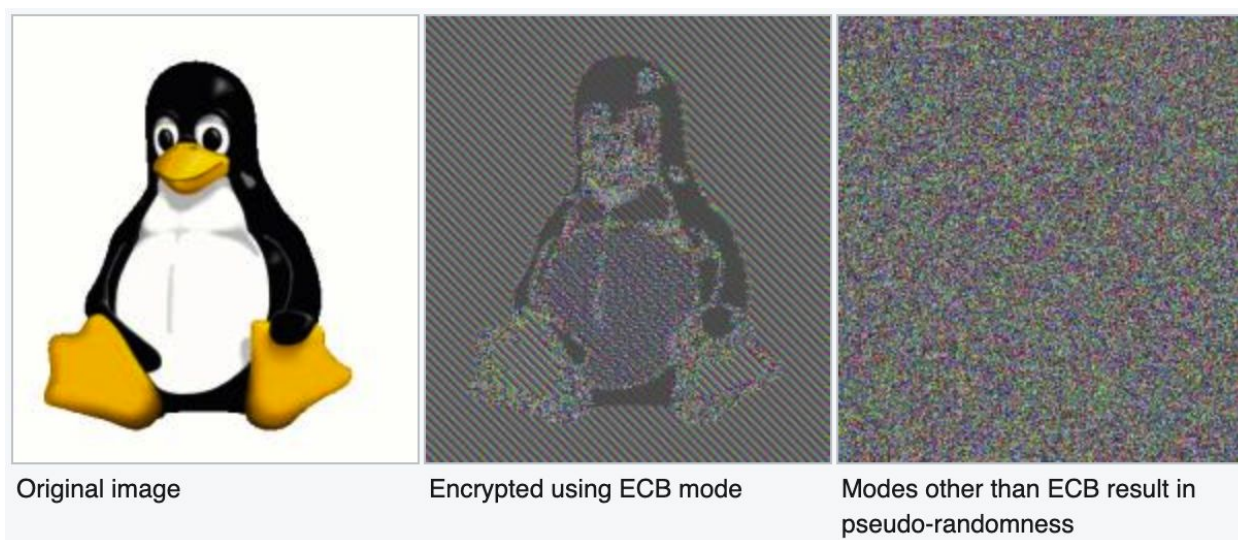




Protecting your Data

Communications are established using 256-bit TLS encryption and all shared content can be encrypted using AES-256 encryption.

“Citizen Lab found, “Zoom’s encryption and decryption use [128-bit] AES in ECB mode, which is well-understood to be a bad idea, because this mode of encryption preserves patterns in the input.” They cite this image from Wikipedia¹⁴ as an example:



According to CitizenLab, industry standard video streaming encryption is performed with alternatives to Zoom’s use of ECB.

In his April 1st blog post, Zoom’s Gal also says, “[the company] has never built a mechanism to decrypt live meetings for lawful intercept purposes, nor do we have means to insert our employees or others into meetings without being reflected in the participant list.”

¹⁴ [Block cipher mode of operation \(Wikipedia\)](#)



But Zoom already decrypts live video for participants during meetings — that’s what you’re watching in a Zoom call. It’s difficult to imagine that extending this code for a third party would be technically challenging.

Our threat model should consider that (a) Zoom may be lying, (b) China and the NSA may have these capabilities at this time and (c) attacking Zoom’s weak encryption is every skilled hacker’s 2020 project goal.

Zoom’s past deception casts doubt on its current claims and future promises.

Is Zoom Safe to Use?

If you’re sharing any information on Zoom that is completely private, you are taking a risk that your information will be acquired by unauthorized parties.

Similarly, if you’re having sensitive medical and mental health conversations on Zoom, you’re vulnerable to the same security weaknesses and threats described earlier. Medical facilities promoting Zoom for Health as “HIPAA¹⁵ compliant” and “encrypted” may be unintentionally misleading patients about the privacy of their video calls.

In addition to the risks of illegal surveillance and hacking, Zoom does not publish a transparency report which would show the number of government requests and disclosures of account and video data worldwide. Apple, Facebook, Google and others do publish these reports.

For example, Google’s transparency reports show that it has disclosed some portion or all of requested data to its requestors 82% of the time in the United States over the past five years¹⁶. That’s a high percentage rate of disclosure of user data.

With Zoom, there’s not even a way to know how much data has been disclosed to law enforcement in the United States or to state actors in China. In fact, it’s reasonable for our threat model to consider the possibility that China has access to data on demand.

Similarly Edward Snowden’s disclosures included the NSA PRISM program which allowed the NSA to collect data directly from companies such as Apple and Google. Imagine if the NSA has direct access to Zoom’s servers.

“PRISM collects stored internet communications based on demands made to internet companies such as Google LLC under Section 702 of the FISA

¹⁵ [Health Insurance Portability and Accountability Act \(Wikipedia\)](#)

¹⁶ [Google Transparency Report: Requests for user information](#)



Amendments Act of 2008 to turn over any data that match court-approved search terms. Among other things, the NSA can use these PRISM requests to target communications that were encrypted when they traveled across the internet backbone, to focus on stored data that telecommunication filtering systems discarded earlier, and to get data that is easier to handle.” - Wikipedia¹⁷

To its credit, Zoom has responded to its failings with a handful of promises:

- To improve its video encryption and make it available to users of free accounts
- Not to surveil, use or sell data from customers’ video calls or messages.
- To exclude China-based servers from key distribution and video conference data originating outside of China, which it says it has now done¹⁸.
- To begin publishing a regular transparency report revealing government requests and disclosures. (Keep in mind that transparency reports may not include FISA warrants, National Security Letters or other top secret requests where disclosure is forbidden. In Google’s case, they provide an additional report on National Security Requests¹⁹.)

But, instead of trusting this at face value, our threat model should consider the abundance of existing corporate apologies for breaking past promises.

¹⁷ [PRISM \(surveillance program\) \(Wikipedia\)](#)

¹⁸ [Data Routing Control is Here \(Zoom\)](#)

¹⁹ [United States National Security Requests for User Information \(Google\)](#)



Mark Zuckerberg apologizes for Facebook's data privacy scandal in full-page newspaper ads

Capital One CEO apologizes for data breach

Jeff Bezos offers apology for Orwellian mistake

Ex-Equifax CEO Richard Smith apologizes; doesn't say why a fix wasn't carried out

Apple apologises for listening to Siri conversations

Zoom CEO: 'I Really Messed Up' on Security

Zoom CEO 'deeply sorry' for privacy and security issues

Instagram apologizes to users: We won't sell your photos

Facebook CEO apologizes for data privacy scandal

Zoom CEO apologizes for having 'fallen short' on privacy and security

Zoom CEO apologises for privacy, security concerns marring video meetings

Microsoft apologizes for, but doesn't really fix, software validation snafu

Former Equifax CEO Apologizes For Data Breach, Details Remediation Efforts

Spotify's chief executive apologises after user backlash over new privacy policy

Sony CEO Apologizes for Data Breach

Google Apologizes for Buzz Privacy Issues

Zuckerberg apologizes, promises reform as senators grill him over Facebook's failings
Twitter apologises for business data breach

Any corporate communication service that distributes encryption keys on behalf of users carries with it the risk of surveillance and government monitoring and all the risks described earlier.

True end-to-end encrypted communication requires that the participants in conversations hold and exchange their own encryption keys. Only Signal provides this in a simple, free, easy to use application model.

Signal Was Designed for Privacy

Signal provides text, audio or video messaging fully end-to-end encrypted with sophisticated algorithms designed to protect user privacy. Its one-on-one video calling is only available with its mobile applications. Group video conferencing is not available but the company says it is working on it²⁰.

²⁰ [Messaging App Signal Is Working on Encrypted Group Video Calls \(PC Magazine\)](#)



Signal's threat model assumes that cellular and data networks are surveilled and insecure — which has been repeatedly proven. And, it assumes that no third parties can be trusted with our private information or encryption key services.

Signal servers do not issue encryption keys as a third party such as Zoom does. Instead, what's called a private key is created on users' devices in the Signal app and kept on the device. A separate public key also created on the device is shared with Signal's servers to facilitate secure conversations. The public key is useless without access to the private key. They work together. Even if the government seized Signal's servers, the public keys would not allow them to reveal our messages or conversations.

The Signal app was created by privacy activist Moxie Marlinspike²¹, evolving over the past decade into the current multi-platform app that we know today. Marlinspike has done a great service to privacy, Internet communications and human rights.

For example, Signal became the most downloaded messaging app in Hong Kong during the week of July 6th as its residents sought privacy from China's hostile takeover and security crackdown²². And, when the Hong Kong Free Press reported the Telegram messaging app would refuse data requests to Hong Kong Courts, Signal retweeted, "We'd announce that we're stopping too, but we never started turning over user data to HK police." and "Also, we don't have user data to turn over."²³

²¹ [Meet Moxie Marlinspike, the Anarchist Bringing Encryption to All of Us \(Wired\)](#)

²² [Signal Tops Hong Kong Downloads After Fears of China Law Deepen \(Bloomberg\)](#)

²³ [Signal Tweets "we don't have user data to turn over." \(Twitter\)](#)





The way participants find each other on Signal is by sharing their phone number. If you're text messaging, it's a good idea to verify that the person you want to talk to has control of their phone number when you get started. For example, you can confirm they received your message in person, on email or by a regular phone call or Signal audio or phone call.

According to technology writer Yael Grauer, Signal is only safe on Apple products and Nexus and Pixel phones. He says, most other Android-based phones "don't meet the security requirements of a teenager."²⁴ Nexus and Pixel phones receive regular operating system updates but other Android models do not update automatically but instead depend on manufacturers and carriers to issue updates²⁵.

Signal is Open Source

By publicly sharing the source code for Signal's apps²⁶ on each of its platforms and devices, it increases trust in the organization, allowing security experts and researchers to regularly study and review its encryption methods and its application code.

Because Signal is open source, we can trust Signal more than other proprietary services that its applications are indeed protecting the privacy of our messages and calls.

²⁴ [WikiLeaks says the CIA can "bypass" Signal. What does that mean? \(Slate\)](#)

²⁵ [Check & update your Android version - Android Help \(Google\)](#)

²⁶ [Signal Source Code on GitHub](#)



If you're interested, the International Association for Cryptologic Research offers [A Formal Security Analysis of the Signal Messaging Protocol](#).

As a counterexample, Zoom is not open source — so it's much more difficult to verify how the company protects our calls and access to our cameras and microphones. And, it's much more difficult to verify Zoom's new claims of encryption and routing control.

With Signal, in most circumstances, no one can watch or listen to your video calls, not Signal, not the government or police and not IT staff. But let's threat model the vulnerabilities:

- **Device attack.** It's possible that a government actor or sophisticated hacker compromises a mobile device such that they have access to the microphone and camera on the device. Signal cannot protect you from this, no service can.
- **Government decryption.** The full extent of the NSA's capabilities are not known and the possibility exists that the NSA has the ability to capture the encrypted data from your video call and decrypt it over time .
- **Betrayal.** The person you are communicating with could betray your confidence and use a secondary device to record the audio or video — or share the content of your text messages with a third party. In some cases, your conversation partner might be adhering to the law, providing access to your conversation under subpoena.
 - Signal cannot protect against screenshots of text messages or video images.
 - In default mode, Signal does share your IP address with the participant's application. They could be monitoring their network traffic and disclose your IP address, possibly revealing your whereabouts. There is a Signal setting to protect against this, called "Always Relay Calls" but it reduces the quality of audio and video calls. A VPN might assist with this but might also lower the quality.
- **SIM swap attack**²⁷. Someone you text message with on Signal could possibly be the victim of a SIM attack where another party is able to convince their cellular provider that they are the owner of that phone number. In these cases, your ongoing text or audio conversations could be compromised until you hear from your friend that they've lost access to their phone. With a video call, you can at least see the person you are speaking to. Signal's implementation of Personal Identification Numbers potentially mitigates this risk²⁸.

²⁷ [SIM swap scam \(Wikipedia\)](#)

²⁸ [Signal >> Blog >> Introducing Signal PINs](#)



- **Signal is forced by the government to provide a backdoor, such as the PRISM program.** Theoretically, the government could force Signal to modify its algorithm for surveillance. Hopefully this would become obvious in its open source code and public audits. Signal has also indicated they would stop operating in the US under circumstances where US laws could cause user privacy to be compromised²⁹.

While it is difficult to protect conversations from all of these scenarios, for most of us, Signal provides outstanding protection that is the best that we can get. Some countries outlaw encryption, so please understand your local laws.³⁰

Telehealth is Not Fully Private

Our medical health deserves the utmost in privacy especially when reflecting on diagnosis of a serious disease or the privacy of conversations with a mental therapist or counselor.

While “telehealth” is a generic term for phone-based or internet-based health conversations, the term often refers to “Zoom for Healthcare.”

It’s often said that telehealth is HIPAA Compliant — an overused and abused phrase. The HIPAA telehealth requirements were written in a way to meet service providers where they are.

The HIPAA requirements do not require or enforce end-to-end encryption and we should meet provider claims with skepticism.

If you have medical conversations on Zoom’s telehealth service, consider threat modeling that your medical conversations are vulnerable to all the threats listed at the beginning of this article.

Zoom claims its 256-bit encryption makes it “HIPAA Compliant”³¹ despite Citizen Lab’s findings that it used 128-bit encryption, an unfavored algorithm and still lacks end-to-end encryption.

²⁹ [Signal >> Blog >> 230, or not 230? That is the EARN IT question](#)


³⁰ [signalapp/Signal-iOS: A private messenger for iOS \(Github\)](#)

³¹ [HIPAA Compliance Guide \(Zoom\)](#)



HIPAA Standard	How Zoom Supports the Standard
<p>Access Control:</p> <ul style="list-style-type: none"> Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to authorized persons or software programs. Unique User Identification: Assign a unique name and/or number for identifying and 	<ul style="list-style-type: none"> Meeting data transmitted across the network is protected using a unique Advanced Encryption Standard (AES) with a 256-bit key generated and securely distributed to all participants at the start of each session. Multi-layered access control for owner, admin, and members.

And, here's Zoom describing administrative access³² providing the above “multi-layered access control for owner [and] admin”:


[Help Center](#)
[SALES](#)
[PLANS](#)
[JOIN A MEETING](#)

[Zoom Help Center](#) > [Audio, Video, Sharing](#) > [Recording](#)

[Getting Started](#)
[Audio, Video, Sharing](#)
[Meetings & Webinars](#)
[Zoom Phone](#)
[Account & Admin](#)
[Zoom Rooms](#)
[H.323/SIP](#)
[Messaging](#)
[Integration](#)
[On-Premise](#)

Managing cloud recordings

Overview

Recording management allows account owners and admins to manage their users' cloud recordings, including view, delete, and share the video, audio, transcript, and chat files.

“Recording management allows account owners and admins to manage their users' cloud recordings, including view, delete, and share the video, audio, transcript, and chat files.”

It's reasonable for your threat model to consider a voyeuristic or corrupt IT manager.

Unfortunately, end-to-end encryption is not a requirement for telehealth video to earn the “HIPAA Compliant” label. This shortcoming may be an example of Congress' lack of technical expertise and/or the power of the health care lobby.

³² [Managing cloud recordings \(Zoom\)](#)



Zoom for Health is not a fully secure offering. For one-to-one conversations, Signal app is a better alternative.

One drawback to Signal is that it currently requires medical professionals to share their phone number with patients and clients. While Signal is hoping to solve this problem in the future³³, there is a solution. Cell carriers often offer inexpensive secondary numbers which ring the same device.

verizon✓

Multiple phone numbers. One phone.

Your phone is how you handle pretty much everything in your life. And with Verizon My Numbers, you can get multiple phone numbers to keep it all organized for \$15/mo per phone number. Add up to four phone

Verizon offers a second number for \$15 per month and T-Mobile DIGITS offers one for \$10/month.

For example, a mental health professional could make their Signal calls with their secondary number, protecting their primary cell number. They could also terminate the second number if they ever leave the organization or facility.

Alternately, health care clinics could provide cell phones for providers to use for their Signal-based healthcare calls as long as they physically secure them from tampering.

³³ [Technology Preview for secure value recovery \(Signal Blog\)](#)



Beware of Security Propaganda in Corporate Statements and Journalism

As we've seen with Zoom, corporations routinely mislead and overstate the security they provide customers. And, unfortunately, journalists frequently repeat corporate lies without taking the time to assess the details in the technology.

In April, USA Today reported, "By the end of May, Zoom plans for its entire platform to use tougher encryption, AES 256-bit GCM encryption, which Zoom says 'offers increased protection of your meeting data in transit and resistance against tampering.'" But again it's not end-to-end encryption so your conversations will remain vulnerable to most of the threats described earlier.

Here's a June 17, 2020 story from The Verge entitled, "[Zoom says free users will get end-to-end encryption after all](#)." The story repeatedly quotes Zoom's blogpost without skepticism or commentary from an outside expert: "We plan to provide end-to-end encryption to users for whom we can verify identity..." and "Free/Basic users seeking access to E2EE will participate in a one-time process..." Again, Zoom's planned upgrades do not appear to offer a timeline for actual end-to-end encryption.

When it comes to security, don't trust what you read without verification. You will rarely find factually accurate statements at corporations' product pages. And remember, "HIPAA Compliant" is no guarantee of actual privacy.

Even good organizations like the University of Washington medical system rely on Zoom's claims of HIPAA compliance and vague terms such as encrypted and protected:

⇒ You will use a program/app called Zoom to connect for your appointment.

What is Zoom? Zoom is a health information (HIPAA) compliant video conferencing system that allows you to have a video visit with your UW medicine care provider.

UW Medicine uses a HIPAA-compliant Zoom platform for telemedicine visits. All information and data related to your visit is encrypted and protected. We have legal agreements in place with Zoom to ensure that all federal privacy laws around protected health information are followed.

Screenshot from UW Medicine telehealth Information

"UW Medicine uses a HIPAA-compliant Zoom platform for telemedicine visits. All information and data related to your visit is encrypted and protected."³⁴

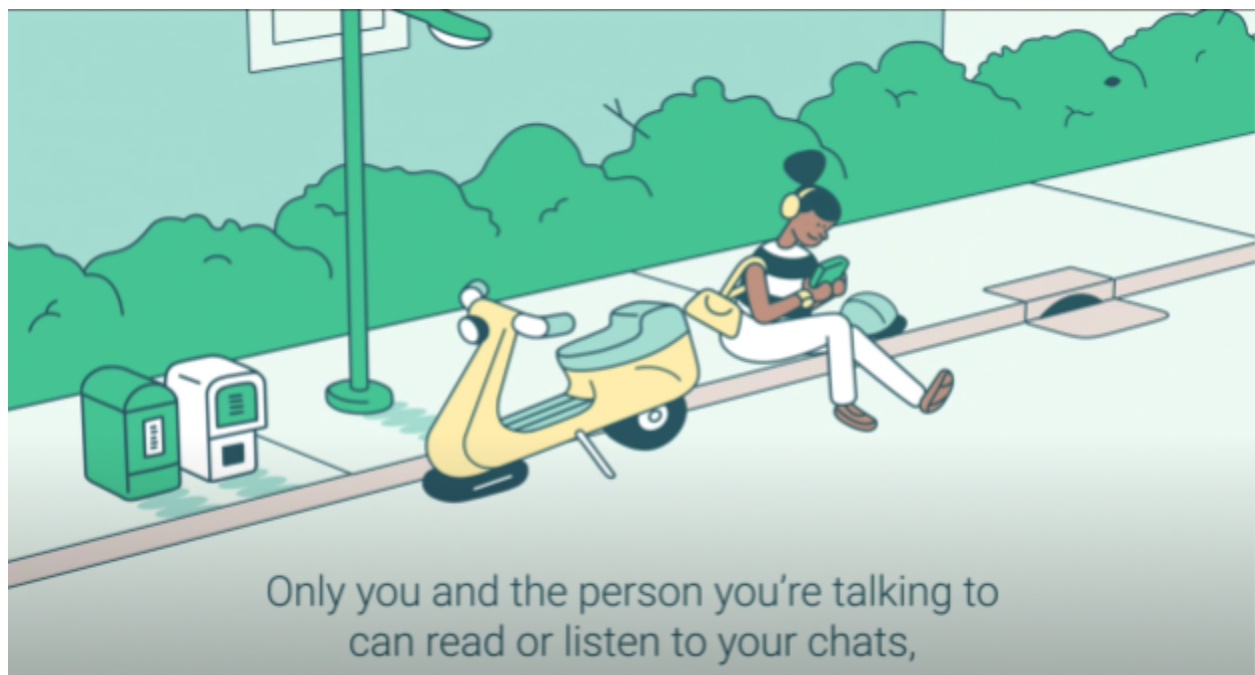
³⁴ [Job Aid Zoom Patient Instructions \(UW Medicine\)](#)



Take the time to investigate claims and look for reporting that consults security experts. Wired has done a good job in their reporting, frequently including commentary from cryptographer Mathew Green³⁵. And, Citizen Lab's dissection of Zoom's service is an excellent example of good technology journalism. You can also [follow Green on Twitter](#).

In my research for this document, I was repeatedly stymied by misleading and vague claims not backed up by detailed technical descriptions.

This [Facebook WhatsApp video](#) cheerily claims that What'sApp offers end-to-end encryption. And, it does so by integrating portions of Signal's technology.



It's a great example of content that doesn't tell the whole story and avoids technical description. But, Facebook is intent on monetizing WhatsApp which may require working around Signal's encryption model to find other ways to target advertising at users.

Both WhatsApp founders, Jan Koum and Brian Acton, left Facebook as a result of their concerns.

“According to the Washington Post, which spoke to ‘people familiar with internal discussions’ over Koum’s departure, there were tensions with Facebook over

³⁵ [Encrypted Messaging Apps Have Limitations You Should Know \(Wired\)](#)



WhatsApp's end-to-end encryption, which ensures that messages can't be intercepted and read by anyone outside of the conversation, including by WhatsApp or Facebook - [WhatsApp CEO Jan Koum quits over privacy disagreements with Facebook \(The Guardian\)](#)

"Acton told Forbes that Mark Zuckerberg and other Facebook executives wanted to begin targeting ads at users and selling business analytics tools, two plans that Acton didn't agree with. 'At the end of the day, I sold my company,' Acton told Forbes. 'I sold my users' privacy to a larger benefit. I made a choice and a compromise. I live with that every day.'" [WhatsApp co-founder explains why he left Facebook \(CNBC\)](#)

Acton later donated \$50 million to Signal app to support its ongoing development³⁶.

Freelance writer K.G Orphanides says³⁷, "Perhaps the most compelling reason to use Signal [vs What'sApp] is Facebook's long-standing lack of respect for its users' privacy. Facebook has an appalling history when it comes to data collection and handling, from the Cambridge Analytica affair to its practice of sharing data about users with phone manufacturers. It's already proved that it can't be trusted with WhatsApp user data that should, under EU law, have remained private."

Even the NSA's current recommendations for government workers³⁸ conflate "partial end-to-end encryption" with the real thing. Below is a heavily reduced view of the NSA's chart to show Signal and Zoom together. Zoom is listed as Yes, having E2E Encryption but with just a footnote saying partial — as if these two models remotely offer the same privacy.

³⁶ [WhatsApp Co-Founder Brian Acton Injects \\$50 Million in Newly Formed Signal Foundation \(Wired\)](#)

³⁷ [Why everyone should be using Signal instead of WhatsApp \(Wired\)](#)

³⁸ [National Security Agency - Cybersecurity Information Selecting and Safely Using Collaboration Services for Telework - UPDATE](#)



Service	Basic Functionality	1 – E2E Encryption	2 – Testable Encryption	3 – MFA	4 – Invitation Controls	5 – Minimal 3 rd Party Sharing	6 – Secure Deletion	7 – Public Source Code Shared	8 – Certified Service (FedRAMP / NIAP)
Signal ^{®viii}	a, b, d	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Zoom ^{®xiii}	a, b, c, d, e	Y ^{1, 4}	Y	Y ¹	Y	Y	Client – Y Server – N ³	N	FedRAMP

Table of Assessments against Criteria

Legend: Y = Yes, N = No; (a) text chat, (b) voice conferencing, (c) video conferencing, (d) file sharing, (e) screen sharing.

¹ Configurable

² Free Version - N

³ No Published Details

⁴ Partial

Don't ever assume the NSA is concerned about helping you protect your privacy. The NSA's tacit approval of Zoom here leaves millions of Americans further to open to legal and illegal surveillance.

Jitsi, Wire and Other Services

Since Signal provides end-to-end encryption only for one-to-one video calls, let's look at alternatives to Zoom for group video conferencing.

Jitsi

Jitsi is an open source video conferencing service now owned by [8x8](#), a for profit corporation, which plans to use the Jitsi technology in its products (8x8 acquired it from Atlassian).

Jitsi's video conferencing is not as polished as Zoom but it's relatively easy to use and may meet some people's needs, especially for group conferencing. Currently, Jitsi claims it supports up to 75 participants but they are working to expand this to 100³⁹. It also claims the quality of its video calls is highest with 35 or fewer participants⁴⁰. It's best to verify these claims for yourself or look for an independent expert to verify them before relying on them for an important event.

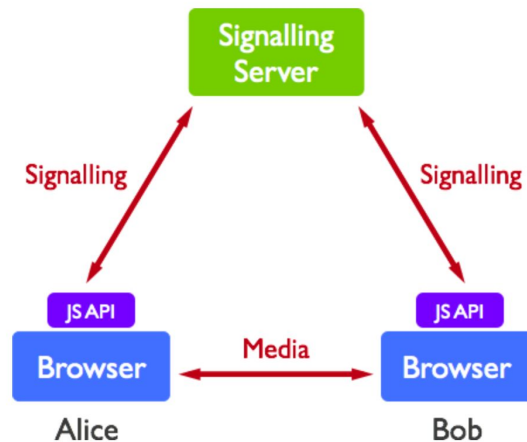
Jitsi meetings today rely on the WebRTC standard for secure browser-based video transmission. While not as secure as Signal's end-to-end encryption, it may be the next best technology available to us with caveats highlighted further below.

³⁹ [Maximum number of participants on a meeting on meet.jit.si server \(Jitsi.org\)](#)

⁴⁰ [Jitsi Employee Provides Information on the Maximum Number of Participants \(Jitsi.org\)](#)



Encrypted video in one-to-one video calls is delivered directly from browser to browser (person to person or P2P) as this graphic from [A Study of WebRTC Security](#) shows:



While some information about the two callers may be sent over the Internet, the peer to peer encrypted video is probably more secure than encryption based on delivery of a key by a third party server, such as Zoom's.

“Signalling requires the initial use of an intermediary server for the exchange of metadata, but upon completion WebRTC attempts to establish a direct P2P connection between the users.”

For group video calls, Jitsi requires encrypted video data to be routed through a server called a video bridge. The presence of this additional server creates the possibility for the kinds of third party security vulnerabilities we described about Zoom.

At least Jitsi, like Signal, is open source, so security experts can see how it operates and system administrators can choose to install and operate their own Jitsi server, avoiding the threat of exposure from Jitsi servers which you have no control over.

“...people who feel they cannot trust existing service providers not to eavesdrop on their meetings, can run their own bridges [or servers]. We spend considerable effort to make sure this is very easy to do, but ... it will never be as simple or as hassle-free as a single click on a link.” - [This is what end-to-end encryption should look like! \(Jitsi\)](#)



Jitsi is currently developing its [partial end-to-end encryption solution](#) which you can use experimentally on the current product. However, it also appears to be incorrectly calling it “end-to-end encryption” as a video bridge is required in the middle for group calls.

Threat Modeling for Jitsi

Our threat model should consider that corporate web browsers such as Chrome and Safari may have government backdoors built into them for WebRTC, possibly as part of the aforementioned NSA PRISM program.

While Google’s Chromium codebase for the Chrome browser is open source, the actual Chrome download includes proprietary code which is not inspectable. Such code could include a government-enforced back door, but Google denies it⁴¹. Note that participants in government top secret government operations may be forbidden legally from disclosing their involvement or what they know.

Using Jitsi with open source browser Firefox or Jitsi’s open source mobile apps’ implementation of WebRTC may be more secure than using Jitsi in a browser such as Chrome or Safari.

We also need to threat model that government spy agencies who successfully penetrate WebRTC will not disclose these weaknesses to browser makers — and that these vulnerabilities remain open.

If privacy is not required, I’d choose Jitsi over Zoom because it’s a free, open source and there are technical steps available to reduce exposure, whereas Zoom has troublesome known vulnerabilities.

If you need a high degree of privacy, there is no accessible end-to-end encrypted video conferencing solution for a large number of people. However, one company provides a solution for up to four people.

Wire

[Wire](#) is an open source, independently audited, end-to-end encryption messaging, phone call and video conferencing platform. It supports four participants for video conferencing and ten participants for phone conferences. And, with a Wire account, you can start video calls with people without requiring them to set up an account.

⁴¹ [NSA Prism program taps in to user data of Apple, Google and others \(Guardian\)](#)



While Wire is primarily oriented towards business users, it's affordable at \$6 and \$10 per month depending on your plan, as of this writing.

Wire may be preferable for some users who wish to have the option of using their desktop computer for video calls, Signal currently is limited to mobile devices.

Wire checks many of the key boxes for secure conversations:

- Open source⁴²
- Independently audited⁴³
- End-to-end encrypted
- Uses recommended encryption practices such as the Double Ratchet Algorithm⁴⁴

Wire's security page provides a transparent and technical overview and links to a whitepaper on their security implementation⁴⁵:

Technical overview

Text messages and pictures use the [Proteus protocol](#) for end-to-end encryption. Proteus is based on the Axolotl ratchet and pre-keys that are optimized for mobile and multi-device messaging.

Voice and video calls use the WebRTC standard. More precisely, DTLS and KASE are used for key negotiation and authentication and SRTP is used for encrypted media transport. This means that voice calls are end-to-end encrypted with perfect forward secrecy enabled without compromising HD call quality.

Wire's encryption works transparently in the background and doesn't need to be activated — it's always on. There's no need to compromise security for usability or settle for missing features. Wire keeps everything private while avoiding the complexity that is common to other secure messengers.

However, Wire is not yet HIPAA compliant and neither is Signal. It's ironic that these two options provide two of the most secure video solutions available but are not yet certified, while less secure options such as Zoom are certified.

⁴² [Wire's Github Page to Inspect Source Code \(Github\)](#)

⁴³ [Wire's Audits Page](#)

⁴⁴ [Double Ratchet Algorithm \(Wikipedia\)](#)

⁴⁵ [Wire Conferencing Security Page](#)



Wire is a compelling option for those needing up to four person conference solutions and desktop video.

In my own brief experience with Wire, I found the application interface to be a bit confusing and unintuitive but it appears to be easily learnable.

FaceTime

FaceTime is an option for group video calls as long as everyone on the call has an Apple device. And, in 2013, Apple published its “Commitment to Customer Privacy”⁴⁶:

“There are certain categories of information which we do not provide to law enforcement or any other group because we choose not to retain it. For example, conversations which take place over iMessage and FaceTime are protected by end-to-end encryption so no one but the sender and receiver can see or read them. Apple cannot decrypt that data.”

Apple seems to adhere to this claim in denying requests from the federal government⁴⁷. But TechDirt’s Mike Masnick disagrees:

“While Apple boasts of ‘end-to-end encryption’ it’s pretty clear that Apple itself holds the key -- because if you boot up a brand new iOS device, you automatically get access to your old messages. That means that (a) Apple is storing those messages in the cloud and (b) it can decrypt them if it needs to. As Julian Sanchez discusses in trying to get to the bottom of this, the memo really only suggests that law enforcement can’t get those messages by going to the mobile operators. It says nothing about the ability to get those same messages by going to Apple directly.”

Again, our threat model should forecast for Apple’s broken promise and future apology.

All the Others

WhatsApp may still have true end-to-end encryption but why should you trust Facebook? It’s unclear for how long Facebook will continue to honor the historical privacy of WhatsApp users.

Microsoft Teams and Google Meet also use partial end-to-end encryption similar to Zoom.

⁴⁶ [Apple's Commitment to Customer Privacy](#)

⁴⁷ [Apple and Other Tech Companies Tangle With U.S. Over Data Access \(New York Times\)](#)



In Closing

Use Signal as much as you can for one-on-one conversations. And, consider Wire for up to four person video calls and ten person phone calls.

We recommend avoiding Zoom for conversations that require privacy, including for telehealth. That said, another expert we spoke to recommended that if it comes down to the question of not receiving necessary medical care or receiving care, you should use Zoom rather than foregoing such care.

Be cautious with FaceTime. And, why trust Facebook with What'sApp?

Lastly, keep an eye on Jitsi for the future.

Groups that require higher levels of privacy should meet in person, pandemics and geographic location notwithstanding. For group conversations that don't require privacy, consider using the corporate service provider you least distrust.

Acknowledgements

Thank you to author and digital rights advocate [Cory Doctorow](#) for his detailed review and suggestions. And, to Gunner here at Aspiration for his encouragement, ideas and valuable corrections.

Related Links

Here are some resources that I used to compose this article:

Understanding Zoom

- [Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings \(Citizen Lab\)](#)
- [So Wait, How Encrypted Are Zoom Meetings Really? \(Wired\)](#)
- [Zoom's Flawed Encryption Linked to China \(The Intercept\)](#)
- [End-to-End Encryption Update \(Zoom\)](#)
- [CEO Report: 90 Days Done, What's Next for Zoom \(Zoom\)](#)
- [It's Here! 5 Things to Know About Zoom 5.0 \(Zoom\)](#)
- [Data Routing Control is Here \(Zoom\)](#)



Signal

- [Signal](#)
- [Signal, the secure messaging app: A guide for beginners \(Freedom of the Press Foundation\)](#)
- [Why everyone should be using Signal instead of WhatsApp \(Wired UK\)](#)
- [Demystifying the Signal Protocol for End-to-End Encryption \(E2EE\) \(Medium\)](#)
- [Meet Moxie Marlinspike, the Anarchist Bringing Encryption to All of Us \(Wired\)](#)

Encryption and Threat Modeling

- [AES Video Encryption: 256 vs 128 Bit \(IBM Watson Media\)](#)
- [What is 256-bit Encryption? How long would it take to crack? \(Patrick Nohe, The SSL Store\)](#)
- [Creating Your Own Personal Threat Model \(Security Innovation\)](#)

Jitsi

- [Jitsi.org - develop and deploy full-featured video conferencing](#)
- [Jitsi Videobridge](#)
- [This is what end-to-end encryption should look like!](#) Note: I am concerned about the technical accuracy of the claims.

Apple

- [Apple's Commitment to Customer Privacy \(Apple\)](#)
- [Apple's hired contractors are listening to your recorded Siri conversations, too \(The Verge\)](#)

WhatsApp and Facebook

- [WhatsApp co-founder explains why he left Facebook \(CNBC\)](#)

Transparency Reports

- [Signal](#)
- [Google](#)
- [Apple](#)
- [Facebook](#)

