GoToMeeting, GoToWebinar, GoToTraining & GoToStage

Security and Privacy Operational Controls

V1

February 4, 2020

LogMeIn GoToMeeting, GoToWebinar, GoToTraining, & GoToStage Security and PrivacyOperational Controls (SPOC)

Publication Date: 2/4/2020

1 Products and Services

This document covers the security and privacy controls for LogMeIn GoToMeeting, GoToWebinar, GoToTraining, and GoToStage (collectively referred to as “GoTo Services”).

The GoTo Services are online communication services that enable individuals and organizations to interact using various features, depending upon service offering, that may include desktop screen sharing, video conferencing, and integrated audio. The GoTo-Services are delivered via web browser or client executable, through a globally distributed network of proprietary hardware and software.

- GoToMeeting enables users to schedule, convene and moderate meetings using the GoToMeeting web site and/or executable customer software.
- GoToWebinar enables organizations to conduct one-to-many information presentation events reaching local and global attendees over the Internet. Webinars are scheduled, convened and moderated using the GoToWebinar web site and/or executable customer software.
- GoToTraining enables users to schedule, convene and moderate training sessions using the GoToTraining web site and/or executable customer software. It provides specific features applicable to web-based training, such as online access to tests and materials and a hosted course catalog.
- GoToStage is an online portal where GoToWebinar organizers can create customizable channels and publish their webinar recordings. Published recordings are showcased on the GoToStage homepage, organized by business categories. At any point, organizers can unpublish their recording through GoToWebinar, which removes the video from their channel page and the GoToStage ecosystem.

2 Product Architecture

Screen-sharing between participants in GoTo Services sessions occurs via an overlay networking stack that logically sits on top of the conventional TCP/IP stack within each user's PC (see Figure 1).

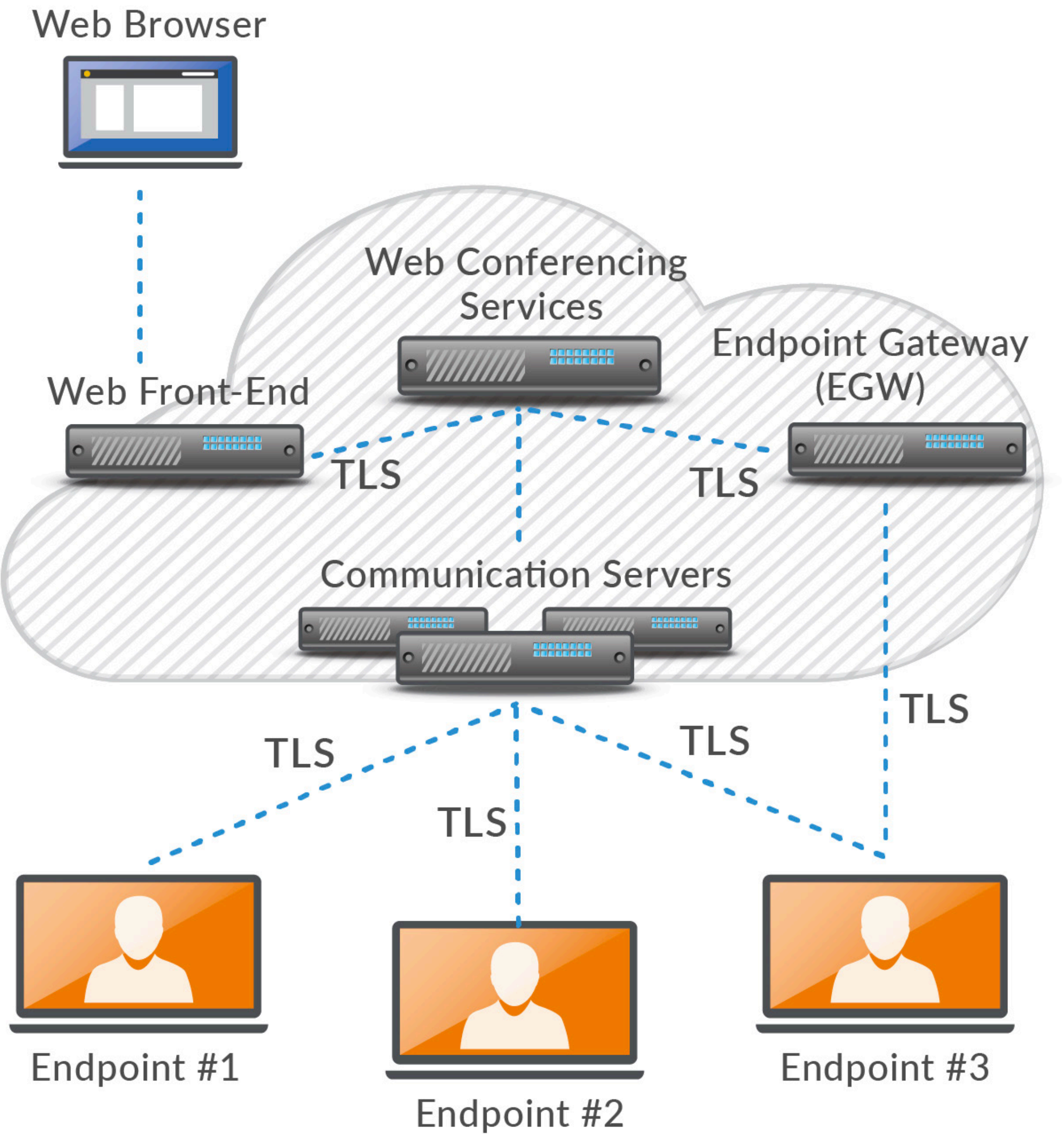

Figure 1- LogMeIn GoToMeeting, GoToWebinar, GoToTraining, & GoToStage architecture.

***Web Front-End** – Portal Web Page of GoTo suite; Hosted in Tier 1 co-location data centers*

***WCS** – Session Scheduling; Meeting History; GTM Organizer Settings; Hosted in Tier 1 co-location data centers*

***Communication Server** – incl. Screen Sharing Server, Audio Bridges & Voice gateways (acts as proxy), H.323 gateways – hosted on Amazon Web Services / **Multicast Communication Server** and Video Cluster Server are hosted in Tier 1 co-location data centers*

***Endpoint Gateway (EGW)** – handles Organizer and Participant Endpoint connections and encryption mechanism – EGW is hosted on Amazon Web Services*

Participants (session endpoints) communicate with infrastructure communication servers and gateways using outbound TCP/IP connections on port 443, where the participants can be located anywhere on the Internet. Clients generally communicate to the GoTo Services via the endpoint gateway. However, new clients communicate directly using Representational State Transfer (REST) calls to the backend services via load balancers. The service infrastructure also allows public switched telephone network (PSTN) users to dial into a meeting.

The GoTo Services use an application service provider (ASP) model designed to ensure secure operations while integrating with a company's existing network and security infrastructure.

The architecture has been designed for high performance, reliability and scalability, and is driven by high-capacity servers and network equipment with appropriate security patches in place. Redundant switches and routers are designed to preclude single points of failure. Clustered servers and backup systems are in place to ensure application processes in the event of a heavy load or system failure. Web Conferencing Services load balance the client/server sessions across geographically distributed communication servers intended to ensure performance and adequate latency.

The service infrastructure is primarily hosted in Tier 1 co-location data centers, with some component services hosted on cloud hosting providers. The audio bridge services are hosted completely on cloud providers, while some of the product Web Conferencing Services are hosted on cloud providers. The data associated with any service hosted on a cloud provider is also stored on that provider.

Physical access to co-location hosted servers is restricted and continuously monitored. All facilities have redundant power and appropriate environmental controls. Firewall, router and VPN-based access controls are employed to secure LogMeIn private-service networks and backend servers. Infrastructure security is continuously monitored, and vulnerability testing is conducted regularly by internal staff and external third-party auditors.

For more information, please see the UCC Security White Paper [1].

3 GoTo Services Technical Security Controls

LogMeIn employs industry standard technical controls appropriate to the nature and scope of the Services (as the term is defined in the Terms of Service [2]) designed to safeguard the Service infrastructure and data residing therein.

3.1 Logical Access Control

Logical access control procedures are in place, designed to prevent or mitigate the threats of unauthorized application access and data loss in corporate and production environments. Employees are granted minimum (or "least privilege") access to specified LogMeIn systems, applications, networks, and devices as needed. Further, user privileges are segregated based on functional role and environment.

3.2 Perimeter Defense

LogMeIn employs industry standard perimeter protection tools, techniques and services that are designed to prevent unauthorized network traffic from entering our product infrastructure. The LogMeIn network features externally facing firewalls and internal network segmentation. Cloud resources also utilize host-based firewalls. In addition, a third party, cloud-based distributed denial of service (DDoS) prevention service is used to protect against volumetric DDoS attacks; this service is tested at least once per year. Critical system files are protected against malicious and unintended infection or destruction.

3.3 Data Segregation

LogMeIn leverages a multi-tenant architecture, logically separated at the database level, based on a user's or organization's LogMeIn account. Only authenticated parties are granted access to relevant accounts.

3.4 Physical Security

Datacenter Physical Security

LogMeIn contracts with co-location data centers to provide physical security and environmental controls for server rooms that house production servers. These controls include:

- Video surveillance and recording
- Multi-factor authentication to highly sensitive areas
- Heating, ventilation, and air conditioning temperature control
- Fire suppression and smoke detectors
- Uninterruptible power supply (UPS)
- Raised floors or comprehensive cable management
- Continuous monitoring and alerting
- Protections against common natural and man-made disasters, as required by the geography and location of the relevant data center
- Scheduled maintenance and validation of all critical security and environmental controls

LogMeIn limits physical access to production datacenters to authorized individuals only. Access to a hosting facility requires the submission of a request through the relevant ticketing system and approval by the appropriate manager, as well as review and approval by Technical Operations. LogMeIn management reviews physical access logs to datacenters and server rooms on at least a quarterly basis. Additionally, physical access to datacenters is removed upon termination of previously authorized personnel.

3.5 Data Backup, Disaster Recovery and Availability

LogMeIn's architecture is generally designed to perform replication in near-real-time to geographically diverse locations. Databases are backed up using a rolling incremental backup strategy. In the event of a disaster or total site failure in any one of the multiple active locations, the remaining locations are designed to balance the application load. Disaster recovery related to the system is tested periodically.

3.6 Malware Protection

Malware protection software with audit logging is deployed on all GoTo Services servers. Alerts indicating potential malicious activity are sent to the appropriate response team.

3.7 Data Confidentiality and Authenticity

LogMeIn maintains a cryptographic standard that aligns with recommendations from industry groups, government publications, and other relevant standards groups. The cryptographic standard is periodically reviewed, and selected technologies and ciphers may be updated in accordance with the assessed risk and market acceptance of new standards.

3.7.1 Data in Transit

GoToMeeting, GoToWebinar and GoToTraining provide security measures for data in transit that are designed to protect against passive and active attacks against confidentiality, integrity and availability. Screen and video-sharing, VoIP, webcam video, keyboard/mouse control and text-based chat information (each, “Session Data”) have industry standard communications security controls.

Session Data is never exposed in clear text during transmission between endpoints and LogMeIn’s Communication Servers.

Communications security controls based on strong cryptography are implemented at two layers: (i) on top of the transmission control protocol (TCP) and user datagram protocol (UDP); and (ii) the multicast packet security layer (MPSL).

TCP and UDP Security

Internet Engineering Task Force (IETF)-standard transport layer security (TLS) protocols are used in order to protect TCP communication between endpoints.

For their own protection, LogMeIn recommends that customers configure their browsers to use strong cryptography by default whenever possible, and to ensure that operating system and browser security patches are kept up to date.

When TLS connections are established to the website and between GoToMeeting, GoToWebinar or GoToTraining components, LogMeIn servers authenticate themselves to clients using public key certificates. For added protection against infrastructure attacks, mutual certificate-based authentication is used on all server-to-server links (e.g., Communication Servers to Web Conferencing Services).

For data sent with UDP, an existing TLS connection is leveraged to securely exchange cryptographic keys that are used to encrypt and authenticate UDP data.

Multicast Packet Layer Security

Session Data is protected by encryption in transit and integrity mechanisms, designed to prevent anyone with access to the communications servers (whether friendly or hostile) from eavesdropping on a session or manipulating data without detection. Unique to LogMeIn products, the MPSL provides an added level of communication confidentiality and integrity.

Multicast Data such as screensharing, keyboard/mouse control, chat and in-session state information is protected by this additional security layer which uses a 128-bit AES encryption in counter mode for further protection against eavesdropping.

Plaintext data is typically compressed before encryption using proprietary, high-performance techniques to optimize bandwidth. Data integrity protection is accomplished by including an integrity check value currently generated with the HMAC-SHA-1 algorithm.

Key establishment is accomplished by using a randomly generated 128-bit seed value selected by the GoTo service, that is distributed to all endpoints over TLS and used as the input to a NIST-approved key-derivation function. The seed value is erased from the service memory when the session ends.

Audio Security

Integrated audio conferencing for GoToMeeting, GoToWebinar and GoToTraining sessions is provided through the PSTN as well as Voice over Internet Protocol (VoIP). The PSTN is, by design, intended to provide for the confidentiality and integrity of voice communications. To protect the confidentiality and integrity of VoIP connections from the endpoints to the voice servers, The SRTP with AES-128-HMAC-SHA1-based protocol is used over UDP and TCP. Keys are exchanged by the client and server over an established TLS-protected HTTPS connection.

Video Security

To protect the confidentiality and integrity of video connections provfrom the endpoints to the video servers, LogMeIn leverages a SRTP with AES-128-HMAC-SHA1-based protocol. Keys are exchanged by the client and server over an established TLS-protected HTTPS connection

Webcast Security

GoToWebinar webcasts use communications servers, broadcast gateways and third-party content delivery networks which are designed to reliably deliver screen sharing, audio and video to attendees joining from a browser. Media is transmitted through HTTP Live Streaming (HLS) protocol, while the broadcast gateways mix and transcode the data into multiple bitrates to enable adaptive delivery for clients with sub-optimal network connections. The gateways use RTP and HTTP to transport the output media streams to the CDN, which then delivers the streams to attendees over HTTPS.

GoToStage

GoToStage is an online portal where GoToWebinar organizers can create customizable channels on which to publish their webinar recordings. Published recordings are showcased on the GoToStage homepage, organized by business categories. A video published to GoToStage is available for discovery on the GoToStage homepage and in search engine results, unless the organizer restricts discoverability using the administrative settings on his or her channel page. Otherwise, anyone registered to GoToStage can view the recording with a direct link to the channel or to the video's unique "Watch Now" page. Visitors register for GoToStage using their name and email address or may connect via select social media accounts such as LinkedIn, Facebook and Gmail. Once registered, a signed S3 URL with a set TTL is used to playback the webinar recording. At any point, organizers can unpublish their recording through GoToWebinar, which removes the video from their channel page and the GoToStage ecosystem. GoToStage administrative functions are password secured, and all connections in the GoToStage portal are protected using TLS.

3.7.2 Data at Rest

GoToMeeting, GoToWebinar and GoToTraining allow organizers to record their live sessions, including audio, video and screen content. When an organizer starts recording, every attendee is notified that the recording has begun, and a visual indicator appears on the control panel to reflect that recording is in progress.

Customers can elect to store session recordings on their local machine or in the cloud.

Cloud Recordings
Cloud recordings are stored on AWS S3. Files are encrypted at rest using server-side encryption using 256-bit AES

Transcripts
If enabled by the organizer, Google Cloud Speech-to-Text technology is used to transcribe session recordings. Audio files are transferred using TLS for transcription, where the file is encrypted using 256-bit AES and deleted immediately after speech-to-text processing is complete. Transcripts will be maintained by LogMeIn using its AWS S3 instance and made available to the organizer under Cloud Recordings.

Content uploading
Some of LogMeIn's services provide capabilities for organizers to upload videos for use in live sessions. This uploaded content is also stored in AWS S3 with 256-bit AES encryption enabled at rest, as well as in transit.

3.8 Vulnerability Management

Internal and external system and network vulnerability scanning is conducted monthly. Dynamic and static application vulnerability testing, as well as penetration testing activities for targeted environments, are also performed periodically. These scanning and testing results are reported into network monitoring tools and, where appropriate and predicated on the criticality of any identified vulnerabilities, remediation action is taken.

Vulnerabilities are also communicated and managed with monthly and quarterly reports provided to development teams, as well as management.

3.9 Logging and Alerting

LogMeIn collects identified anomalous or suspicious traffic into relevant security logs in applicable production systems.

4 Organizational Controls

LogMeIn operates a comprehensive set of organizational and administrative controls to protect the security and privacy posture of GoToMeeting, GoToWebinar, GoToTraining, and GoToStage.

4.1 Security Policies and Procedures

LogMeIn maintains and implements a comprehensive set of security policies and procedures, aligned with business goals, compliance programs, and overall corporate governance. These policies and procedures are periodically reviewed and updated as necessary to ensure ongoing compliance.

4.2 Standards Compliance

As a public company, LogMeIn complies with applicable legal, financial, data privacy, and regulatory requirements, and conforms with the following compliance certification(s) and external audit report(s):

- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 Type II attestation report incl. BSI Cloud Computing Catalogue (C5)
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 3 Type II attestation report
- Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI DSS) compliance for LogMeIn’s eCommerce and payment environments
- TRUSTe Enterprise Privacy Certification

4.3 Security Operations and Incident Management

LogMeIn’s Security Operations Center (SOC) is staffed by the Security Operations team and is responsible for detecting and responding to security events. The SOC uses security sensors and analysis systems to identify potential issues and has developed an Incident Response Plan that dictates appropriate responses.

The Incident Response Plan is aligned with LogMeIn’s critical communication processes, the Information Security Incident Management Policy, as well as associated standard operating procedures. It is designed to manage, identify and resolve suspected or identified security events across its systems and Services, including the GoTo Services. Per the Incident Response Plan, technical personnel are in place to identify potential information security-related events and vulnerabilities and to escalate any suspected or confirmed events to management when appropriate. Employees can report security incidents via email, phone and/or ticket, according to the process documented on the LogMeIn intranet site. All identified or suspected events are documented and escalated via standardized event tickets and triaged based upon criticality.

4.4 Application Security

LogMeIn's application security program is based on the Microsoft Security Development Lifecycle (SDL) to secure product code. The core elements of this program are manual code reviews, threat modeling, static code analysis, dynamic analysis, and system hardening.

4.5 Personnel Security

Background checks, to the extent permitted by applicable law and as appropriate for the position, are performed globally on new employees prior to the date of hire. Results are maintained within an employee's job record. Background check criteria will vary depending upon the laws, job responsibility and leadership level of the potential employee and are subject to the common and acceptable practices of the applicable country.

4.6 Security Awareness and Training Programs

New hires are informed of security policies and the LogMeIn Code of Conduct and Business Ethics at orientation. This mandatory annual security and privacy training is provided to relevant personnel and managed by Talent Development with support from the Security Team.

LogMeIn employees and temporary workers are informed regularly about security and privacy guidelines, procedures, policies and standards through various mediums including new hire on-boarding kits, awareness campaigns, webinars with the CISO, a security champion program, and the display of posters and other collateral, rotated at least bi-annually, that illustrate methods for securing data, devices, and facilities.

Furthermore, new engineering hires perform a mandatory secure development onboarding training.

5 Privacy Practices

LogMeIn takes the privacy of its Customers and end users very seriously and is committed to disclosing relevant data handling and management practices in an open and transparent manner.

5.1 Privacy Policy

LogMeIn discloses the types of information it collects and uses to provide, maintain, enhance, and secure its Services in its Privacy Policy on our public website [3]. The company may, from time to time, update the Privacy Policy to reflect changes to its information practices and/or changes in applicable law, but will provide notice on its website for any material changes prior to any such change taking effect.

5.2 GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law on data protection and privacy for individuals within the European Union. GDPR aims primarily to give control to its citizens and residents over their personal data and to simplify the regulatory environment across the EU. The Services are compliant with the applicable provisions of the GDPR. For more information, please visit www.logmeininc.com/trust.

5.3 CCPA

LogMeIn hereby represents and warrants that it will be in compliance with the California Consumer Privacy Act (CCPA) and will implement and maintain the necessary controls to adhere to the applicable provisions of CCPA no later than January 1, 2020. For more information, please visit www.logmeininc.com/trust.

5.4 EU-U.S. and Swiss Privacy Shield

LogMeIn, Inc. and its US affiliates participate in the EU-U.S. Privacy Shield Framework and Swiss Privacy Shield regarding the collection, use and retention of personal information from European Union member countries and Switzerland [4]. Certification is reviewed annually by TRUSTe and any findings are promptly addressed by LogMeIn.

5.5 Return and Deletion of Customer Content

GoToWebinar and GoToTraining Customers can delete their recordings within their services environment. Further, at any time, GoTo Services Customers may request the return or deletion of their Content through standardized interfaces. If these interfaces are not available, LogMeIn will otherwise make a commercially reasonable effort to support the Customer, subject to technical feasibility, in the retrieval or deletion of their Content. Additionally, Customer Content will be deleted within thirty (30) days of Customer request.

Upon the expiration or termination of a paid subscription to GoToMeeting, Customer's accounts shall revert to a free account. Free GoToMeeting accounts shall automatically be deleted after two (2) years of user inactivity (e.g. no logins). To account for a seasonal user base, GoToWebinar and GoToTraining accounts shall be deleted two (2) years after expiration or termination of the then-final term. GoToStage users may unpublish/remove any published webinars at any time, during an active GoToWebinar subscription, via self-service through the GoToWebinar services environment and/or by submitting a support request to LogMeIn. Upon written request, LogMeIn will certify to relevant account and Content deletion.

5.6 Sensitive Data

While LogMeIn aims to protect all Customer Content, regulatory and contractual limitations require us to restrict the use of GoToMeeting, GoToWebinar, GoToTraining, and GoToStage for certain types of information. Unless Customer has written permission from LogMeIn, the following data must not be uploaded or generated to GoToMeeting, GoToWebinar, GoToTraining, and GoToStage:

- Government-issued identification numbers and images of identification documents.
- Information related to an individual's health, including, but not limited to, Personal Health Information (PHI) identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA) and related laws and regulations.
- Information related to financial accounts and payment instruments, including, but not limited to, credit card data. The only general exception to this provision extends to explicitly identified payment forms and pages that are used by LogMeIn to collect payment for GoToMeeting, GoToTraining, GoTo Webinar, and GoToStage.
- Any information especially protected by applicable laws and regulation, specifically information about individual's race, ethnicity, religious or political beliefs, organizational memberships, etc.

5.7 Tracking and Analytics

LogMeIn is continuously improving its websites and products using various third-party web analytics tools, which help LogMeIn understand how visitors use its websites, desktop tools, and mobile applications, what they like and dislike, and where they may have problems. For further details please reference our Privacy Policy [3]

6 Third Parties

6.1 Use of Third Parties

As part of the internal assessment and processes related to vendors and third parties, vendor evaluations may be performed by multiple teams depending upon relevancy and applicability. The Security team evaluates vendors that provide information security-based services including the evaluation of third-party hosting facilities. Legal and Procurement may evaluate contracts, Statements of Work (SOW) and service agreements, as necessary per internal processes. Appropriate compliance documentation or reports may be obtained and evaluated at least annually, as deemed appropriate, to ensure the control environment is functioning adequately and any necessary user consideration controls are addressed. In addition, third parties that host or that are granted access to sensitive or confidential data by LogMeIn are required to sign a written contract outlining the relevant requirements for access to, or storage or handling of, the information (as applicable).

6.2 Contract Practices

To ensure business continuity and that appropriate measures are in place to protect the confidentiality and integrity of third-party business processes and data processing, LogMeIn reviews relevant third parties' terms and conditions and either utilizes LogMeIn-approved procurement templates or negotiates such third-party terms, where deemed where necessary.

7 Contacting LogMeIn

Customers can contact LogMeIn at https://support.logmeininc.com/ for general inquiries or privacy@logmein.com for privacy-related questions.

8 References

[1] LogMeIn, Inc., "UCC Security White Paper," LogMeIn, Inc., May 2019. [Online]. Available: https://logmeincdn.azureedge.net/gotomeetingmedia/-/media/pdfs/ucc_security_white_paper.pdf.

[2] LogMeIn, Inc., "Terms of Service for LogMeIn," LogMeIn, Inc., June 2019. [Online]. Available: https://www.logmeininc.com/legal/terms-and-conditions.

[3] LogMeIn, Inc., "LogMeIn Privacy Policy," LogMeIn, Inc., January 2018. [Online]. Available: https://secure.logmein.com/policies/privacy.aspx.

[4] LogMeIn, Inc., "LogMeIn EU-U.S. Privacy Shield Notice," LogMeIn, Inc., September 2019. [Online]. Available: https://www.logmeininc.com/legal/privacy-shield.