Norton Mobile Privacy Notice

Effective: October 25, 2016

Symantec and the Norton brand have been entrusted by consumers around the world to protect their computing devices and digital assets. This Norton Mobile Privacy Notice tells You how We keep Your data protected and private with all Norton Mobile Apps. By using the Norton Mobile App, You consent to Symantec Corporation and its group of companies ("Symantec", "We", "Us," "Our") using Your data as described in this Notice.

Our Principles

We Tell You What We Collect

For each Norton Mobile App, We tell You the data it collects from Your device and what We do with it. Just click one of the links below to understand the data collected or accessed by the specific Norton Mobile App You are interested in or have installed.

View Norton Mobile Security Privacy Notice

View Norton Mobile Utilities Privacy Notice

View Norton WiFi Privacy Notice

Security, Technology, Processes, and Procedures

Security stores data within Our secured data centers and encrypts transmitted data. We continually work to ensure Our website, products, and services are protected against potential attacks to protect Your digital assets and Personal Information. For purposes of this Privacy Notice, "Personal Information" means any information that can be used to directly or indirectly identify an individual.

Data We Collect

Registration Data

You will be asked to provide information including Your email address, country, and password to register for a Norton Account.

Mobile Device Data

When You use a Norton Mobile App, We record certain information about Your mobile device. This may include information such as an equipment identifier (e.g., IMEI or UDID), subscriber identifier, mobile phone number, device name, type and manufacturer, operating system type and version, wireless carrier, network type, country of origin, and Internet Protocol (IP) address.

Location Data

Norton Mobile Apps only collect Your location data if it is required to provide the needed functionality of the product or service. The Norton App indicates whether We collect location data. If We do, We may receive it directly from the GPS on Your device or through cell tower or WiFi hotspot information even when the Norton App is not currently in use. In certain cases and depending on the service purchased, the Norton Mobile App may provide Your administrator (the account holder) with remote commands to help locate the device if it is lost or stolen and the location of Your device may be accessed by the administrator for this purpose only. We may use third-party service providers to translate that information into usable location information.

Backup Data

We store a copy of the data from Your mobile device that You choose to back up with the Norton Mobile App. This data may include Your contacts, call history, photos, text messages, and other data.

We back up Your data automatically at the frequency provided in settings, We restore Your data to a new or existing mobile device, and We allow You to retrieve Your data anytime at the Norton website.

Scans and Scan Results

We collect names of files and applications on Your device each time Norton Mobile Security performs a scan.

Log Data and Cookies

We may use cookies and analytical tools inside the Norton Mobile App to aggregate data to determine how You discovered the Norton Mobile App, how You use it, and in general to measure traffic and performance.

Social Media

If You choose to access third party Social Media Web sites and services through Our Norton Mobile App, You will be sharing information with those Social Media Services, and the information You share will be governed by their privacy policies and terms of service.

Children's Data

Our Norton Mobile Apps are not directed to persons under 13, and We do not knowingly collect Personal Information from children under 13. If You become aware that Your child has provided us with Personal Information without Your consent, please call customer support. We will take steps to remove the information and to terminate the child's account.

Data We Access

In order to perform the services You request, the Norton Mobile App may access other data on Your device, without collecting it or storing it. In such event, this will be indicated in each specific Norton Mobile App Privacy Policy.

How We Use Your Data

Your Data may be processed to provide you with the Norton mobile service You requested for one or more of the following purposes:

- Enabling and optimizing the performance of the Norton Mobile App;
- Research and development, including improving Symantec's products and services through data analytics;
- Providing You with information about potentially harmful applications on Your device;
- Combating fraud or any other criminal activity;
- Sending You promotional information, in accordance with Your permission, as required by applicable law;
- Any other purpose with Your consent; and/or
- Processing in an anonymized and/or aggregated form for one or more of the following:
  - The general security research purposes of improving the detection of malware;
  - Filing sample analysis to discover advanced malware; and/or
  - Statistical analysis of product deployment and usage, including analysis of trends and comparisons in our aggregated install base.

Sharing Your Data

We are a global organization and may transfer Your Information to other countries, including countries that may have less protective data protection laws than the country in which You are located. We will take steps to ensure the necessary level of protection is in place for these transfers. For the purposes described in this privacy statement, Your Information (i) may be stored and processed manually and/or electronically through global systems and tools; (ii) may be disclosed to vendors or third parties that process data on behalf of Symantec; (iii) may be disclosed in connection with any proposed or actual sale or other transfer of some or all assets of Symantec in the event of a reorganization, merger, acquisition, or sale of our assets; (iv) may be disclosed and shared if we are required to do so by law or in response to a request from law enforcement authorities; and/or (v) may be disclosed as otherwise permitted by You.

Additionally, in certain cases and depending on the service purchased, the Norton Mobile App may provide Your administrator (the account holder) with remote commands to help locate the device if it is lost or stolen and the location of Your device may be accessed by the administrator for this purpose only.

To promote research, awareness, detection, or prevention of security risks, Symantec may disclose Information to relevant public and private entities such as cybersecurity research organizations and security software vendors. In such cases, we will endeavor to anonymize such information or to minimize any Personal Information to the extent reasonably possible without defeating purposes of security risk research, awareness, detection, or prevention.

Your Data is Necessary

Providing Your data is not mandatory, but it is necessary for the functionality of the Norton Mobile App. If You do not agree to the collection of the data, Symantec will be unable to provide the Service to You. For example, We require the location data of Your mobile device in order to be able to provide location information back to You when You request it. In addition, We use data from Your mobile device to innovate and develop better products and services to protect You better. We anonymously aggregate information from users and then develop insights to better help Our customers stay protected.

Securing Your Data and Information

We have taken appropriate administrative, technical, organizational, and physical security and risk management measures in accordance with applicable laws to ensure Your Data is adequately protected against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure, or access, use, and all other unlawful forms of processing of Your Data in our possession.

Norton Community Watch

Norton Community Watch (“NCW”) is a product feature that, with Your permission, collects non-personal data from Your device (e.g. selected security and application data), aggregates it with other user’s mobile devices that have joined NCW, and submits the data to Symantec by WiFi network for analysis to identify new threats and their sources. Our backend technology uses sophisticated algorithms to compute a security reputation rating for each file downloaded, installed, or run. NCW data is not cross-referenced or associated with any of Your data. You can join Norton Community Watch by selecting the "Norton Community Watch" checkbox when You install Your Norton product or through the "Anti-Malware" option of Your Norton product. Make sure the "Enable Norton Community Watch" option is turned "On". This setting can be used also to disable Norton Community Watch.

The data includes:

- Hashed version of Your IMEI, which cannot be converted back to Your IMEI nor correlated with any Personal Information;
- System Information such as: Model, Brand, Manufacturer, Product, Build Type; Firmware, Kernel, Baseband, Internal Version, Software Version, Rooted status, hardware features;
- Apps static information that includes: Version Code, Version Name, Activity, Receiver, Service, Permission, signature;
- Apps runtime information: Battery info, CPU info, Network info, Memory info, Size info, Crash info, Call info, SMS info;
- Carrier Information: Network Type, Operator, SIM info, etc.; and/or
- Applications (APKs), which are unknown to Symantec, for threat and reputation analysis.

You can terminate Your participation in NCW from the “Anti-Malware" option Norton product by changing the "Norton Community Watch" option to "Off", or by reinstalling Your Norton product with the "Enable Norton Community Watch" checkbox unselected.

Your Right to Access and Change Your Data

Subject to applicable laws, you have the right to ask us to provide you with information regarding the Personal Information we process about you, to revise Your Data, or to delete your information, to withdraw your consent, or to remove you from any of our mailing lists.

We may retain certain Information if necessary to prevent fraud or future abuse or as otherwise required or permitted by law.

Contact Us

Please contact us at privacyteam@symantec.com if You have any questions.

Changes to the Notice

We reserve the right to revise or modify this Privacy Notice and will note the date of its most recent revision above. If we make significant changes to this Privacy Notice, and where required by applicable law, we will either notify You either by prominently posting a notice of such changes or by directly sending You a notification.

Norton Mobile Security Privacy Notice

This Norton Mobile Security Privacy Notice tells You what information We collect and what We do with it. This policy and the master Norton Mobile Privacy Notice, above, apply to Your use of Norton Mobile Security. You can access features and settings for Norton Mobile Security on Your devices from the website at www.norton.com/mobilesecurity.

Device Information

Information We Collect from Your Mobile Device

- This information may include information such as equipment identifier (e.g. WiFi MAC address or IMEI), subscriber information, mobile phone number, country of origin, device name, device type/manufacturer, operating system type and version, network type, Internet Protocol (“IP”) address, wireless carrier/operator, support case ID, user-installed certificates, the website domain name and its associate SSL certificate chain from device, and a record of Your actions within the Norton Mobile Security product.

- We use this information to provide the most effective Norton Mobile Security service in various locations, devices, connectivity, and situations. We also use this information in the aggregate to improve Our products and services (for more details, please see “How We Use Your Data”).

Network Services

- We may collect information about how You connect to Your network services.
- We use this to 1) determine if You are online when a Norton Mobile Security anti-theft command (Lock, Locate, Scream, Sneak Peek, and Wipe) is sent; and 2) allow You to save on data services by downloading malware and greyware definitions and/or product updates on WiFi connection only.

Contacts

- If You use the call/text blocking or backup functions, We will access or collect the contacts on Your device.
- We use this to 1) allow You to block calls and text messages from specific contacts; and 2) save encrypted copies of Your contacts on Our secure servers that You can retrieve on an authorized device at any time.

Call and SMS Logs

- We access Your call and SMS logs. We do not store this information.
- We use this to allow You to block calls and text messages from Your call and SMS history.

SD Card Contents

- We may access Your SD card contents if there is a SD card available. We do not store these contents. We access the card to 1) scan the SD card for malware; and 2) wipe the personal contents from the card in the device when You execute the Norton Mobile Security Wipe command.

Location

- We may retrieve the location of Your device. We do this by either a GPS transmission from Your device or from a nearby cell tower or WiFi hotspot information. We require the location data of Your mobile device in order to be able to provide location information back to You when You request it. Depending on the service, the Norton Mobile Security App may also provide Your administrator (the account holder) with remote commands to help locate the device if it is lost or stolen, and the location of Your device may be accessed by the administrator for this purpose only. For certain devices, when Your device is reported lost or stolen, the device will be remotely blocked. Alternatively, when Your device is reported lost or stolen, You may also close the Norton Mobile security App at any time. However in this case, Symantec will be unable to provide the service to You.
- We use this information to provide You with the location of Your device when You request it from an authorized device or from the website.
- With your permission, We may store a history of up to the last ten (10) known locations of Your device to allow You to track recent movements of the device, even when the Norton App is not currently in use.

Scanned Apps

- We collect scanned apps that are not currently in Our database of known apps. We only do this when the device is connected to WiFi and connected to a power source to prevent impact to Your battery and Your data plan, if applicable.
- We analyze these apps and add them to Our growing database to ensure that they are safe to use and are free of any malicious or risky features. Once We have completed an analysis of new apps, We scan for them in future releases to You and other Norton mobile customers. This data is maintained in an anonymous, aggregated format.

Information About the Use of Norton Mobile Security on Your Device

- We collect data about the usage of Our product, such as where the application was downloaded from, how often the application is used, and which events were triggered inside the application.
- We use mobile analytics software to analyze this information anonymously and in aggregate format to improve Our products and services.

Web Browsing URLs, History, and Bookmarks

- We may access your web browser history and bookmarks. We do not store this information.
- When You use the Wipe command in the Norton Mobile Security app, We will access Your mobile device web browser history and bookmarks to wipe it from Your device. If the Web Protection feature is enabled, in the Norton Security app, We analyze URLs in Your browsing history to determine if they are unsafe, and We inform You if any URL You are about to visit is unsafe and should be avoided. We also anonymously collect the record of unsafe URLs to improve Our products and services and to better understand current mobile threats.

Calendar

- We may access the calendar. We do not store this information.
- When You use the Norton Mobile Security Wipe command, we will access Your mobile device calendar to wipe it from Your device. We do not store any of these data.

Phone Settings

- We may access Your phone settings. We do not store these settings.
- We use this access to 1) block incoming calls from contacts that You have previously chosen to block; and to 2) modify the audio settings to increase the phone volume if You use the Norton Mobile Security Scream command.

Norton Mobile Utilities Privacy Notice

This Norton Mobile Utilities Privacy Notice tells You what information We collect with Norton Mobile Utilities and what We do with it. This policy and the overall Norton Mobile Privacy Notice apply to Your use of Norton Mobile Utilities.

Device Information

Information We Collect from Your Mobile Device

- This information may include information such as equipment identifier (e.g. WiFi MAC address or IMEI), subscriber information, mobile phone number, country of origin, device name, device type/manufacturer, operating system type and version, network type, Internet Protocol ("IP") address, wireless carrier/operator, and a record of Your actions within the Norton Mobile Utilities product.
- We use this information to provide the most effective Norton Mobile Utilities service in different locations, devices, connectivity, and situation. We also use this information in the aggregate to improve Our products and services (for more details, please see "How We Use Your Data").

Network Services

- We collect information about how You connect to Your network services.
- We use this in order to determine if You are connected via WiFi or through Your Mobile Data Plan. We will collect information on the amount of data sent and received in order to display how much You have used against any data plan You may have. We also use this information in order to determine what items to disable as a part of Our Battery Saver.

Contacts

- We access the contacts list as a part of Your call and SMS log.
- The Plan Tracker feature accesses the contacts list to keep track of Your minutes and SMS used. We do not store any of Your contacts.

Call and SMS Logs

- We access Your call and SMS logs.
- We use this to keep track of the minutes used as well as the number of SMS sent and received. We do not store this information.

SD Card Contents

- We may access Your SD card contents if there is an SD card available.
- We access the card if You choose to 1) make a copy of an Android Install Package in the App Manager feature; 2) move an app to the SD card; 3) list all Android Install packages present on the SD card; or 4) create a copy of Your license if You have the paid version of Norton Mobile Utilities.

Apps on Your Device

- We detect the apps on Your device each time Norton Mobile Utilities performs a scan. If We detect an app that is not currently in Our database of known apps, We may collect it for further analysis. We only collect apps when Your device is connected to WiFi and plugged into a power source to prevent impact to Your battery and data plan. We do not collect any Personal Information or usage data associated with these apps.

- We analyze these apps to check for potential risks to Your privacy and security and to provide You with information about potentially undesirable and harmful applications on Your device as well as remediation options. We also use data about threats anonymously and in aggregate to improve Our products and services and to better understand current mobile threats. Based on Our analysis We will update Our product to protect Your device from malicious apps.
- We list what apps are installed and are running on Your device. We use this to allow You to 1) stop an app from running; 2) uninstall an app; 3) move an app to Your SD card; and to 4) clear the cache of an app.

Norton Mobile Utilities on Your Device

- We collect data about the usage of Our product, such as where the application was downloaded from, how often the application is used, and which events were triggered inside the application.
- We use mobile analytics software to analyze this information anonymously and in aggregate format to improve Our products and services.

Phone Settings

- We may access Your phone settings.
- We use this access to modify the audio settings to change the phone volume and vibrate settings if You use the Norton Mobile Utilities Battery Saver feature. We do not store these settings.

Norton WiFi Privacy Notice

The Norton Mobile Privacy Notice including this Norton WiFi Privacy Notice apply to Your use of Norton WiFi Privacy.

Information We Access or Collect from Your Device may Include:

- Device name, type, OS version, language, location, browser type and version, IP address, anonymous identifier, country where the customer signed-up in based on IP address, device ID status, and identity;
- For iOS devices, We ask for Your consent to alert You with notifications and/or VPN configuration profile;
- For Android devices, when installing the app, We ask for Your consent to make in-app purchases and/or collect WiFi connection information;
- For Android devices, when turning on VPN for the first time, We ask for Your permission to setup a VPN profile;
- Your approximate location based on what network You are using;
- Your network connections and access when You power on Your device; and/or
- Your WiFi connection information.

We May Use Your Information for the Following Purposes:

- For customer support and to provide the services You requested;
- To help with account billing and for production operations and improvements, including real-time analysis of traffic;
- To provide reminders of Your security settings;
- To select the most appropriate server to connect to;
- To provide You proactive reminders to protect the information You are transmitting
- Product usage statistics;
- User device statistics;
- Product ratings provided by users;
- Software configuration, product details, installation status;
- License status, license entitlement information, license ID, and license usage; and
- To improve Our products and services, using data anonymously and in the aggregate.

For more details, please see “How We Use Your Data.”