We read the privacy policies of Skype, Meet, and Webex: 10 ways videoconferencing systems can better protect privacy for customers

medium.com/cr-digital-lab/skype-meet-webex-videoconference-privacy-845bc8360fd3

April 30, 2020

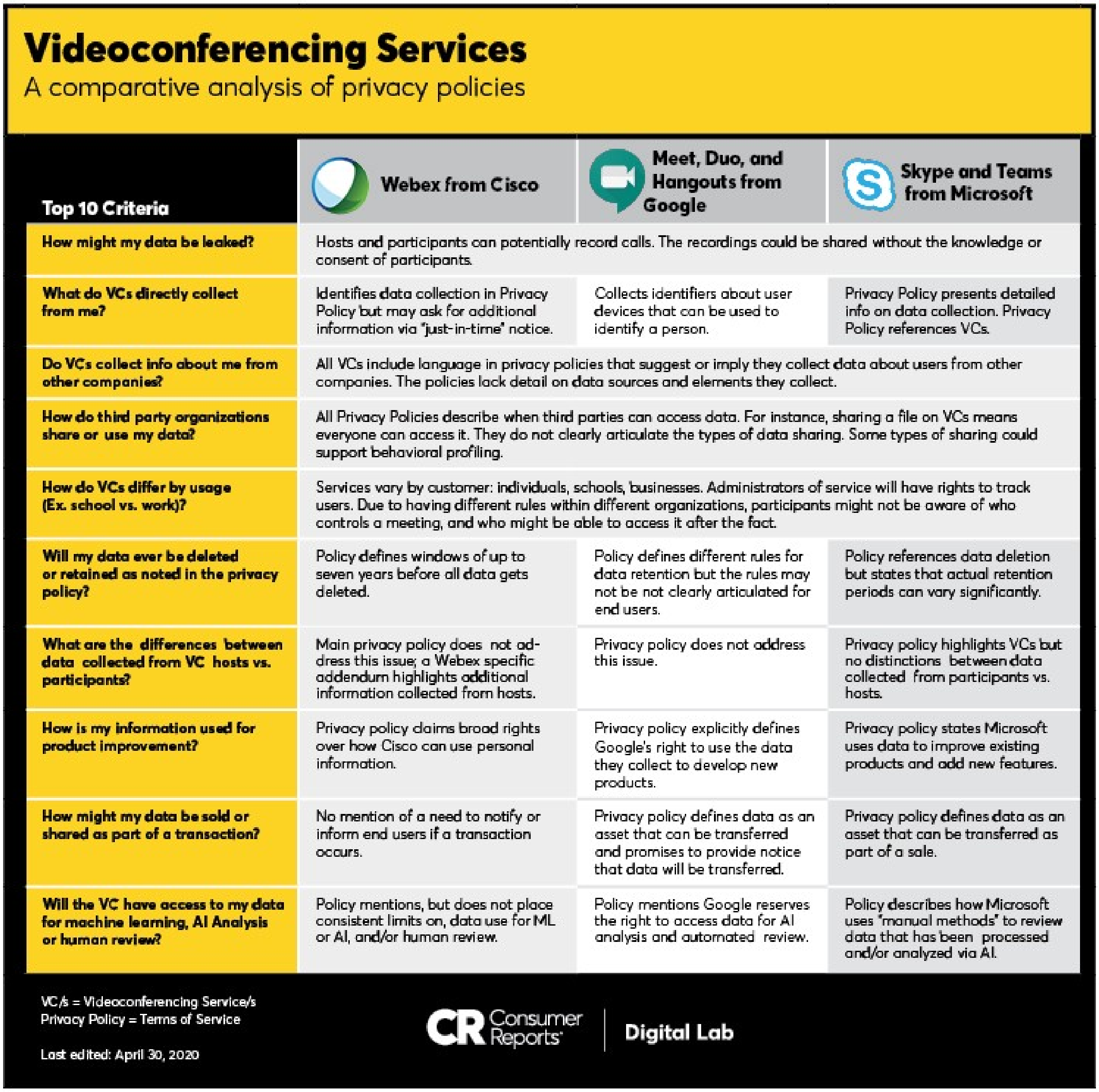
The rise of videoconferencing services

As of mid-April 2020, 95% of the American population are under orders to stay home. This new reality has triggered a spike in users accessing videoconferencing services. Zoom has received a significant amount of attention, but other major platforms — Webex, Google Meet, and Skype — require similar scrutiny.

Consumers are caught in a difficult place. For millions of people, a videoconferencing service is the lifeline they need to stay employed, to access medical care, to keep in touch with family and friends. For many students — from pre-K through graduate school — videoconferencing is a central part of their education and connecting with classmates and teachers. There are also low-tech methods aimed to meet needs of all learners during distance-learning. If a person does not want to use a videoconferencing service out of privacy and security concerns, they may not be able to access classes, show up for a job, gain access to medical care or maintain contact with friends and family.

On the surface, it's hard for consumers to determine which videoconferencing service best aligns with their privacy expectations. These videoconferencing services have opaque privacy policies. As more people use videoconferencing, these companies are collecting more information about their users. Our images, the sound of our voices, who we speak with, what we talk about, when we interact all have the potential to provide these companies with information that could be folded into behavioral profiles, marketing, and/or facial recognition or voice printing services.

Consumers should be able to trust that companies will provide clear, simple language that shows how they respect and protect user privacy and security. There is an opportunity in the market for videoconferencing services to distinguish themselves as a leader in respecting user privacy as a core foundation of their business.



Videoconferencing Services

A comparative analysis of privacy policies

Top 10 Criteria	Webex from Cisco	Meet, Duo, and Hangouts from Google	Skype and Teams from Microsoft
How might my data be leaked?	Hosts and participants can potentially record calls. The recordings could be shared without the knowledge or consent of participants.		
What do VCs directly collect from me?	Identifies data collection in Privacy Policy but may ask for additional information via "just-in-time" notice.	Collects identifiers about user devices that can be used to identify a person.	Privacy Policy presents detailed info on data collection. Privacy Policy references VCs.
Do VCs collect info about me from other companies?	All VCs include language in privacy policies that suggest or imply they collect data about users from other companies. The policies lack detail on data sources and elements they collect.		
How do third party organizations share or use my data?	All Privacy Policies describe when third parties can access data. For instance, sharing a file on VCs means everyone can access it. They do not clearly articulate the types of data sharing. Some types of sharing could support behavioral profiling.		
How do VCs differ by usage (Ex. school vs. work)?	Services vary by customer: individuals, schools, businesses. Administrators of service will have rights to track users. Due to having different rules within different organizations, participants might not be aware of who controls a meeting, and who might be able to access it after the fact.		
Will my data ever be deleted or retained as noted in the privacy policy?	Policy defines windows of up to seven years before all data gets deleted.	Policy defines different rules for data retention but the rules may not be not clearly articulated for end users.	Policy references data deletion but states that actual retention periods can vary significantly.
What are the differences between data collected from VC hosts vs. participants?	Main privacy policy does not address this issue; a Webex specific addendum highlights additional information collected from hosts.	Privacy policy does not address this issue.	Privacy policy highlights VCs but no distinctions between data collected from participants vs. hosts.
How is my information used for product improvement?	Privacy policy claims broad rights over how Cisco can use personal information.	Privacy policy explicitly defines Google's right to use the data they collect to develop new products.	Privacy policy states Microsoft uses data to improve existing products and add new features.
How might my data be sold or shared as part of a transaction?	No mention of a need to notify or inform end users if a transaction occurs.	Privacy policy defines data as an asset that can be transferred and promises to provide notice that data will be transferred.	Privacy policy defines data as an asset that can be transferred as part of a sale.
Will the VC have access to my data for machine learning, AI Analysis or human review?	Policy mentions, but does not place consistent limits on, data use for ML or AI, and/or human review.	Policy mentions Google reserves the right to access data for AI analysis and automated review.	Policy describes how Microsoft uses "manual methods" to review data that has been processed and/or analyzed via AI.

VC/s = Videoconferencing Service/s
Privacy Policy = Terms of Service

Last edited: April 30, 2020

CR Consumer Reports | Digital Lab

Summary results comparing the privacy policies of Webex, Meet, and Skype

3 Videoconferencing Services: A Comparative Analysis of Privacy Policies

We examined the privacy policies for three popular videoconference tools: Webex from Cisco, Skype from Microsoft, and Meet from Google. The analysis is designed to identify potential risks and highlight areas where a lack of clarity creates doubt about how a company protects the privacy of the people who use services and products from a company. This analysis does not imply every company is exploiting every possible loophole. We focus on a comparative analysis with privacy policies as they create publicly defined commitments about what a company values. Consumers should take these policies literally. If something is true in the privacy policy, it should be true in the product, the user experience and the technical architecture behind the service. There are areas where the actual intentions of a company and their current daily practices are not accurately captured in their privacy policies.

By sharing this work, we aim to support consumers making informed choices about their privacy. We also want to see the companies providing these services articulate strong commitments to protect the privacy of people who use and rely on these services — which is why we are sending a letter to the companies highlighted in this report to give them the opportunity to make these needed improvements. It should be noted that these recommendations are broadly applicable to any platform that offers videoconferencing features. Video conferencing services are a critical part of how people are weathering the physical distancing required at this time, and people shouldn't have to make a choice between social connections, or work, or their privacy. Consumers deserve to access these services without sacrificing the privacy or security of their data and conversations.

Methodology: Honing in on 10 privacy policy criteria

The privacy policy comparative analysis — the name of the process used to create this report — is focused on several elements informed by the Digital Standard, a set of benchmarks that can be used by companies and organizations to design digital products that are respectful of consumer privacy rights. It distills key principles into 10 criteria for analysis. This is more narrowly focused than our standard product rating process which incorporates over 100 questions derived directly from the Digital Standard. This streamlined analysis results in valuable insights without the more comprehensive evaluation that would be needed for comparative ratings.

The privacy policy comparative analysis for individual products consists of three sections:

- A high level summary of key findings across all 3 platforms
- 3 summaries focused on each videoconferencing platform that maps to the of the rubric
- Policy notes consisting of excerpts from the privacy policy with commentary on what the language means

We invite you to review our comparative analysis of the privacy policies for Skype, Meet, and Webex. Based on this examination of the privacy policies and additional research into some related features, we have also recommended areas where all videoconferencing services can better support and protect consumers. Some are fairly simple clarifications; others would require additional work and thought. The areas of improvement are changes that would immediately benefit consumers.

Recommendations for Consumers and Service Providers

The criteria used for these areas for improvement are defined in this document. This section contains recommendations for consumers and for companies. For specific details on the services and a breakdown of these privacy policies, please visit the accompanying overview of Skype, Meet, and Webex.

1. Personal Data Leak

When using **Cisco WebEx**, **Google Meet**, and **Microsoft Skype** — and most other videoconferencing services — hosts can record calls and potentially share those recordings, and other participants can make surreptitious recordings of calls without the knowledge or consent of participants. This creates the potential for personal data leaks.

: Video calls should be thought of like emails, or any other post online: copies can be made and shared. When participating in any videoconference, if you are not aware whether or not a call is being recorded, ask the host to clarify. If it is not possible to ask the host (for example, if there is an uncomfortable or problematic power dynamic between a participant and a host), assume that the call is being recorded, and adjust your level of participation in the call to whatever feels comfortable (for example, turn off your camera, call into the meeting, etc.).

: All services should include instructions for hosts that include best practices for storing any recordings securely and secure meetings, including how to protect against unauthorized meeting crashers. These instructions should include details that cover the hosts' obligations under any relevant privacy law.

2. First Party Data Collection

Cisco's Webex: Cisco identifies multiple data elements that can be collected, but Cisco's terms also note that they might include additional information about privacy practices within applications. While this "just in time" notice is good, it needs to be paired with equally clear notice in policies so people can make informed decisions before using a service.

Google Meet, Duo, and Hangouts: Google collects multiple identifiers about devices used when a person uses a Google service. Individually, these data elements could be used to identify a person even in the absence of a name, email address, or physical address. However, these data elements are often connected to a Google account that can include an email address, phone number, name, and profile photo.

Microsoft Skype and Teams: Microsoft's terms provide a detailed overview of data elements collected.

: When possible, avoid creating an account to access a one-time conference. During account creation, share as little information as possible. Consider creating a throwaway “videoconference only” email address, or making strategic “mistakes” in the accuracy of the information you provide.

: Companies should clearly define the data elements collected when a person uses their specific videoconference service in their privacy policies. Data collection should be strictly limited to only what is needed to deliver the service. This definition should include how data collected from participants differs from data collected from hosts.

3. Data Enhancement

All three services include language in their privacy policies that indicate that they collect additional data about users from third parties. The terms of all three services lack precision about the sources of the data, and the specific data elements collected.

: Unfortunately, unless a company makes a strong and clear commitment to not engage in data enhancement, the only “option” is to not use the service. Given that not using videoconferencing is not a realistic option for many people, this is a clear power imbalance in favor of companies. If you live in a state like California that offers limited rights under CCPA, consider using those rights to get more insight into the data the company collects and holds about you, and how the data are used.

: In their privacy policies, companies should commit to not appending user data from outside sources unless there is a clearly limited, narrowly defined reason why the additional data is essential for the service. If this narrow criterion is met, then companies should list all sources outside the videoconferencing service that provide data, list the specific data elements that are collected from these other sources, and commit to providing user review of and control over all data, including data collected from third parties.

4. Third Party Access

The terms of **all three services** describe when they allow third parties to access data. Some of these scenarios are normal and expected — for example, when a person shares a file as part of a videoconference, the other people on the conference can access the file. However, not all sharing is that clearly defined, and some of the reasons for sharing are vaguely defined, and some sharing could potentially support behavioral profiling.

: Unfortunately, unless a company makes a strong and clear commitment to curtail third party access, the only “option” is to not use the service or be very conservative with any information you share. Given that not using videoconferencing is not a realistic option for many people, this is a clear power imbalance in favor of companies. If you live in a state like California that offers limited rights under CCPA, consider exercising those rights to get more insight into the data the company collects and holds about you, and how the data are used.

: Companies should define if and how data collected as part of videoconferencing could be shared with third parties. Additionally, companies should clearly commit to only sharing data with third parties if it is essential to running the service. This includes incorporating clear guarantees that third parties are forbidden from using shared data for any profiling, targeting, or other behavior not directly connected to providing the videoconferencing service. People use a videoconferencing service because they want to talk to other people, not because they want to have their usage patterns tracked, and that core user expectation should be respected.

5. Implications of Employer or School Sponsorship of Service

All three services have different offerings directed toward individuals, schools, and businesses. Each of these offerings have features that differ slightly between versions. For versions of the service where a school or business provides access, the chain of control regarding who can access what, and who can ultimately control data access and data sharing, isn't always clear. From the perspective of a participant in a conference, it can be difficult to know who controls the meeting. When a school, business, or other organization is offering the service, the administrators of the service will generally have rights to track users of the service.

: If you are using a required service as part of your work, be aware that the systems administrators at your workplace could have permissions to see information about meetings you host. This is true for videoconferencing tools, as well as other productivity suites.

: When a videoconferencing service is offered by a school, business, or other organization, the name of the entity controlling the videoconference should be clearly and obviously visible to all conference participants. This notice would include contact information for an administrator of the service. Additionally, meeting hosts and/or system administrators should not be able to use surveillance-like features (such as attention tracking, accessing or downloading text messages between participants) without clear notice to participants before the conference, or as the tracking is enabled.

6. Data Deletion & Retention

Cisco's Webex: Cisco's primary terms do not define any clear data sunsets. Some Webex-specific documentation specifies retention periods of up to seven years.

Google Meet, Duo, and Hangouts: Google's terms describe multiple different rules for retaining data, but the rules are not especially clear, and would be difficult to follow for a person not versed in data collection and retention practices.

Microsoft Skype and Teams: Microsoft's terms contain a section dedicated to data retention, but this section does not contain many specific commitments to deleting the data they hold within a clearly defined time frame.

: If you are at a higher level of risk or want to minimize exposure, avoid creating an account with a service. If you can't avoid creating an account with a service, share as little information as possible. This can include using a throwaway email address, or making strategic "mistakes" in the accuracy of the information you provide.

: In their privacy policies, companies should specify clear retention periods paired with data minimization strategies for the data they collect from videoconferencing services, and any data that gets combined with data collected from videoconferencing services. In addition to clearly defined deletion periods, users should have the right and the ability to delete data that have been collected from them or maintained about them before the company-specified time window.

7. Differentiation between data collected from hosts versus participants

Cisco's Webex: Cisco's main terms do not mention words generally associated with videoconferencing (conference, audio, recording, meeting, group). Cisco has multiple Webex-specific documents that contain additional information, but they are not presented to users during signup.

Google Meet, Duo, and Hangouts: Google's terms mention videoconferencing, but do not provide significant detail about data elements specifically collected from videoconferences.

Microsoft Skype and Teams: Microsoft is the only service that highlights its videoconference service in its main privacy policy, but even Microsoft's terms do not make consistent distinctions between data collected from participants and data collected from hosts.

: When possible, join a videoconference without creating or logging into an account on the service. If you can't avoid creating an account with a service, share as little information as possible. This can include using a throwaway email address, or making strategic "mistakes" in the accuracy of the information you provide.

: Companies providing videoconferencing services should add clear, simple language to their privacy policies that distinguishes between data collected from hosts (who have chosen to have a business relationship with a service) and participants (who haven't made a comparable choice). The privacy policy should clearly define any data collected from participants that do not have an account on the service. This language should specify data deletion windows for any data and metadata collected from participants.

8. Information used for Product Improvement

Cisco's Webex: Cisco's terms claim broad rights over how it can use personal information.

Google Meet, Duo, and Hangouts: Google's terms explicitly define Google's right to use the data they collect to develop new products.

Microsoft Skype and Teams: Microsoft's terms clearly state that they use data to improve existing products, including adding new features.

The combination of a large amount of accurate, sensitive information, paired with the ability to use that information to develop just about any new product, creates a significant privacy risk. Some secondary uses of customer information may be beneficial, such as bug tracking or narrowly defined user analytics. But often, companies fail to place meaningful limits on using consumer information to develop new products. In practice, this means that even if companies are well-intentioned today, data that is retained may be used in the future in ways that users wouldn't expect or agree with.

: Unfortunately, unless a company makes a strong and clear commitment to not use consumer data for product development or improvement, the only "option" is to not use the service. Given that not using videoconferencing is not a realistic option for many people, people concerned about minimizing exposure should make sure that cameras are only on when needed, backgrounds are obscured, and microphones muted except when speaking offer a level of protection.

: People using a videoconferencing service should only have their information used to develop new products or develop new features if the feature is clearly related to the service they are signed up for such as bug fixes, better video quality, or other directly related improvements. Secondary uses of data that are not directly related to the videoconferencing service should only happen with the clear and informed consent of the user.

9. Data That Can be Sold or Shared as Part of a Transaction

Cisco's Webex: Cisco's language does not mention any need to notify or inform end users if a transfer occurs.

Google Meet, Duo, and Hangouts: Google's terms define data as an asset that can be transferred, and promises to provide notice that data will be transferred.

Microsoft Skype and Teams: Microsoft's terms define data as an asset that can be transferred as part of a sale.

All companies have general language that states that data collected from users is an asset, and that data can be included in transactions including a bankruptcy, merger, acquisition, or other types of sales.

: Cisco, Google, and Microsoft are all adequately large companies that the chances of any of them being acquired are relatively small. However, without clear commitments from companies that allow users to delete any information before it is transferred, people should be aware of the possibility that a bankruptcy, sale, merger, or acquisition could result in their data being transferred to or accessed by another company.

: Mergers, sales, bankruptcies, and acquisitions are all very different types of events, and language in privacy policies should make clear distinctions between how data are handled in each of these distinct events. In case of a bankruptcy, user data should be destroyed. In case of other types of mergers, acquisitions, or sales, explicit advance notice (two or more weeks) of a transfer with the ability to cancel an account prior to transfer would allow people a reasonable amount of time to remove their information. In the case of a merger where one set of user data would be merged into a larger data set (for example, if Google were to acquire Zoom) the company seeking to merge the data sets should commit to getting informed opt in consent from affected people. These commitments should be clearly defined in privacy policies.

10. Access to Data for Machine Learning, AI Analysis, or Human Review

Cisco's Webex: Cisco's main terms place no clear or obvious limits placed on using data for ML or AI, and/or human review. Some Webex-specific terms describe optional facial recognition that is opt-in.

Google Meet, Duo, and Hangouts: Google's terms contain general descriptions that reserve the right to access data for AI analysis and automated review.

Microsoft Skype and Teams: Microsoft's terms describe how "manual methods" are used to review data that have been processed and/or analyzed via AI.

Automated analysis of data has valid uses. For example, closed captions generated in real time from audio are generally created via automated analysis. However, other uses — such as facial recognition or voice printing — take advantage of biometric identifiers present in audio and video data, and these secondary uses pose significant privacy risks.

: Unfortunately, unless a company makes a strong and clear commitment to not use consumer data for automated analysis, the only option is to not use the service. Given that not using videoconferencing is not a realistic option for many people, making sure that cameras are only on when needed, backgrounds are obscured, and microphones muted except when speaking offer a level of protection.

: Companies should make a clear written commitment in their privacy policies that they will not use any data collected via videoconferencing for developing facial recognition, voice printing, or any other automated analysis that uses biometric identifiers. Uses that support accessibility such as automated captioning could be exempt from these prohibitions. If there is the possibility of any automated analysis paired with human review of that analysis, participants should be clearly informed of this possibility, and hosts should be required to opt in to this use of data collected from their meetings.

Improving Video Conferencing Service Privacy Policies

For many people, videoconferencing provides a lifeline that allows connections with family, employers, and friends. Videoconferencing is becoming essential infrastructure, and companies have an opportunity to distinguish themselves by making clear and unequivocal promises about how they handle users' sensitive data. We look forward to engaging with these companies and others to strengthen their privacy disclosures and raise the standard around data use and limitation. Our letter to these companies outline improvements they should make. The privacy policy comparative analysis of Webex from Cisco, Skype and Teams from Microsoft, and Meet, Duo, and Hangouts from Google are intended to provide support for consumers as we all navigate these issues together.