Lookout Privacy Policy

Effective Date: September 21, 2016

A lot of companies say they care about your privacy - we say it and mean it!

This document is our Privacy Policy, which describes what information we collect from you and how we use it. Our Privacy Policy applies to our website at www.lookout.com, our mobile website, our mobile application, and all other services and products Lookout provides. It covers personal information, which is information we can link to you personally. Personal Information ("PI") includes data like your name, email address, phone number, or mobile device's unique identifier, among other things.

This Privacy Policy is part of the Lookout Terms of Use. Lookout reserves the right to change this Privacy Policy to reflect changes in the law, our data collection and use practices, the features of our services, or advances in technology. Please check this page periodically for changes. By continuing to use our services, you accept those changes and agree to be bound by both policies, so please read them carefully. Please contact us at privacy@lookout.com if you have any questions about this Privacy Policy.

1. We Collect Information From You to Provide You with a Service.

We are committed to only collecting the information necessary to provide and improve Lookout's services. When we do collect your information, we store it and associate it with your account unless otherwise noted. We take your privacy very seriously and will only use and disclose this information under the terms described in this Privacy Policy. Note that some of our products are standalone products, collect only limited information or no information at all. Not every section of this Privacy Policy will apply to these products.

2. Information Lookout Collects

a. Registration Information

To create an account, you must provide your email address and a password. You may also enter your mobile phone number on our website to initiate a text message with directions on how to download the app and register.

b. Credit Card Information

If you wish to upgrade to a Premium Account billed directly to us, we collect your credit card number, expiration date, and security code. We use this information to bill you for services. Lookout uses third-party payment processors and therefore has only limited information about your payment transactions.

c. Device Information

When you use Lookout services, our servers automatically record certain information about your mobile device. This information may include an equipment identifier (e.g., IMEI, UDID), subscriber identifier (e.g., IMSI), device name, mobile phone number, device type and manufacturer, operating system type and version, wireless carrier/operator, network type, country of origin, Internet Protocol ("IP") address, and the dates and times of your requests. We use this information to provide our services, and support if needed, and to calculate de-identified, aggregate statistics about the users of our products. For example, collecting your device's phone number allows the service to contact your phone via SMS when you locate your phone from the Lookout web application.

d. Employment Application Information

If you wish to fill out our employment application form, we will ask for information, including your name, email address, phone number, and allow you to upload your resume and cover letter. We use this information to determine if you are an eligible candidate for an available position, to contact you to set up an interview if appropriate and to follow up with you about your application experience.

e. Social Media Features

Our website includes social media Features ("Features"), like the Facebook recommend button or interactive mini-programs that run on our site. If you use these Features, they will collect your IP address, which page you are visiting on our site, and set a cookie to enable the Feature to function properly. Features may be hosted by a third party or hosted directly on our site. Your interactions with these Features are governed by the privacy policy of the company providing the Feature, not by Lookout's Privacy Policy.

f. Information About Your Use of Lookout Services on Your Phone

We use analytics software so that we can improve the features and usability of our products. This software may analyze information such as how often you use the application, the events that occur within the application, and where the application was downloaded. We may also use such information to show you relevant content and suggest new features, products and services that can enhance your use of the Lookout Service. We do not link the information we store within the analytics software to any personally identifiable information you submit within the mobile app.

g. Information About Your Use of Lookout's Website and Mobile Website

We use analytics services to measure how people use our website so that we can improve our products and services and provide more relevant content to you. Analytics services may work by embedding invisible images that are associated with unique identifiers on our site.

h. Premium Content & Promotions

We may ask for your email address and other contact information in order to access various Lookout content, such as whitepapers, videos, or other research materials, to participate in surveys, contests, promotions, or sweepstakes, or to obtain additional information about Lookout services and products. This information will be used to provide you with additional information on products and services from Lookout or our business partners, which might be of interest to you. You can choose not to receive such marketing communications by clicking on the unsubscribe link in our emails.

i. Other Information You Provide to Us

To the extent you use our services to voluntarily provide us with any other information, we may collect such information and use it for the purposes for which you provided such information, or as otherwise provided in this Privacy Policy.

3. What You Should Know About Specific Products

a. Security and Anti-Virus

Lookout Security products, which are available on different platforms, protect your device from malware and spyware. They scan files and applications after you download and activate Lookout Security and as new applications are installed or accessed to detect any threats to you and your mobile device. They also automatically scan your entire device periodically, and regularly update your threat definitions. In order to perform these functions, we need to collect information about the applications and files present on your device, the results of any scans performed by our services, and actions you take as a result of scanning. This may include downloading a copy of part or entire copies of application files on your device if we encounter an application that we have not previously analyzed.

What types of information Security products collect:

- Information about the type of device you are using and the operating system you are running

  Lookout's Security products collect information about the type of device and operating system you are running so that we can both improve our products and also give you more accurate information about malware and spyware that might affect you and your device(s).

- Information about scans and scan results.

  We collect information about the applications on your device in order to conduct scans and to download copies of scanned files. We also may collect information about how applications behave on your device (e.g., whether an application is sending premium-rate text messages that charge money to your phone bill) and the network services with which your applications communicate, in order to determine if any applications are behaving maliciously (e.g., whether an application is talking to a server known to host phishing websites). Each time Lookout performs a scan, we collect information that describes what files and applications are identified by the scan as potentially undesirable and your choice for remediation of those files (e.g., uninstall or ignore).

How the information that Security products collect is used:

Our purpose in collecting application data and security scan data is to provide you with protections to keep you and your data safe and to optimize and improve our Lookout services and products.

We may aggregate your data with other customers' data in non-personally identifiable, aggregated, and deidentified form to better understand current malware and spyware threats and to improve the Security service. We may also share this de-identified aggregated data publicly, in order to help others understand mobile threats and gain insights into particular mobile applications.

b. **Backup** Lookout Backup securely stores copies of data that you choose to back up from your phone.

What types of information Backup collects:

- Backup Data.

  Backup transmits a copy of the data you choose to back up to on your device to a secure server using an encrypted protocol. The data may include your contacts, call history, pictures, and other data. Lookout Backup automatically backs up your data weekly or daily, based on your settings, can download your data to transfer to a new or existing phone, and allows you to retrieve your data any time from Lookout.com.

How the information that Backup collects is used:

If you choose to use the Lookout Backup feature, we will use the data you provide to deliver the Backup service. In order to notify you in the case of malicious behavior on your phone, Lookout may scan both the data that is stored on your phone and backed up to our servers. For example, some malware has been known to spread via malicious text messages or steal money by dialing expensive phone numbers. To detect this, our system would scan the SMS messages or call history stored on your phone or backed up on our servers.

c. **Missing Device** Lookout Missing Device helps you find and secure your phone or tablet if it is lost or stolen. You can locate your phone on a map using location information provided by your phone, activate a loud siren even if your volume is muted so that you can find a phone lost nearby, wipe your phone, or lock your phone. Features and settings are controlled through our website at Lookout.com.

What types of information Missing Device collects:

- Location Data.

  Lookout derives location information in two ways. We may receive it directly from your mobile device, or, in some situations, we may receive location data from cell tower or Wi-Fi hotspot information. We may use third-party service providers to translate that information into usable location information.

How the information that Missing Device collects is used:

Our purpose in collecting this information is to provide you with the location of your device when you request it. If you activate the locate feature in Missing Device, your browser will send location information to third-party map providers (e.g. Google Maps) in order to display a map of the location within your Lookout account webpage. When activating this feature, we track the device's location for several minutes in order to provide an accurate location for you. This information is retained in your account history for as long as you wish and may be deleted by you at any time, from your account settings. If you choose to delete this information or disable your account, Lookout de-identifies this data so that it is no longer associated with any personal information. We keep that de-identified data for aggregate statistical purposes only.

d. **Signal Flare**

Signal Flare collects and stores information in the same way as Missing Device (see above). If you have enabled Signal Flare, it collects location information and sends it back to Lookout only when your battery is running low. After which, we save the phone's location at the time we received the low battery alert to Lookout.com. This feature will help you locate your phone near its last known location if you lose it and its battery dies.

e. **Safe Browsing**

Safe Browsing is a feature available when using the Android default browser or the Chrome browser. Safe Browsing identifies and warns you of unsafe websites so that you can choose to avoid visiting them.

What types of information Safe Browsing collects:

- URLs.

  To provide the Safe Browsing service, we may transmit the URLs you visit on your phone to a Lookout-provided or third-party service to determine if those URLs are unsafe (e.g., if the URLs contain phishing attacks, malwares, or exploits). If a URL you visit is determined to be unsafe, we store a record of the unsafe URL.

How the information that Safe Browsing collects is used:

We use the record of unsafe URLs you visit (1) to provide you with notice that you attempted to reach an unsafe site (e.g., when you log in to the Lookout website or via email) and (2) to improve our product. If you do not want us to record the unsafe URLs you visit, you may turn Safe Browsing off; all other Lookout features will continue to function.

f. **Theft Alerts** Lookout's Theft Alerts feature uses your device's camera and location features to help you figure out where your device might be (and who might have it) in the event that your device is lost or stolen. If Theft Alerts is activated, the application monitors the below device behaviors to trigger user alerts, which you can turn on or off at any time:

1. Incorrect password entries on your device or Lookout mobile application's lock screen;
2. Removal or change of SIM cards;
3. Enablement of airplane mode;
4. Disablement of Lookout device administrator capabilities (via device settings or through the mobile application); and
5. Powering down the device (not through a battery event).

Theft Alerts starts Backup and activates your device's camera remotely, without sound or other notification, and sends the resulting picture and its GPS coordinates to the email address associated with your account. For example, if someone steals your phone and fails to enter your password at least three times, removes your SIM card, or powers off your device, Theft Alerts could allow you to see what they look like and figure out where they are without alerting them.

What types of information Theft Alerts collects, if activated:

- Password and technical device data.
- In addition to the photographic and location information described above, the application keeps track of the above device behaviors that trigger Theft Alerts.

How the information that Theft Alerts collects is used:

When Theft Alerts is activated and a photo is taken, the picture and location data are stored briefly on our servers so we can send you an email with the picture and a map of your device's location. The picture is then deleted. We send the email to the address associated with your account (or for Group Plans, to the address associated with the device that took the photo), so remember to keep your email address up to date in your account settings. We use technical information about Theft Alert's activities on your device to study, optimize, and troubleshoot our products.

g. Group Plans

Group Plans link multiple devices to one master account that controls the Group Plan owner's device as well as certain features of devices associated with the Group Plan. Users of the additional devices on the plan retain their own unique accounts, but Group Plan owners have control over some functions of Group Plan members' devices, as described below.

What types of information Group Plans collect:

- Lookout does not collect any additional information from users in Group Plans.

How the information that Group Plans collects is used:

In a Group Plan, such as a Family Plan, one master user has authority to perform certain functions on devices belonging to other members of the group. For example, in a Family Plan, a parent device may be able to lock, wipe, or locate a child's device. The latter feature would allow a parent to access data about the child's device in the section on "Missing Device." A parent device having authority over other Group Plan users, generally does not have access to the data on a child's device unless, for example, the data on the device is downloaded and transferred to another device to which the parent phone has access. Users must agree to give the "parent" this functionality. You can determine if your device is part of a Group Plan by checking the settings on your device.

h. Customer Care Web Application

If your mobile operator participates in our Customer Care Web Application program, you can call your mobile operator to find and secure your phone or tablet if it is lost or stolen. Customer Care Web Application enables mobile operators and their customer service representatives to perform remote functions on your device at your request, including:

- Locating the device,
- Locking the device,

- Wiping the device, or
- Activating a loud siren (Scream®).

Customer service representatives may perform such functions only at your request and with your consent.

Additional types of user information Customer Care Web Application collects:

- Your phone number, if available, and information about the type of device and operating system you are using to ensure that customer service representatives accurately identify and manage the remote functions on your device.

To protect users' privacy, whenever a customer service representative executes any of the above functions, Lookout immediately notifies the user via email. Customer service representatives do not have access nor control over any user data backed up via Lookout's mobile application.

4. Cookie Policy

Like many online services, we use cookies and other tools to collect and analyze information about you and your usage of our services. We also use these technologies to deliver content for relevant Lookout products and services. Cookies are small data files that we transfer to your computer. We use "session" cookies to keep you logged in while you use our services, to better understand how you interact with our services, and to monitor aggregate usage and web traffic information on our services. Session cookies disappear when you log out and close your browser. We also use "persistent" cookies to recognize you when you return to our services. Persistent cookies can stay on your computer for a longer period of time than session cookies do.

Most Internet browsers automatically accept cookies, but you can change your settings or use third-party tools to refuse cookies or prompt you before accepting cookies from the websites you visit. You can also use your browser settings or other tools to delete cookies you already have. Please be aware that some parts of our services may not work for you if you disable cookies.

Cookies From Third-Parties

We believe it is important for you to know exactly what cookies we use in our services. Here is a list of the thirdparty cookies that we currently use, which may collect personal information about your online activities over time and across third-party websites or online services. As we develop and improve our services, we may use other third parties that are not listed below. We have also included a link to the privacy policy governing the third-party cookie.

- **Google Analytics and MixPanel -** These cookies allow us to see how you use our website and mobile application so that we can improve your experience. We encourage you to read the Google Privacy Policy and MixPanel Privacy Policy. If you don't want data reported by Google Analytics, you can install the Google Analytics Opt-out Browser Add-on.
- **Optimizely -** These cookies allow us to optimize the look, feel and messaging of our website based upon how you use it. You can read the Optimizely Privacy Policy here.
- **Greenhouse -** These cookies are used to provide you with a personalized user experience when you apply for a job with us. You can read the Greenhouse Privacy Policy here.

- **Marketo -** These cookies help us track your visits to our website and enable us to create an engaging marketing experience for you. We also use Marketo cookies to understand your interaction with the emails we send you, and to ensure we're sending you relevant information. For example, Marketo cookies let us know whether our emails have been opened, and which links are clicked. You can read the Marketo Privacy Policy here.
- **LinkedIn Insights -** These cookies help us track your visits and your interactions on our website so that we can provide with you an engaging marketing experience. They also enable us to deliver more relevant services and content on lookout.com and on LinkedIn's partner sites. You can read the LinkedIn Privacy Policy here.

If you prefer not to use any cookies, you can also opt out in some browsers by turning on "Do Not Track" or by visiting the Network Advertising Initiative Consumer Opt-Out Page or the Digital Advertising Alliance Opt-Out Page to opt out directly from providers who participate in those programs. Lookout does not control or operate these tools or the choices that advertisers and others provide through these tools. We currently do not support Do Not Track browser settings, but are committed to supporting it in the future once there is a consistent industry standard for compliance.

5. We Use Your Information to Provide, Improve, and Promote our Services.

We use your information to provide you with a better service, improve the quality of our products and services, and promote our services. For example:

- If you fill out a survey or email Lookout for support, we may retain the information you give us in order to provide you with support and to improve our services.
- Where available, Lookout may use client device information to let you know you need to update your operating system.
- We may send text messages to your phone to communicate with your device.
- We may use your email address or mobile number to send privacy or security related notices and notify you of major Lookout services changes.
- We may use your email address or mobile phone number to communicate about product announcements and special promotions from Lookout or our business partners, or to administer participation in special events, surveys, contests and sweepstakes.
- We may use your information to conduct market research and engage in joint promotional activities with companies that have products that can add value to Lookout products or services (for example, with mobile operators).

You can choose to opt out of receiving emails or notices from us at any time by logging into your web account and changing your account preferences or by clicking the unsubscribe button/link at the bottom of our emails.

6. We May Disclose Your Information in Accordance with the Law.

Like other companies, we may disclose your information in accordance with law, for example, to (i) comply with a law, regulation, or legal request (including to meet national security or law enforcement requirements); (ii) protect the safety of any person; (iii) address potential violations of our Privacy Policy or Terms of Service; (iv) investigate fraud, security, or technical issues; or (v) protect Lookout's rights or property, our employees, users and the public.

However, we strongly believe that you have a right to know if we are required by law to disclose your information. As such, before we disclose your Information in response to a law enforcement request (for example, a subpoena or court order), we will notify you at the email listed in your account, unless (a) we are prohibited from doing so or (b) in emergency cases where notice could create a risk of injury or death to an identifiable individual or group of individuals, or the case involves potential harm to minors. In such cases, we might delay notice to you. Furthermore, nothing in this Privacy Policy is meant to limit any legal defenses or objections that you may have to a third party's, including the government's, request to disclose your information.

7. We Share Your Information to Provide or Improve Our Services

- We share your information to provide or improve our services. For example:
- We may share your information with third party providers of products and services integrated with our software that need to know your information to fulfill your product or service requests (for example, to map your location or send you an SMS), support our products and services, or analyze data for product performance and product improvement purposes.
- We may share your information with mobile operators who participate in our Customer Care Web Application program to enable them to assist you directly with Lookout Missing Device features, such as remote locate, lock, wipe, or Scream® through our Customer Care Web Application, at your request.
- We may share your information to perform accounting, auditing, billing reconciliation, and collection activities.
- We may share your information with our affiliates, resellers or other third party service providers that are working with Lookout (for example, mobile operators and MDM providers) to ensure proper delivery of your purchase and related support services, perform business-related functions, and provide you with information about products and services.

8. We Share Your Information to Avoid Unnecessary Marketing

In order to prevent you from receiving duplicate or unnecessary marketing about Lookout products or service, we may share your information or your status as a current Lookout customer with our partners or service providers.

9. We Share Data That is Aggregated and De-Identified

We share de-identified, aggregated data with partners and third-parties and in security reports. For example, we may share the number of devices that have ever encountered a particular piece of malware in our security reports. Aggregated data will not reveal any registration information, credit card information, or unique mobile device identifiers associated with you.

10. You Can Access and Update Your Privacy Settings

Both the Lookout website and the Lookout 'Settings' on your device have options that allow you to update or modify your privacy settings at any time. To protect your privacy and security, we require your username and password in order to verify your identity before granting you profile access or making changes. If your email address changes, you may update your information within the Lookout website. Simply go to the "Account" page and select the information you wish to update. If you wish to correct or delete inaccuracies within your personal information, or to request access to any personal information we obtain about you, please contact us at privacy@lookout.com. We will respond to your request to access within 30 days. In certain situations, however, Lookout may not be able to provide access to or delete all of the personal information that it holds about you.

11. Data Retention Policy

Our policy is to retain data only as long as reasonably necessary to provide our products and services to you and others.

Except for current Premium Accounts, we reserve the right to delete (i) all Backup Data if you have not accessed our services for 90 consecutive days, or (ii) pictures and call history from your Backup Data if you have not upgraded to a Premium Account within 90-days after your Premium trial or if you have discontinued your Premium Account for 90 consecutive days. We will notify you via the email address associated with your account before deleting your Backup Data.

12. You Can Delete Location Data at Any Time

When you delete location data through your account dashboard on Lookout.com, it is no longer linked to your account and is de-identified on our application production systems.

13. Information Posted to Our Blog and Community Forum Are Public

If you comment on our blog or other public forums, you should be aware that any information you submit there can be read, collected, or used by other users of those blogs, and could be used to send you unsolicited messages. We are not responsible for the information you choose to submit in these blogs or for any content you receive as a result of sharing such information.

To request removal of your personal information from our blog or community forum, contact us at privacy@lookout.com. If we are not able to remove your personal information, we will let you know why.

14. We Take Security Seriously

Lookout is a security company, and securing your data is one of our top priorities. Lookout uses commercially reasonable physical, managerial, and technical safeguards. For example, we use a combination of firewalls, encryption, authentication, physical security, and other safeguards to protect your account and your data.

We perform third-party penetration tests to harden our systems from attack. Because no method of transmission over the Internet or method of electronic storage is 100% secure, we cannot ensure or warrant the security of any information that Lookout receives on your behalf to operate the Lookout services, or information that you transmit to Lookout. All such receipt or transmission of your information is at your own risk.

We cannot guarantee that such information will not be accessed, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards.

The security of your personal information is important to us. When you enter sensitive information (such as credit card number or location based information) on our website, within the Lookout app, or in our order forms, we encrypt that information using secure socket layer technology (SSL).

If Lookout learns of a security breach, we may attempt to notify you electronically so that you can take appropriate protective steps. Lookout may also post a notice on the Lookout services if a security breach occurs. Depending on where you live, you may have a legal right to receive notice of a security breach in writing.

15. You Are Responsible for Maintaining the Accuracy and Confidentiality of Your Email Address & Password

You are responsible for maintaining the secrecy of your password at all times. We recommend a strong password that you do not use with other services. If you believe your password has been compromised, please change your password immediately via the Lookout website, or contact us at support@lookout.com for assistance. You are responsible for ensuring that the email address associated with your account is accurate. We use that email to contact you about service updates, changes to our policies, and account activities such as requests for your information or locate attempts on your device. Lookout is not responsible for personal data transmitted to a third party as a result of a user's providing an incorrect email address.

16. International Visitors and the Privacy Shield

Lookout is a San Francisco-based company with servers housed in the United States. Personal information collected from users outside the United States is transferred to the United States. Lookout has certified with the U.S. - Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from Switzerland. Lookout may process some personal data from individuals or companies in Switzerland via other compliance mechanisms, including data processing agreements based on the EU Standard Contractual Clauses. To learn more about the U.S.-Swiss Safe Harbor program, and to view Lookout's certification, please visit http://export.gov/safeharbor.

Lookout has further certified with the Privacy Shield as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of "personal data" (as defined under the Privacy Shield principles) from applicable European Union member countries. 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, view a list of entities who have current certifications under 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

Residents of the European Union may 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, nonmonetary, 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.

17. You Need a Parent's Permission to Use Lookout if You Are Under 13

Lookout does not knowingly collect or store any personal information about children under the age of 13 unless they are part of a Group Plan purchased by a parent who consents to such collection and storage as described in the Lookout Terms of Service. If you believe a child is using this service without parental consent, please contact us at privacy@lookout.com.

18. We Are Not Responsible for Content on Third-Party Websites

Our site contains links to other websites. When you click on one of these links, you leave Lookout's website and go elsewhere. Lookout does not accept liability for misuse of any information by any website controller to which we may link. We encourage you to read the privacy statements of these linked sites, which may differ from ours. In addition, if you take advantage of an offer from one of our partners, you may be providing information directly to that partner. We encourage you to review the privacy statements of these partners, as we are not responsible for the privacy practices of any partners or linked sites.

19. This Privacy Policy Will Apply Upon Change in Control

In the event that Lookout is involved in a bankruptcy, merger, acquisition, reorganization, or sale of assets, your information may be sold or transferred as part of that transaction.

20. We Post Updates on Our Website Whenever This Policy Changes

This Privacy Policy may be revised to keep pace with changes in our products and services and laws applicable to Lookout and you. If we make material changes to this policy, then we will notify you in our application, here on this website, by email, or by means of a notice on the Lookout home page. Please note that your continued use of our services means that you agree with, and consent to be bound by, the new Privacy Policy. If you do not wish your information to be subject to the revised Privacy Policy, you will need to close your account.

21. Contact Us if You Have Any Questions or Concerns

Please contact our privacy manager at privacy@lookout.com, or by postal mail at Lookout, Inc., Attn: Privacy Officer, One Front Street, Suite 2700, San Francisco, CA 94111, with any questions or comments about this privacy policy.

- Effective as of June 25, 2015. Updated to (i) include additional cookies, (ii) remove sections on Lookout for Business and Lookout Enterprise Security, and (iii) clarify how Lookout uses and shares personal information.
- Effective as of June 2, 2015. Updated to include Marketo to cookie policy.
- Effective as of October 15, 2014. Updated to include a section on Lookout Enterprise Security.

- Effective as of August 4, 2014. Updated to include a section explaining the Customer Care Web Application and to clarify our data retention policy.
- Effective as of May 15, 2014. Updated to include a section on Theft Alerts.
- Effective as of January 10, 2013. Updated to clarify how we respond to Do Not Track browser settings.
- Effective as of November 18, 2013. Updated to (1) include a section explaining information collection and use as it relates to the “Lookout For Business” product, (2) assure that, unless prohibited by law or there is an emergency creating risk of injury or death, Lookout will notify users of a request for information before disclosure or preservation, (3) clarify Backup data feature, and (4) include Greenhouse, MixPanel, and Olark privacy policy.
- Effective as of May 21, 2013. Updated to (1) include that information submitted with an employment application is a type of PII that we collect, (2) include a section on Social Media Features, (3) inform that Lookout may share PII in to prevent its customers from receiving unnecessary marketing, (4) include a section explaining information collection and use as it relates to the “Signal Flare” feature, (5) clarify use of cookies, (6) assure that, unless we are legally prohibited from doing so, Lookout will notify users of a request for information, (7) clarify data storage, and (8) assure that the Privacy Policy will continue to control information if Lookout ever experiences a change in control.
- Effective as of December 13, 2012. Updated to include section on Lock Cam.
- Effective as of October 1, 2012. Updated to (1) include section on Group Plans, (2) clarify use of cookies, and (3) permit use by children with parent’s consent as part of Group Plan.
- Effective January 12, 2012. Updated to clarify that unique device identifier (UDID) is a subset of equipment identifier that may be recorded on our servers when you use the Lookout Services, and to clarify our policy regarding the removal of personal information from blogs and community forums.
- Effective as of June 15, 2011. Updated to include Safe Browsing and Lookout Security.
- Original policy effective as of May 8, 2009.