Enterprise Privacy Statement

Effective Date: 10/24/2016
Origination Date: 10/24/2016
Revision Date: 05/25/2018
Status: Approved

Table of Contents

Revision History

Lookout, Inc. controls this document and therefore any printing of the material will constitute a “reference” copy. Users are responsible for confirming they have the current revision. When any part of this information requires an update, the entire document shall be re-issued.

Release	Date	Description	Submitted By
1.0	10/24/2016	Current draft on public website	Marcelo Guerra
2.0	04/01/2018	Revisions to policy to maintain alignment with product offering	Kimberly Snow

Mobile Endpoint Security Privacy Statement

Lookout firmly believes that your privacy is as important as your security, so we want to be completely transparent about the data we collect to help safeguard your device and the security of your employer. Lookout, Inc. ("Lookout," "we," or "us" or "our") provides you with this Enterprise Privacy Statement to describe our information practices with respect to our Mobile Endpoint Security Products (the "Endpoint Security Product"). This Enterprise Privacy Statement governs the data collected from or about you through your installation and activation of our Endpoint Security Product on your mobile device. By downloading and activating the Endpoint Security Product, you authorize the data collection, use, disclosure, and storage practices described in this Enterprise Privacy Statement.

You may have been directed to download and install the Endpoint Security Product as a result of your employment by an organization that either (1) requires all or some of its workforce to install the Endpoint Security Product or (2) requires all or some of its workforce to install a mobile device management suite that includes the Endpoint Security Product. Please be advised that this Enterprise Privacy Statement governs only our information practices with respect to our Endpoint Security Product. To the extent you have questions or requests regarding the data collection, use, disclosure, and security practices of your employer ("Employer") or a mobile device management provider ("MDM Provider"), or about data that we collect on behalf of your Employer, you should direct those questions or requests to those parties.

Lookout reserves the right to change this Enterprise Privacy Statement at any time to reflect changes in the law, our data collection and use practices, the features of the Endpoint Security Product, or advances in technology. Please check this page periodically for changes. Your continued use of the Endpoint Security Product following the posting of changes to this Enterprise Privacy Statement will mean you accept those changes.

We have endeavored to structure this Enterprise Privacy Statement to answer your questions about our Endpoint Security Product. The Privacy Statement contains answers to the following questions:

1. What is the Lookout Mobile Endpoint Security Product?

Lookout Mobile Endpoint Security (MES) is a mobile security solution that mitigates the risks of unprotected data accessed via mobile devices. The Lookout Mobile Endpoint Security solution provides visibility into mobile threats across apps, devices and the network. Lookout Mobile Endpoint Security seamlessly integrates with and enhances existing mobile investments while minimizing help desk tickets. Leveraging a global sensor network of over 100M sensors, The Lookout MES platform delivers predictive security by using machine intelligence to identify complex patterns that indicate risk patterns that would otherwise escape human analysts. When a threat has been detected, Lookout provides employees and administrators remediation options (e.g., uninstall app, invoke conditional access). This solution is delivered through integration of the Lookout MES with leading MDM Providers.

2. What data does Lookout collect from your mobile device?

To protect your mobile device and your Employer from threats, Lookout collects certain categories of data from your device. This data **may** include:

- The manufacturer and model of your mobile device
- Certain technical settings of your mobile device, including the display size of your mobile device and firmware version
- Your IP address (which can indicate your country and geolocation)
- The type and version of operating system on your mobile device
- The unique device identifier of your mobile device
- Configuration data of your device, such as whether your device is configured to allow root access or whether hardware restrictions of the device have been removed
- Metadata of all applications installed on your mobile device (including, but not limited to, the names of the apps and the versions of the apps)
- Metadata about networks your mobile device connects to (including, but not limited to, the SID of the network, or the unique MAC/BSSID address of network equipment)
- In certain circumstances, we may also collect a copy of the application
- Data from tracking tools used to analyze product performance on your device
- How you respond to alerts from Lookout that certain applications may pose a security threat

If you use the Privacy Controls feature in our Mobile Endpoint Security Product in conjunction with an MDM Provider, we will not collect any Personal Data such as username or email address.

Please note that we need certain types of information so that we can provide the Lookout Services. If you do not provide us with such information, or if we are asked to delete it, you may no longer be able to access the Lookout Services.

3. If Lookout is collecting information about applications installed on my device, does that mean Lookout will read or review my emails or see my photos?

No. Lookout collects only metadata about applications on your device, or the application itself. Lookout does not collect user data you enter into those applications. Because Lookout does not collect any user data you enter into the applications on your mobile device, Lookout does not collect, read, review, or scan your emails, text messages, photos, or videos.

4. Does Lookout collect any other data about me outside of my mobile device?

Our Mobile Endpoint Security Product requires that all employee mobile devices be associated with a particular email address if it is installed without integration with an MDM Provider. As such, your Employer may provide Lookout with your email address to enable MES services. If the Lookout Endpoint Security Product is integrated with an MDM solution and Privacy Controls are turned on, Lookout will not collect your email address.

If you installed the Mobile Endpoint Security Product as part of a MDM Provider's product, we may also collect information about you from that MDM Provider. Please contact the applicable MDM Provider regarding that provider's privacy practices.

Lookout may also collect other information about you if you provide such information to us directly by contacting us and voluntarily disclosing such information, or by providing your information to third parties such as our partners and marketers. We may use this information to provide you with updates about Lookout and our products and services. We may also invite you to conferences and other events that Lookout may participate in or host.

5. When does Lookout collect data from my mobile device?

As described above, Lookout collects your email address from your Employer if the Mobile Endpoint Security Product is installed without an MDM. If the Mobile Endpoint Security Product is installed in conjunction with an MDM solution and Privacy Controls are turned on, Lookout does not collect your email address. After you download, install, and activate the Mobile Endpoint Security Product, Lookout will immediately begin collecting data from your device. As you install or access applications on your mobile device, we will scan those

applications for potential security threats.

6. How does Lookout use the data collected from my mobile device?

The legal basis for using your information as set out in this Enterprise Privacy Policy will depend on your relationship with your Employer and on your Employer's use case and may include the following: (a) Use of your personal information is necessary to perform our obligations under any contract with you (for example, for your employer's performance of its employment contract, or for Lookout to comply with the Terms of Service which you accept by downloading and using our apps); or (b) Where use of your information is not necessary for performance of a contract, use of your information is necessary for our legitimate interests or the legitimate interests of the Employer or others (for example, to ensure the security of the Lookout Services, operate the Lookout Services, ensure safe environments for our and your Employer's personnel and others, make and receive payments, prevent fraud and to know the customer to whom we are providing the Lookout Services); and compliance with legal requirements, such as those requiring appropriate data security.

The data we collect from your mobile device enables us to detect threats to you and/or your Employer, to improve our Endpoint Security Product, and to improve our other product offerings. In analyzing the applications on your mobile device, if we encounter an application we have not previously analyzed, we may download a copy of part or all of the application to analyze and determine if it poses a risk. We present you with the option of uninstalling the application with a security risk, or ignoring the risk. We will also collect your remediation choice for malicious files and applications (e.g., uninstall or ignore) and may also use the data collected to categorize the risk threat of your device (e.g. Low, Medium, High).

As an enterprise product, the Lookout MES collects the data to protect not just your mobile device, but also the security of your Employer.

We may also combine data collected from your mobile device with data collected from third parties to improve our products, including our Mobile Endpoint Security Product. This data is de-identified. If results of our analysis is shared publicly it will be done so in aggregate and de-identified to protect your privacy and the privacy of your Employer.

Where our processing of data is based on your consent, you may withdraw your consent at any time, without affecting the lawfulness of the processing that was carried out prior to withdrawing your consent. To withdraw your consent, please contact your Employer (or, where applicable, us at the contact info below).

7. Does Lookout share my data with anyone else?

Yes. As an enterprise product, certain data is shared with your Employer, or anyone authorized by your Employer to view such data. Through the Mobile Endpoint Security Product dashboard, Employers or their authorized persons are granted access to certain information related to the security of your mobile device. Your Employer may be able to see your unique device attributes such as device model and carrier. Your

Employer will have visibility into applications that we have identified as malicious, as well as those that are in violations of any applicable company policy of your Employer. Please contact your Employer about how such violations of applicable company policies may affect you.

If you installed and activated our Mobile Endpoint Security Product as part of a product by an MDM Provider, we may share data collected from your mobile device with that MDM Provider.

We may share any data related to you with third parties, including other members of our corporate family, and service providers or partners that we have engaged to perform business-related functions on our behalf. This may include service providers that: (a) provide customer, technical, or operational support; (b) fulfill orders and user or Employer requests; (c) handle payments; (d) host our online services; (e) maintain databases; (f) analyze data for product improvement and enhancement purposes; and (g) otherwise support or market our Endpoint Security Product or any other Lookout products and services. We may disclose any data related to you in response to any subpoenas, court orders, or other legal process we receive, or to establish or exercise our legal rights or to defend against legal claims. If we receive a request for information from a local, state, federal, or foreign law enforcement agency, we will endeavor to transmit those requests to your Employer for processing by the Employer, but we reserve the right to respond directly and provide the information requested where we deem such response legally appropriate. We may disclose any data related to you when we believe in good faith that such disclosure is appropriate in order to investigate, prevent, or take action regarding possible illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of this Privacy Policy, License Agreement or the End User Agreement for the Endpoint Security Product, and/or to protect the rights and property of Lookout, our employees, users and the public. This may involve the sharing of your information with law enforcement, government agencies, courts, and/or other organizations.

We may share any data related to you in connection with any merger, reorganization, a sale of some or all Lookout assets, or a financing or acquisition of all or a portion of our business by another company.

8. What information can my Employer NOT see?

Lookout does not enable your Employer to see the content of your personal email, browsing history, contacts, calendar, or your personal text messages. Your Employer may have certain rights to access this information on their own, where, for example, this information is transmitted using an Employer-provided device or network. Lookout, however, will not afford your Employer visibility into applications on your device unless they appear to contain threats or violate company policy.

9. Do you use my data for marketing purposes?

We do not use data collected by automated means from your mobile device to sell products to you, nor do we share it with third parties for their marketing purposes. We may aggregate information collected from your

device to conduct research and provide insight into mobile device security and threats. In these instances, the aggregated information included in the research is de-identified.

We may, however, use the information you provide to us directly or to third parties such as our partners and marketers to provide you with information about Lookout and our products and services, including conferences and other events that Lookout may participate in or host.

10.How does Lookout protect my data and for how long is it retained?

We have implemented reasonable administrative, technical and physical security measures to protect against the unauthorized access, destruction or alteration of your information. These safeguards are tailored to address the sensitivity of the information that we collect, process and store and as well as to the current state of technology.

Although we take appropriate measures to safeguard against unauthorized disclosures of information, because no method of transmission over the Internet or method of electronic storage is 100% secure, we cannot assure you that information that we collect will never be disclosed in a manner that is inconsistent with this Privacy Statement.

Our policy is to retain personal data only as long as reasonably necessary to provide our products and services to you and others or as otherwise required for legal compliance purposes. We may delete your data after 90 days if your account is inactive and as otherwise provided in our Terms of Service. Information may persist in copies made for backup and business continuity purposes. In this situation all data is secured with 256-bit encryption at rest.

11.Where does Lookout store my data?

Lookout is a San Francisco-based company with servers housed in the United States. Personal Data collected from users outside the United States is transferred to the United States. If you are using the Lookout Services from outside the United States your information may be transferred to, stored and processed in the United States where our servers are located and our databases are operated. Lookout has certified with the Privacy Shield framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Data from E.U. States and Switzerland. The Privacy Shield Principles lay out a set of requirements governing participating organizations' use and treatment of Personal Data received from the EU and Switzerland. By joining the Privacy Shield, participants make a commitment to comply with these Principles that are enforceable under U.S. law. Lookout has certified that it adheres to the Privacy Shield Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement for such Personal Data. To learn more about the Privacy Shield and view a list of entities who have current certifications under the Privacy Shield, or view Lookout's certification, please visit http://www.privacyshield.gov.

As required under the principles, when Lookout receives information under the Privacy Shield and then

transfers it to a third-party service provider acting as an agent on Lookout's behalf, Lookout has certain liability under the Privacy Shield if both (i) the agent processes the information in a manner inconsistent with the Privacy Shield and (ii) Lookout is responsible for the event giving rise to the damage.

If you have any questions or complaints about Lookout's privacy practices, including questions related to the Privacy Shield, you may contact us at the email address or mailing address set forth under "Contact Us if You Have Any Questions or Concerns." We will work with you to resolve your issue.

If you are a resident of the European Union and are dissatisfied with the manner in which we have addressed your concerns about our privacy practices, you may seek further assistance, at no cost to you, from our designated Privacy Shield independent recourse mechanism, which you can learn more about by visiting https://www.jamsadr.com/eu-us-privacy-shield. You also have a right to lodge a complaint with the relevant supervisory authority. However, we encourage you to contact us first, and then we will do our very best to resolve your concern.

Residents of the European Union may also elect to arbitrate unresolved complaints but prior to initiating such arbitration, you must: (1) contact Lookout and afford us the opportunity to resolve the issue; (2) seek assistance from Lookout's designated independent recourse mechanism above; and (3) contact the U.S. Department of Commerce (either directly or through a European Data Protection Authority) and afford the Department of Commerce time to attempt to resolve the issue. Each party shall be responsible for its own attorney's fees. Please be advised that, pursuant to the Privacy Shield, the arbitrator(s) may only impose individual-specific, non-monetary, equitable relief necessary to remedy any violation of the Privacy Shield Principles with respect to the individual. Lookout is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

In addition to the rights granted under the section above entitled, "You Can Access and Update Your Privacy Settings," some international users (including those whose information we collect under the Privacy Shield) have certain legal rights to access certain information we hold about them and to obtain its deletion. To exercise those rights, these users may contact us at privacy@lookout.com with their request.

The European Union has taken a step to protect the fundamental right to privacy for EU resident with the General Data Protection Regulation (GDPR) which will be effective from May 25, 2018. Any Organization that works with EU residents' Personal Data in any manner, has obligations to protect the data. Lookout takes every commercially reasonable effort inclusive of recommended technical and organizational measures to comply with the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR").

12.What are my data rights and choices?

Residents of the European Union and certain other jurisdictions may have certain rights to (1) request access to or rectification or deletion of information we collect about them, (2) request a restriction on the processing of their information, (3) object to the processing of their information or (4) in very limited situations request

the portability of certain information. To exercise these or other rights, please contact your Employer (or MDM Provider as applicable). You may also contact us using the contact information below. In appropriate circumstances, we may route the request to the Employer and follow their instructions in addressing it. Residents of France and certain other jurisdictions may also provide instructions regarding the manner in which we may continue to store, erase and share your information after your death, and where applicable, the person you have designated to exercise these rights after your death.

13.How can I contact you with more questions?

If you have additional questions, we encourage you to contact your Employer (or MDM Provider as applicable). You may also direct questions to our privacy officer at privacy@lookout.com or by postal mail at Lookout, Inc., Attn: Michael Musi, Data Privacy Officer, One Front Street, Suite 3100, San Francisco, CA 94111. Residents of the EU contact us by mail at Lookout, Inc., Attn: G.J. Schenk, SVP International Sales, Florapark 3, 2012 HK Haarlem, Netherlands.

Effective Date: May 25, 2018