Norton Mobile Privacy Notice

Effective: December 7, 2015

For over two decades, Symantec and the Norton brand have been entrusted by consumers around the world to protect their computing devices and most important digital assets. We take equally good care of your data. 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 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 Hotspot Privacy Notice

View Norton Wi-Fi Security Privacy Notice

We use your data to provide you with protection and innovation.

We use your data to provide you with the service you requested, to develop better products and services, to protect you better, and, with your permission, to tell you about Symantec products and services that may be of interest to you. We aggregate information from many users and develop insights to better help our customers stay safe.

We do not sell your personal information.

We are not in the business of selling your personal information. In addition, we only share your personal information, registration, mobile device information, backup, or location data with trusted third parties, which operate on our behalf, have accepted our privacy and security terms, and have agreed to operate in compliance with our policies and in accordance with our instructions. 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 employ state-of-the-art technology, processes and procedures to keep your data protected.

Security is our business, and we invest in world-class technologies and solutions to protect the information that you provide to Norton. We store data within our secured data centers and use state-of- the-art encryption whenever it is transmitted. As a leading security provider in the world, we continually work to ensure our web site, products and services are hardened against potential attacks. We are diligent in protecting your digital assets and personal information.

If you join Norton Community Watch you will provide critical security and application data, which helps Symantec to identify new threats.

Norton Community Watch (NCW) collects selected security and application data from your mobile device, aggregates it with other users' mobile devices, which have joined NCW, and submits the data to Symantec by Wi-Fi 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 correlated with any of your personal data.

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 information 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 Wi-Fi hotspot information. 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 backup 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 web site.

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 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.

What we do with your data

The data from your device will be transmitted to Symantec Corporation in the US, where it will be processed to provide you with the Norton mobile service you requested, to enable and optimize the performance of the Norton Mobile App, for internal research and development, including improving Symantec's products and services, for statistical analysis of product deployment, including analysis of trends and comparison in the aggregated install base, and to provide you and others with information about Symantec products and services, as permitted by applicable laws.
The data we collect is stored and associated with the information in your Norton Account unless otherwise noted.

Sharing your data

Symantec does not sell, rent, lease, give away or disseminate your data to any third party, except as necessary to provide you with the functionalities of the Norton Mobile App. We may share your data with partners and vendors that process information on our behalf. Symantec binds these service providers by contract to protect your data. Symantec is a global organization and we may store and process your information with our affiliates located in other countries, including the US and other countries outside the EEA that may have less protective data protection laws than the country in which you are located. For data collected in the European Economic Area (the "EEA"), Symantec has taken steps to ensure that the collected data, if transferred outside of the EEA, receives an adequate level of protection as required by the EEA/Swiss data protection legislations.

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

Symantec has taken all appropriate administrative, technical, physical and procedural security measures, consistent with best-in-class international information security practices, including encrypting your information, in order to protect your personal information. These measures include:

- Physical safeguards, such as locked doors and file cabinets, controlled access to our facilities, and secure destruction of media containing personal data
- Technology safeguards, such as use of Symantec anti-virus and endpoint protection software, encryption, and monitoring of our systems and data centers to ensure compliance with our security policies, and in particular, credit card information is transmitted using secure socket layer (SSL) encryption
- Organizational safeguards, through training and awareness programs on security and privacy, to ensure employees understand the importance and means by which they must protect personal data, as well as through privacy policies and policy standards that govern how Symantec treats personal data.

Norton Community Watch

Norton Community Watch (NCW) is a product feature that, with your permission, collects non personal data from your device. 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
- 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 personal data

According to the laws of your country, you may have the right to access, free of charge, change and delete the data you have provided to us at any time by sending an email to privacy@symantec.com. However, there are exceptions to this right so that access may be denied where we consider that making the information available would reveal personal information about another person or where we are legally prevented from disclosing such information. If we refuse to provide you with access to your personal information, we will provide you with reasons for the refusal.

Contact us

For users located in Europe, Middle East and Africa, Symantec means the Data Controller Symantec Ltd in Ireland. For users in other regions, Symantec means the Data Controller Symantec Corp. in the US. If you have questions, please contact us at: privacyteam@symantec.com or visit http://www.symantec.com/index.jsp to find the Symantec affiliate in your country.

Changes to the Notice

To comply with laws or to conform to the latest business practices, we may change this Notice. Changes will be posted on our website, so please check our pages for updates. The date of the last update will be always indicated at the top of the Notice. If you continue to use the Norton Mobile App after any change or revision to this Notice, this indicates your agreement with the terms of the revised Notice.

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. Wi-Fi 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 Security product.

- We use this information to provide the most effective Norton Mobile Security service in different locations, devices, connectivity, and situation. We also use this information in the aggregate to improve our products and services.

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 to 2) allow you to save on data services, by downloading malware and greyware definitions and/or product updates on Wi-Fi 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 to 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 to 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 Wi-Fi 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.
- When possible, 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.

Scans and scan results

- We collect names of files and applications on your device each time Norton Mobile Security performs a scan.
- We use this 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.

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 Wi-Fi 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.

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 browser history and bookmarks

- We may access your web browser history and bookmarks. We do not store this information.
- When you use the Norton Mobile Security Wipe command we will access your mobile device web browser history and bookmarks to wipe it from your device. We do not store any of these data.

Current web browsing history and URLs

- We may access your web browsing history. We do not store this information.
- If the Web Protection feature is enabled, 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. Wi-Fi 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.

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 Wi-Fi 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 to 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 Wi-Fi 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.

Information about the use of 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 Hotspot Privacy Notice

Privacy Notice

This Privacy Policy tells you what information we collect when you use Norton Hotspot Privacy and what we do with it. This policy and the overall Norton Mobile Privacy Policy apply to your use of Norton Hotspot Privacy. You can access features and settings for Norton Hotspot Privacy on your devices from the website at https://login.hotspot.norton.com/account/

Device Information

- **Information we collect from your device.** This information may include information such as equipment identifier (e.g. Wi-Fi MAC address or UUDID), subscriber information, country of origin, device name, device type/manufacturer, operating system type and version, network type, partial Internet Protocol ($^3IP^2$) address, wireless carrier/operator, and a record of your actions within the Norton Hotspot Privacy product.
- We use this information to provide the most effective Norton Hotspot Privacy service in different locations, devices, connectivity, and situation. We also use this information in the aggregate to improve our products and services.

Network services

- We may collect information about how you connect to your network services (e.g. Gateway and Wi-Fi access point name).
- We use this to determine if you are connected to a known unsafe network.

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 Wi-Fi hotspot information.
- We use this information to select the most appropriate Symantec server to connect to.

Information about the use of Norton Hotspot Privacy 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 analytics software to analyze this information anonymously and in aggregate format to improve our products and services.

Current web browsing history and URLs

- We may access your web browsing history. We do not store this information.
- 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.

Norton Wi-Fi Security Privacy Notice

Privacy Notice

This Privacy Policy tells you what information we collect when you use Norton Wi-Fi Security and what we do with it. This policy and the overall Norton Mobile Privacy Policy apply to your use of Norton Wi-Fi Security.

Device Information

- **Information we collect from your device**. This information may include information such as Device name, type, OS version, language, location, browser type and version, IP address and Device ID status and identity.
- We use this information anonymously and in the aggregate to improve our products and services.

Network and Location

- We may collect your approximate location based on what network you are using.
- We may also view your network connections and access when you power on your device.
- We use this information to select the most appropriate server to connect to.

Wi-Fi Connections

- We may access your Wi-Fi connection information.
- We use this information to provide you with proactive reminders to protect the information you are transmitting.

Information about your use of Norton Wi-Fi Security on your device

- Product usage statistics;
- User device statistics;
- Product ratings provided by users;
- Software configuration, product details, installation status; and
- License status, license entitlement information, license ID and license usage.
- We use this information anonymously and in the aggregate to improve our products and services.