April 30, 2020

John T. Chambers, CEO
Cisco Systems, Inc.
Tasman Way
San Jose, CA 95134

Sundar Pichai, CEO
Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Satya Nadella, CEO
Microsoft Corp.
1 Microsoft Way
Redmond, WA 98052

Re: Based on its Review, Consumer Reports Urges Higher Standards for Videoconferencing Services

Dear John T. Chambers, Sundar Pichai, and Satya Nadella:

Today, Consumer Reports published the results of its evaluation of the privacy policies for your videoconferencing services.[1]

The reason for looking at these services is clear. As of this month, 95 percent of Americans are under stay-at-home orders.[2] Confined to their homes, many have turned to videoconferencing tools to perform essential tasks like accessing medical care, continuing work or schooling, and connecting with family and friends. According to a March report from the Pew Research Center, 25 percent of adults have turned to videoconferencing tools to continue work.[3] Videoconferencing apps have reported record download numbers globally.[4] However, examples of abuse of these platforms[5] and reports of excessive data collection or sharing,[6] in addition to security issues,[7] have made consumers concerned about which platform to trust with their private communications. In

[1] Allen St. John, *It's Not Just Zoom. Google Meet, Skype, and Webex Have Some Privacy Issues, Too*, CONSUMER REPORTS (Apr. 30, 2020), https://www.consumerreports.org/video-conferencing-services/videoconferencing-privacy-issues-google-microsoft-webex/.

[2] Sarah Mervosh, Denise Lu, & Vanessa Swales, *See Which States and Cities Have Told Residents to Stay Home*, N.Y. TIMES (Apr. 20, 2020), https://www.nytimes.com/interactive/2020/us/coronavirus-stay-at-home-order.html.

[3] Monica Anderson & Emily A. Vogels, *Americans Turn to Technology During COVID-19 Outbreak, Say an Outage Would be a Problem*, PEW RESEARCH CTR. (Mar. 31, 2020), https://www.pewresearch.org/fact-tank/2020/03/31/americans-turn-to-technology-during-covid-19-outbreak-say-an-outage-would-be-a-problem/.

[4] Lexi Sydow, *Video Conferencing Apps Surge from Coronavirus Impact*, APP ANNIE (Mar. 30, 2020), https://www.appannie.com/en/insights/market-data/video-conferencing-apps-surge-coronavirus/.

[5] Kristen Setera, *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic*, FED. BUREAU OF INVESTIGATION, BOSTON (Mar. 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; Allen St. John, *How to Prevent Zoombombing*, CONSUMER REPORTS (Apr. 15, 2020), https://www.consumerreports.org/video-conferencing-services/how-to-prevent-zoombombing/

[6] *See, e.g.*, Sean Lyngaas, *Zoom Hit with Class-Action for Sharing User Data with Facebook*, CYBERSCOOP (Mar. 31, 2020), https://www.cyberscoop.com/zoom-lawsuit-facebook-california-privacy-ccpa/.

[7] *See, e.g.*, Lorenzo Franceschi-Bicchierai, *What is the Most Secure Video Conferencing Software?*, MOTHERBOARD (Mar. 24, 2020), https://www.vice.com/en_us/article/m7qwgx/what-is-the-most-secure-video-conferencing-software.

addition to these issues, the privacy and terms of use policies are difficult to read and for consumers to understand.

In response to this growing dependence on videoconferencing services, Consumer Reports[8] reviewed the privacy policies for your videoconferencing platforms: Webex from Cisco, Skype and Teams from Microsoft, and Meet, Duo, and Hangouts from Google.

This evaluation was informed by our Digital Standard.[9] Based on this review,[10] we have the following recommendations (also available in the appendix) for your videoconferencing service and services like yours:

1. **Personal Data Leak.** All services should include instructions for hosts that include best practices for secure data storage and secure meeting setup, including how to protect against unauthorized meeting crashers. These instructions should include details that cover the hosts' obligations under any relevant privacy law.[11]
2. **First Party Data Collection.** 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.** 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,

[8] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For 83 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

[9] The Digital Standard (theDigitalStandard.org) was launched on March 6th, 2017 and is the result of a collaboration with our cybersecurity partners, Disconnect, Ranking Digital Rights, and the Cyber Independent Testing Lab. The Standard is designed to hold companies accountable and equip Consumer Reports and other organizations to test and rate products for how responsibly they handle our private data. This is a collaborative and open source effort. The Standard is designed to empower consumers to make informed choices about the connected products, apps, and services consumers use every day. *The Standard*, THE DIGITAL STANDARD, https://www.thedigitalstandard.org/the-standard.

[10] You can learn more about our review by going to our Medium post about this work: Bill Fitzgerald, *We read the privacy policies of Skype, Meet & Webex: 10 ways videoconferencing systems can better protect privacy for consumers*, DIGITAL LAB AT CONSUMER REPORTS (Apr. 30, 2020), https://medium.com/cr-digital-lab/skype-meet-webex-videoconference-privacy-845bc8360fd3.

[11] *State Laws Related to Internet Privacy*, NAT'L CONFERENCE OF STATE LEGISLATURES (Jan. 27, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

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.** 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.** 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 and Retention.** 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 from Participants.** 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 have not 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 Development.** 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.** 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.** 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.

We urge your companies, and other providers of videoconferencing platforms to adopt these changes and recommended adjustments. We at Consumer Reports are interested in knowing whether or not your company plans to make changes to your privacy policies or services based on these recommendations. In addition, we also welcome a conversation about what measures providers of videoconferencing services should be implementing in order to protect their users and the privacy and security of those users' personal information.

We would love to schedule a call to discuss our letter and your feedback. Please let us know what works best over the next two weeks.

Sincerely,

Katie McInnis
Policy Counsel

Consumer Reports
1101 17th Street NW, Suite 500
Washington, DC 20036

Appendix: Graphic of Consumer Reports' Recommendations to Videoconference Providers

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