September 30, 2020

Re: Cisco Systems, Inc. (Cisco WebEx) Response to Joint Statement on Global Privacy Expectations of Video Teleconferencing Companies

Dear Commissioners:

Thank you for the opportunity to respond to the joint statement on global privacy expectations of Video Teleconferencing Companies (VTC). We applaud your efforts to carefully examine the privacy and security implications of how these technologies are built, deployed, and used. The imperative to engage in social distancing during the COVID-19 pandemic has resulted in a dramatic uptick in the use of VTC technologies to enable distance and hybrid work, education, healthcare delivery and other critical functions to maintain the health and safety of the public and to enable economic activity. Cisco Webex securely supported 500 million meeting participants, generating 25 billion meeting minutes in April alone – more than triple the pre-pandemic volume. With increased reliance on VTC technology, security and privacy are more important than ever.

We understand the concerns you raise and have been focused on privacy and security by design and default for years. Our Chairman & CEO, Chuck Robbins, has publicly taken the position that "privacy is a fundamental human right" and Cisco is committed to respecting and protecting the privacy rights of our customers, partners, end users, workers, and others. Our Data Protection & Privacy Program is anchored on the principles of transparency, fairness, and accountability and has been certified to align to privacy frameworks and requirements from around the world (e.g., EU Binding Corporate Rules for Controllers (BCR for Processors application pending), EU/Swiss/UK-US Privacy Shield, APEC Cross Border Privacy Rules system and Privacy Recognition for Processors). Privacy is front and centre in the design, development, deployment, and maintenance of our networks, platforms, applications, and offers. For more information about Cisco's approach to privacy, please visit our online Trust Center here.

Cisco Webex

Cisco Webex is a video conferencing service delivered through the Cisco Webex Cloud, a highly secure service-delivery platform with industry-leading performance, integration, flexibility, scalability, and availability. The Cisco Webex Cloud is a communications infrastructure purpose-built for real-time web-based communications. The service enables global users, employees, and virtual teams to collaborate in real time from anywhere, anytime, on mobile devices, PCs, laptops, or video systems almost as though they were working in the same room. Solutions include meetings, events, training, and support services.

In response to the specific questions and principles raised in your open letter, we provide a brief summary and overview in turn below.

1. Security

Cisco Webex enables global workforce and virtual teams to collaborate in real time almost as though they were in the same room. Businesses, institutions, schools, and governments worldwide rely on Cisco Webex solutions to help simplify business processes and improve collaboration and results for sales, marketing, training, project management, and support teams. For all these customers and users, security and privacy

are top of mind. Online collaboration tools must provide multiple layers of security depending on the sensitivity of the data involved for tasks that range from scheduling meetings, to authenticating participants, and to sharing confidential documents.

At Cisco, we are committed to building trustworthy solutions with embedded security across multiple platforms. Cisco's Security and Trust Organization works with teams throughout the company to build security, privacy, trust, and transparency into a framework that supports the design, development, and operation of core infrastructures to meet the highest levels of security and privacy in everything we do. We integrate data protection, privacy, and security requirements into product design and development methodologies throughout the entire product lifecycle, from ideation and concept commit through to launch, operations, use, and end of life with the Cisco Secure Development Lifecycle (CSDL). CSDL is a repeatable and measurable process designed to increase Cisco product resiliency and trustworthiness and confirm privacy requirements, impact, and risks are appropriately addressed. The combination of tools, processes, and awareness training introduced during the development lifecycle promotes defense-in-depth, provides a holistic approach to product resiliency, and establishes a culture of security and privacy. Click here for more information on CSDL.

Cisco conducts rigorous penetration testing regularly, using internal assessors and "red teams". Beyond its own stringent internal procedures, Cisco's Information Security team also engages independent third parties to perform audits against Cisco internal policies, procedures, and applications. These audits are designed to validate mission-critical security requirements for both commercial and government applications. Cisco also uses third-party vendors to perform ongoing, in-depth, code-assisted penetration tests and service assessments. Users are promptly notified of software updates (security patches and feature/functionality enhancements) and prompted to install the latest version immediately.

End-to-end security controls are embedded within the Cisco Webex platform to protect intellectual property, privacy, and data. The Cisco Webex platform common identity service supports customer owned identity provider (IdP) solutions from multiple vendors for authentication and authorization through the SAML and Oauth 2.0 standard protocols. Customers opting for a corporate identity provider can also add any multi-factor authentication (MFA) mechanism that they choose. For customers that do not operate their own IdP service, an advanced security offer is available to add Cisco's world class MFA solution. Administrators and hosts determine if attendees need to be authenticated before joining a meeting to ensure only

known and authorized users can participate. Password policies (length, complexity, renewal, excluded or previous passwords, etc.) are determined by the IdP administrator and can be as complex as the chosen IdP solution permits.

All communications between Cisco Webex applications and Cisco Webex Cloud occur over industry standard encrypted channels that utilize high strength cipher suites. All media streams (i.e., audio VoIP, video, screen share, and document share) are encrypted. The security controls within Cisco Webex are designed with the principle of least privilege or "need to know" in order to protect sensitive information that could potentially be shared over the platform.

For standard meetings, Cisco Webex media servers may need to decrypt media for PSTN, transcoding and recording. However, these features can be disabled by the administrator. For businesses requiring a higher level of security, Cisco Webex customers can opt for true end-to-end encryption (E2EE) of video, audio, text, and meeting content. With E2EE enabled by the administrator, Cisco Webex does not have access to the encryption keys used by meeting hosts and participants and cannot decrypt the data nor media streams.

With E2EE, the meeting encryption key is generated by the meeting host and securely distributed to only the meeting participants. While E2EE provides enhanced security, customers will lose some optional functionality (e.g., image thumbnails, transcription, virtual assistant, etc. - anything that would require Cisco to have access to meeting content) as the trade-off.

To verify and demonstrate our security posture, Cisco Webex maintains SOC2 Type II and ISO 27001, 27017 and 27018 certifications. The SOC2 Type II certification includes the Privacy Trust Principle, which addresses the collection, use, retention, disclosure and disposal of personal information. The Cisco Webex ISO 27001 certification assures compliance with requirements for an Information Security Management System, of which privacy is an integral element. Cisco shares additional information regarding our compliance with these certifications to our customers and key stakeholders upon request, under a non-disclosure agreement.

2. Privacy-by-design and default

As mentioned above, Cisco integrates data protection, privacy, and security requirements into product design and development methodologies from ideation through to end of life with CSDL. Satisfying the product security baseline (PSB) -- which includes a privacy impact assessment (PIA) -- within CSDL is a mandatory requirement and integral part of product development at Cisco. Privacy by design/default principles, such as data minimization, role-based access controls etc., and ensuring functionality is built-in to honor data subject rights are a core part of Cisco engineering. We use privacy engineering techniques and threat modelling to evaluate and build better offerings to turn privacy by design principles into actionable product requirements. The CSDL process with a mandatory PIA enables us to assess whether a product processes sensitive personal data or other confidential information and make sure privacy controls are built in from the start. As the product matures and evolves, any material changes in data collection, processing, or use also goes through CSDL and a PIA.

Cisco also conducts a variety of multi-media (online, print, video, etc.) campaigns throughout the year to raise awareness and train employees about data protection and privacy. We maintain an active intranet for collaboration and communications at all levels within the company. These include business conduct, data protection, security, privacy, and specialized training on GDPR and other global laws. Beyond basic awareness training, Cisco encourages employees to pursue further training with options ranging from websites, multimedia, self-paced courses, and relevant external certifications (e.g., Certified Information Privacy Professional (CIPP) from the IAPP). All trainings are available to all employees and required for those with direct responsibility for privacy compliance. We currently have over 200 CIPP trained privacy professionals within Cisco. We believe that employee awareness and skills in these disciplines are vital to Cisco's long-term success and ensuring that everyone is focused on building products with appropriate privacy protections and functionality.

Cisco Webex includes multiple privacy protecting and enhancing features that are configurable by the customer/administrator of their instance to meet their own privacy requirements. For example, Cisco Webex includes role-based access to meetings enabling different participants in meetings to have different permissions, access, and controls. We also allow clients to control whether their end users can record meetings, upload files, or use additional features that would result in additional data collection.

To assist customers with completing an internal security impact analysis (SIA) and PIA, Cisco can provide, upon request and under a non-disclosure agreement, standardized information gathering (SIG) and consensus assessment initiative questionnaires (CAIQ).

3. Know your audience

Cisco Webex is used by customers in a variety of industries and has been designed to address their specific needs. Cisco Webex has been a key tool for businesses, schools, medical institutions, governments, and others for more than a decade. The Cisco Webex Trusted Platform page on the Cisco Trust Center, located here, provides additional details around how customers in specific verticals can use Cisco Webex consistent with their own security and privacy requirements. For example, Cisco Webex is a FedRAMP approved solution for use by the U.S. government and has been assessed for compliance as a Business Associate under the U.S. Health Insurance Portability and Accountability Act (HIPAA).

Cisco Webex is also a trusted tool for use in schools and supports the increased demand for distance learning solutions. Cisco provides extensive documentation and guidance for schools, districts, universities, and others around the data collected, how it is used, any third-party recipients, and how it is secured. It also includes education materials to help parents and guardians understand how Cisco Webex works and what it means for their children. Please visit the Cisco WebEx for Education page, located here, for more details.

Cisco WebEx provides full control and flexibility to hosts and meeting moderators so they can enable appropriate measures and safeguards based on the sensitivity of their discussions and data sharing. In addition, Cisco WebEx integrates with Cisco Cloudlock, which is a cloud-native access security broker (CASB) for security policy enforcement.

Cisco WebEx adheres to accessibility requirements and has been tested against the Voluntary Product Accessibility Template (VPAT) 2.1 to conform to Section 508 of the US Rehabilitation Act. Cisco continuously updates VPAT templates and related documentation on our public website to make sure our products meet evolving accessibility needs.

4. Transparency and Fairness

Transparency and fairness are key pillars of Cisco's Data Protection & Privacy Program. Our Online Privacy Statement provides an overview of how personal information is handled company-wide, globally. For product specific information, we have also created privacy data sheets and maps that supplement the general Privacy Statement and provide more detailed, product specific information about how and what personal information is collected, used, processed, transferred, secured, stored, and deleted. In addition, notifications and disclosures are provided within the application pro-actively when certain features are utilized. For instance, if the meeting host decides to record a meeting, all participants are notified via an on-screen pop-up and an automated voice/audio message. This notification is also provided to new participants when they join the meeting. A red circle icon is also visible to all participants and persistent so long as the recording is enabled.

5. End-user control

Cisco strongly believes that individuals should have control of their own data and provides a best practices guide for secure meetings for Site Administrators and Hosts to help them enforce our recommended settings and practices to enhance security and privacy.

The Cisco Webex Meetings platform was designed with an individual's privacy in mind. From the start of the meeting experience where users are prompted to enable access to their video and microphone (both off by default) to in meeting capabilities such as recording, close captioning, and transcription. Multi-lingual and accessible icons with tool tip text are located throughout the user interface to draw attention to these capabilities, giving an individual the opportunity to enable/disable at their discretion.

To ensure an individual has a transparent view of how the Cisco Webex platform handles any data that may be collected using these Cognitive Collaboration based capabilities, Cisco has created the following white paper to outline what data is being collected, used, and stored and also how each individual user may opt-in or opt-out of these services.

Thank you again for the opportunity to respond to your open letter and provide information on how we, at Cisco, approach privacy within our videoconferencing product – Cisco Webex. We are committed to providing Cisco Webex as a world class collaboration tool that maintains strong security and privacy protecting and enhancing functionality for all our customers and users. If there is any further information we can provide you as you explore these important issues, please don't hesitate to reach out to the Cisco Privacy Office by emailing privacy@cisco.com. We would welcome the opportunity to work with you and your teams to ensure privacy is appropriately respected and protected when using videoconferencing technologies.

Best regards,

Harvey Jang
Vice President & Chief Privacy Officer Cisco Systems, Inc.