Norton Product and Service Privacy Notice - *Last updated on December 13, 2018*

This Notice is to be read and applies in conjunction with, and in addition to the Symantec - Norton Global Privacy Statement. It describes the categories of data collected by Norton products and services, and the purposes for which those data categories are processed. It is designed to provide mandatory transparency information both to individual Norton users as data subjects and to Small and Medium Business Norton users as data controllers. Please note that data categories marked with an asterisk (*) are personal data transmitted to Symantec for the purpose of delivering the corresponding Norton product features and service functionalities. All other data categories are collected by the Norton software for processing in a non-identifiable form.

All of Norton's Products and Services are held to the high standards as set forth in the Symantec - Norton Global Privacy Statement. Furthermore, to inform you transparently about the unique characteristics and specific purposes of each Norton product and service, in addition to a description of the product or service, this Notice describes the Personal Data we collect and the purposes for which the Personal Data is processed.

If any part or aspect of this Notice is unacceptable to you, then please do not download, install or otherwise use the corresponding Products, Services or their features, and/or please immediately uninstall or stop using any Products, Services or features concerned. For those Product and Service features that require you to provide additional Personal Data to us, or which require you to consent to the processing of such Personal Data as necessary for the purpose of benefitting from specific optional features of a Product or Service, at the time of download, installation, activation or use of said feature, you will be asked to review this Notice so as to be in a position to give your informed and specific consent accordingly.

Contents

Norton App Lock

Product/Service Description	Data Access and Collection	Data Processing
Norton App Lock allows the user to secure and protect mobile applications using a pin, password or pattern to lock. In case the mobile device is lost or stolen, App Lock can also be configured so that, if so equipped, the device's front facing camera takes a picture upon three unsuccessful attempts to unlock the device.	*1. User's email address 2. User's set up PINs, passwords for mobile applications 3. Per user's choice, pictures based on settings	1. The user's email address is collected and transmitted to Symantec to enable the processing of Norton App Lock password recovery and resets. 2. 3. All other data which the product collects from user input is stored on the user's device.

Norton Clean

Product/Service Description	Data Access and Collection	Data Processing
Norton Clean is a storage maximizer, which sweeps the user's mobile device's memory cache to erase ads and unwanted data to free up additional storage space.	Unique Device Identifier (IMEI) of the mobile device	The IMEI number is collected from the device and transmitted to Symantec. Upon transmission the IMEI number is immediately hashed prior to any further processing. The hash is processed for the purpose of monitoring unique usage of the product. Once the data is hashed, it cannot be traced back to the original device, so that neither the user, nor the device itself is tracked or monitored.

Norton Error Management

Product/Service Description	Data Access and Collection	Data Processing
Norton Error Management documents issues which are encountered with the Norton Product. In such cases the user can choose to report errors to Symantec.	1. Computer status information (system language, country locale, and the operating system version) 2. Processes running, their status and performance information 3. Data from files and folders that were open at the time the Norton product encountered the problem	1.-2.-3. System information is processed by Symantec for the purpose of correcting the encountered issue and to improve the performance of the Norton Product. In certain cases, if an error is encountered due to a security threat or vulnerability, Symantec may derive and share certain non-user-specific or non-identifying data with partners of the broader cybersecurity community such as research organizations and other security software vendors. The purpose of such sharing is to promote awareness, detection and prevention of the risk. Symantec may also use statistics derived from such information to track and publish reports on security risk trends.

Norton Community Watch

Product/Service Description	Data Access and Collection	Data Processing
Norton Community Watch allows Norton security product users to help improve the identification and reduce the time to deliver protection against new security threats. The program collects selected security and application data and submits the data to Symantec for analysis to identify new threats and their sources. The program helps build a better, stronger security product by analyzing the data sent from the user. By joining Norton Community Watch program: 1. You participate in building better, stronger knowledge of, and protection against cyber-threats through the data you and other participants submit. Our backend technology uses sophisticated algorithms to compute a security reputation rating for each file downloaded, installed or run on your machine, without however making any determination that would concern you or anyone else personally. Norton security product users get the benefits of this new innovative technology when a Norton product: *a. Blocks harmful downloads with Download Insight. Norton tells you whether your download is known to be safe or unsafe, or if it has an unknown security profile. If the download isn't safe, our products take immediate action to protect you; b. Delivers improved detection rates as well as reducing false positives; *c. Runs faster scans using Norton Insight by clearing more quickly files that were submitted, analyzed and determined as known-good through Norton Community Watch. 2. Providing critical security and application data, you contribute to the intelligence required to identify new threats and to block them before they reach any further. *Norton Insight is only available on Windows OS.	1. Machine ID (data generated by Symantec) 2. Product serial number (data assigned to your product by Symantec) 3. Norton Account Number (data generated by Symantec) *4. File paths *5. Non-executable and portable executable files that are identified as malware 6. URLs of websites visited that the Norton product deems potentially fraudulent 7. The URL of the website that the user most recently visited prior to installation on their computer of a downloaded security risk 8. Information about the processes and applications running on the user's device from time to time, including at the time when a potential security risk is encountered 9. A sample of data sent by the user's device in response to a potential security risk	Norton Community Watch being a service hosted and managed by Symantec on the back-end, all data collected is transmitted to Symantec as follows: 1. Machine ID is needed to track the number of unique devices using a product for each subscription, so as to audit and enforce license rights and entitlements. 2. Product serial number is provided to each user and is used to ensure each product is licensed for use by Symantec. 3. Norton Account Number is needed to track the number of users subscribing to specific Norton products. 4.-5. File paths and non-executable and portable executable files are captured to help identify the origin and logical location of cyber-threats affecting or emanating from the user's device. 6.-7. URLs are used to identify web-based sources of potential security risks, and to improve the ability of Symantec's Products and Services to detect malicious actions, harmful events, fraudulent websites, crime-ware, and other forms of Internet security threats. 8.-9. Device data is used to improve Symantec's knowledge and understanding of cyber-threats. Device data is also processed to provide better protection to users of Symantec Products and Services in the future, and for statistical analysis of cybersecurity trends.

Norton Core

Product/Service Description	Data Access and Collection	Data Processing
Norton Core is a wireless router which provides protection against malware, viruses, hackers and other cyber-threats for devices which are connected to the router.	*1. Wireless network SSID/password (encrypted) 2. Device information, including any Personal Data included by the user when assigning device name(s) and, if provided by the user, the name or alias of the person to whom the device is assigned, and device user agent data/app user agent data, including device type, manufacturer, and model, operating system and IP address 3. Data regarding device usage, including data regarding the time of last device use, internet usage time for each connected device, and gateway logs of network connections 4. Parental control information and settings as defined and configured by the user, including blocked websites, visited websites, and time and content filter information, as well as URLs of websites determined or deemed to be dangerous *5. Personal Data which the user may supply to create a Norton Account, including a username and an optional picture *6. Personal Data provided by the user for customer support and connectivity assistance, such as user ID, name, role, user-specific policies, and device information 7. Cyber-threat telemetry including logs of attempts to download malicious executable files/mobile apps, records of other risky events or actions, and artifacts such as malware samples *8. User contact information, expressed preferences *9. Shipping address and related information 10. Norton Core enables participation in Norton Community Watch	1. Wireless network information is processed for the user-defined configuration of the WiFi Network. 2. Device information is processed for license administration, to analyze the device and its traffic in order to monitor the health and connectivity of the router and to assist in debugging it, to understand product usage and respond to alerts. 3. Device usage data is processed for the purposes of: • Optimizing the performance of Norton Core; • Informing users on site safety; and • Blocking browsing to unsafe websites. 4. Parental control information and settings are used to enforce the rules and policies defined by the user for their controlled profiles, help the user detect any misuse of Personal Data associated with such profiles and to communicate with the user and controlled profiles. 5.-6. User account information is collected by Symantec to fulfil services outlined in the customer contract and provide technical support and assistance. 7. Cyber-threat telemetry is transmitted to Symantec for the purpose of research and development to improve Symantec's products and services and better to protect the user's network, devices, data and identity. 8. User contact information and preferences are transmitted to Symantec for the purposes of: • Guiding the user during the software installation process for Norton Core; • Informing the user of ways to improve user experience; • Tailoring information presented to the user based on the user's preferences (such as language and geographical region); and • Improving customer satisfaction from services provided via owned and third-party call centers. 9. Shipping address and related information is processed to deliver the Norton Core hardware to the user. 10. Regarding Norton Community Watch-related information, please refer to the Norton Community Watch section of this Notice for additional details. Additionally, Symantec will use aggregated, de-identified, anonymized or otherwise non-identifying data derived from collected data such as statistics for the purposes of: • Pursuing general cybersecurity research; • Improving the detection of malware and cyber-threats e.g. through file sample analysis; • Tracking and publishing reports on security and identity theft risks/trends; • Conducting statistical analysis of product deployment, including analysis of trends and comparisons in our aggregated user base; • Monitoring and improving product performance in terms of availability and response times; • Understanding frequency of product-related communications to optimize overall user experience; and • Gaining other non-user-specific business and market insights relevant to improving the performance of our operations.

Norton Mobile Security

Product/Service Description	Data Access and Collection	Data Processing
Norton Mobile Security provides to protected users' and their devices whom the subscriber chooses to protect protection for smartphones and tablets against digital threats, lost or stolen device recovery and contact information restoration	1. Protected users' Mobile device data, including equipment identifiers (e.g. IMEI, WiFi MAC address, UDID), subscriber information, mobile phone number and other protected user contact information, device name/type and manufacturer, operating system type and version, wireless carrier, network type, country of origin, support case ID, user-installed certificates, website domain name and associate SSL certificate chain from device, and IP address 2. Usage data such as download and use frequency information, log data and cookies, and network service information about how the user connects to the network services 3. Names of files and applications on the user's device each time the Product performs a scan, including scanned apps that are not currently in Symantec's database of known apps to protect the user against malware or risky features, as well as Calendar and SD card contents if available 4. Web browsing URLs, history, and bookmarks *5. Per the user's choice, contacts on the user's device, including call and SMS logs 6. Phone call and device audio settings *7. Device location data *8. The product can also be configured so that, if so equipped and when the device is reported lost or stolen, the device's front facing camera takes a picture, when the device continues to be used, where an incorrect password is typed upon one unsuccessful attempt	1. Mobile device data, subscriber information and protected user contact information are processed for the purposes of: • Enabling and optimizing the performance of the Product; • Authenticating the protected user's identity for Symantec; • Guiding the user during the software installation process; • Communicating with the protected user to provide the service; • Performing license administration; and • Improving customer satisfaction from services provided via owned and third-party call centers. 2. Usage data is processed for the purposes of: Understanding product usage and preferences to personalize and improve user experience. 3. File, application names, Calendar (e.g. URLS in invites) and SD Card contents are processed for the purposes of: • Alerting the user of potentially harmful applications; • Scanning the device for malware; and • Wiping personal contents from the device if the user chooses to enable and execute the Product's Wipe command. 4. Browsing data is processed for the purposes of: • Informing users on site safety; • Blocking browsing to unsafe websites; and • Wiping browsing history and bookmarks if the user chooses to use the Product's Web Protection feature or the Wipe command. 5. Contacts including call and SMS logs on the user's device are processed for the purpose of providing the call/text blocking functions if the user chooses to use them. 6. Phone settings are used to block incoming calls from contacts or to modify the device's audio settings if the user chooses to enable and use the Product's blocking feature and/or Scream command. 7. 8. Device location and picture data can be collected at the protected user's request to locate the user's device when the device is lost or stolen. The product may also provide the subscriber with remote commands to help locate the protected user's device if it is lost or stolen. In certain cases, when the device is reported lost or stolen, the device will be remotely locked. Alternatively, when the device is reported lost or stolen, the product may also be closed at any time. With the permission of the protected user, a history of up to the last ten known locations of the device may be stored to allow the protected user to track recent movements of the device, even when the product is not currently in use. 9. Backup data is processed for the purpose of delivering the Product's backup and recovery features if the user chooses to use them.

	to unlock the device, or if the device is turned on after switching it off 9. Backup copy of the data on the mobile device, including contacts, call history, phones and text messages	Additionally, Symantec will use aggregated, de-identified, anonymized or otherwise non-identifying data derived from collected data such as statistics for the purposes of: • Pursuing general cybersecurity research; • Improving the detection of malware and cyber-threats e.g. through file sample analysis; • Tracking and publishing reports on security and identity theft risks/trends; • Conducting statistical analysis of product deployment, including analysis of trends and comparisons in our aggregated user base; • Monitoring and improving product performance in terms of availability and response times; • Understanding frequency of product-related communications to optimize overall user experience; and • Gaining other non-user-specific business and market insights relevant to improving the performance of our operations.

Norton Security Scan

Product/Service Description	Data Access and Collection	Data Processing
Norton Secure Scan provides a scan of the endpoint device or devices selected by the user, will identify potential issues or risks, and will recommend products and solutions to the user.	1. Machine ID (data generated internally by Symantec); Install/uninstall function of the device; device information and device user agent data/app user agent data, including device type, OS version, OS language, manufacturer, and model; operating system; and associated geographic information 2. Telemetry information about files scanned, user experience, and threats found, fixed, and remaining; Date and time of scan after submission; Status information regarding installation and operation, which could include personal data incidentally if in a file path or folder name	1. Machine ID and related information are used by Symantec for the purposes of: • Guiding the user during the software installation process; • Communicating with the user to provide the service; • Understanding service usage and preferences to personalize and improve user experience. 2. Telemetry information is used by Symantec for the purposes of: • Enabling and optimizing the performance of the Service; and • Research and development to improve Symantec's products and services and better to protect the user's network, devices, data and identity. Additionally, Symantec will use aggregated, de-identified, anonymized or otherwise non-identifying data derived from collected data such as statistics for the purposes of: • Pursuing general cybersecurity research; • Improving the detection of malware and cyber-threats e.g. through file sample analysis; • Tracking and publishing reports on security and identity theft risks/trends; • Conducting statistical analysis of product deployment, including analysis of trends and comparisons in our aggregated user base; • Monitoring and improving product performance in terms of availability and response times; • Understanding frequency of product-related communications to optimize overall user experience; and • Gaining other non-user-specific business and market insights relevant to improving the performance of our operations.

Norton Secure Login

Product/Service Description	Data Access and Collection	Data Processing
Norton Secure Login (NSL) is an Identity Provider that delivers a simple, secure and centralized way to authenticate users. Symantec provides an infrastructure for identity management for millions of users across various Norton products.	*1. Personal Data to help authenticate the user's identity, such as home address, phone number, birth date, and/or credit card number; user contact information; any additional Personal Data the user may enter into the user's Norton Account, or which the user may provide for the purposes of customer support and connectivity assistance, such as name and device information 2. Device, product and service information and device user agent data/app user agent data, including device type; manufacturer; model; operating system and version; Device information and device user agent data/app user agent data, including device type; manufacturer; model; operating system and version; runtime performance data; installed applications; associated geographic information, MAC address, and IP address 3. Usage data regarding internet usage, such as URLs and IP addresses of websites visited, search keywords and results, and information on potential security risks (including URLs and IP addresses of websites deemed potentially fraudulent, which may contain Personal Data the website attempts to obtain without the user's permission)	1. Personal Data is processed by Symantec for the purposes of: • Authenticating the user's identity for Symantec or for relying third parties that utilize Norton Security Login; • Issuing an identity credential and/or avoiding fraudulent transactions in the user's name; • Guiding the user during the setup process; • Communicating with the user to provide the service, including Support and Assistance; and • Improving customer satisfaction with services provided via owned and third-party call centers. 2. Device, product and service information is processed by Symantec for the purposes of: • Enabling and optimizing the performance of Products and Services; • Performing license administration; and • Understanding product usage and preferences to personalize and improve user experience. 3. Usage data is processed by Symantec for the purposes of: • Informing users on site safety; • Blocking browsing to unsafe websites; and • Research and development to improve Symantec's products and services and better to protect the user's network, devices, data and identity. Additionally, Symantec will use aggregated, de-identified, anonymized or otherwise non-identifying data derived from collected data such as statistics for the purposes of: • Pursuing general cybersecurity research; • Improving the detection of malware and cyber-threats e.g. through file sample analysis; • Tracking and publishing reports on security and identity theft risks/trends; • Conducting statistical analysis of product deployment, including analysis of trends and comparisons in our aggregated user base; • Monitoring and improving product performance in terms of availability and response times; • Understanding frequency of product-related communications to optimize overall user experience; and • Gaining other non-user-specific business and market insights relevant to improving the performance of our operations.

Norton Ultimate Help-Desk & Norton Computer Tune-Up

Product/Service Description	Data Access and Collection	Data Processing
Norton Ultimate Help Desk allows the user to contact an expert to assist with technical issues ranging from network setup to device diagnostics and troubleshooting. Norton Computer Tune-Up is a feature within Norton Ultimate Help Desk, which helps to keep the user's device running like new, using diagnostics.	*1. The request information you provide to Symantec service representatives over the phone or which you enter into the Symantec online interface when requesting the Norton Services 2. System information including: The type and version of the operating system and browser used on your device; Whether a firewall is active; Whether antivirus software is installed, running, and up to date; Memory and disk space, proxy configuration, and directory listings for the Support Software Tool; Browser information including security and temporary file settings; Active ports, hosts file, and network interface settings on the device; Installed programs and active processes information; Application and operating system log file information and registry data 3. Diagnostics information including: The number of files scanned, threats found and threats fixed by the Support Software Tool; The types of threats found; The security status (good/fair/poor) of the device as determined by the Support Software Tool; The number and type of threats remaining that have not been fixed by the Support Software Tool	1. Request information is processed by Symantec for the purposes of: • Communicating with the user to provide the service; • Understanding product usage and preferences to personalize and improve user experience; and • Improving customer satisfaction with services provided via owned and third-party call centers. 2. System information is processed by Symantec for the purposes of: • Delivering the Services requested by the user; • Enabling and optimizing the performance of the Services; and • Guiding the user during the use of the Services; 3. Diagnostics information is processed by Symantec for the purposes of: • Informing the user of the outcome of the services performed; and • Research and development to improve Symantec's products and services and better to protect the user's network, devices, data and identity. Additionally, Symantec will use aggregated, de-identified, anonymized or otherwise non-identifying data derived from collected data such as statistics for the purposes of: • Pursuing general cybersecurity research; • Improving the detection of malware and cyber-threats e.g. through file sample analysis; • Tracking and publishing reports on security and identity theft risks/trends; • Conducting statistical analysis of product deployment, including analysis of trends and comparisons in our aggregated user base; • Monitoring and improving product performance in terms of availability and response times; • Understanding frequency of product-related communications to optimize overall user experience; and • Gaining other non-user-specific business and market insights relevant to improving the performance of our operations.

Norton Privacy Manager

Product/Service Description	Data Access and Collection	Data Processing
Norton Privacy Manager protects online privacy and limits your digital footprint by providing private communications, anonymized Sudo identities**, and private browsing within the app. Norton Privacy Manager also incorporates subsets of features from Norton Secure VPN and Norton Password Manager (formerly known as Norton Identity Safe). For information about the data collection and use practices of those Norton services, please see their respective privacy notices at www.symantec.com/privacy. **** Norton Privacy Manager allows you to create anonymized Sudo identities, but Symantec customer service personnel and agents will be able to identify you in order to administer your account and provide customer support.**	*1. Communications information related to the use of App functions/features: telephone calls and telephone numbers, emails and email addresses, and texting/messages, including communication metadata and cellular location, city, and country code, and browser usage (bookmarks and history) *2. Log information for email address, IP address, and user account *3. App-related usage data information	1. Communications information is necessary to provide and optimize the functions of the App – i.e. telephone, email, app-to-app or SMS/MMS messaging services and search and web-browsing. For maximum browsing privacy, the Private Browser should be used in conjunction with StartPage as the default search engine. Your use of StartPage is subject to its Privacy Policy which can be viewed here. The default search engine can be changed within the Software settings; however, third-party search engine sites may track Your browsing activity even while using the Private Browser so you should review their respective privacy policies to learn about their data collection and use practices. 2-3. Log data and aggregate usage information is collected to understand app usage and improve the product (e.g. bug fixes).

Norton Secure VPN (formerly Norton WiFi Privacy)

Product/Service Description	Data Access and Collection	Data Processing
Norton Secure VPN protects the user's devices and safeguards the user's data by encrypting the user's information on any internet connection and preserving the user's privacy.	1. Subscriber information and mobile device data, including device name, type, OS version, and language; 2. Aggregate bandwidth usage; 3. Temporary usage data to assist with debugging a problem with the service.	1. Subscriber information and mobile device data are processed by Symantec for the purposes of: • Enabling and optimizing the performance of the Services; • Understanding product usage and preferences to personalize and improve user experience; • Guiding the user during the installation of the software and the use of the Service; • Communicating with the user to provide the service; • Reminding the user to protect the information the user is transmitting; and • Improving customer satisfaction from services provided via owned and third-party call centers. 2. Bandwidth usage data is processed by Symantec for the purposes of billing, network operations, and support. 3. Temporary usage data is processed by Symantec for the purposes of: • Selecting the most appropriate server to connect to; and • Research and development to improve Symantec's products and services and better to protect the user's network, devices, data and identity. During the use of Norton Secure VPN, we route the user's internet traffic through Symantec's network, which is a "No Log" network. This means that Symantec does not store the user's originating IP address when connected to Norton Secure VPN and therefore Symantec cannot identify individuals. Symantec's automated rule-based traffic management may require real-time analysis of internet data traffic, including destination websites or IP addresses and originating IP addresses, though no log is maintained regarding this information. Symantec does not store information about the applications, services, or websites which the user downloads, uses, or visits. Since Symantec manages a global network, the user's internet traffic may be routed through one or more different countries as explained in the Symantec - Norton Global Privacy Statement. Additionally, Symantec will use aggregated, de-identified, anonymized or otherwise non-identifying data derived from collected data such as statistics for the purposes of: • Pursuing general cybersecurity research; • Improving the detection of malware and cyber-threats e.g. through file sample analysis; • Tracking and publishing reports on security and identity theft risks/trends; • Conducting statistical analysis of product deployment, including analysis of trends and comparisons in our aggregated user base; • Monitoring and improving product performance in terms of availability and response times; • Understanding frequency of product-related communications to optimize overall user experience; and • Gaining other non-user-specific business and market insights relevant to improving the performance of our operations.

Norton Security Products (Security, Internet Security, One, Antivirus & 360)

This section covers Norton Security (Standard, Deluxe and Premium), Norton Internet Security, Norton One, Norton Antivirus, Norton Antivirus Basic, Norton 360, Norton 360PE and Norton 360MD.

Product/Service Description	Data Access and Collection	Data Processing
Norton Security Products provide endpoint security which defends against ransomware, viruses, spyware, malware and other online threats.	1. Subscriber information and device data, including *Personal Data the user may enter to create a Norton Account such as a username and an optional picture; Any *Personal Data which the user includes when assigning device name(s) and, if provided, the name or alias of the person to whom the device is assigned, and device user agent data/app user agent data, including device type, manufacturer, and model; operating system and version; applications and versions; associated geographic information, MAC address, Machine ID, and IP address; Status information regarding installation and operation, which could include Personal Data incidentally if in a file or folder name; Any additional Personal Data which the user provides to Symantec for customer support and connectivity assistance, such as userID, name, role, policies, and device information 2. Data regarding internet usage, such as URLs and IP addresses of websites visited, search keywords and results, and information on potential security risks (including URLs and IP addresses of websites deemed potentially fraudulent, which may contain Personal Data the website attempts to obtain without the user's permission) 3. Data regarding device usage and diagnostics, including: Data regarding the time of last device use, internet usage time for each connected device, and gateway logs detailing network connection activities; Executable files identified as potential malware, which could include Personal Data obtained by the malware without the user's permission; Email messages sent to Symantec with the user's permission reported as spam or incorrectly identified as spam; "Crash dump" information, or information contained in a report which the user may choose to send to Symantec when the Products and Services encounter a problem, which may include system language, country locale, operating system, and processes/files running at the time of error 4. Parental control information and settings as defined and configured by the user, including blocked websites, visited websites, and time and content filter information, as well as URLs of websites determined or deemed to be dangerous.	1. Subscriber information and device data are processed by Symantec for the purposes of: • Enabling and optimizing the performance of the Products and Services; • Authenticating the user's identity for Symantec; • Understanding product usage and preferences to personalize and improve user experience; • Guiding the user during the software installation process; • Communicating with the user to provide the service; • Performing license administration; and • Improving customer satisfaction from services provided via owned and third-party call centers. 2. Internet usage data is processed for the purposes of: • Informing the user on site safety; and • Blocking browsing to unsafe websites. 3. Device usage and diagnostics data are processed by Symantec for the purposes of: • Understanding product usage; • Delivering the protection features of Products and Services; and • Research and development to improve Symantec's products and services and better to protect the user's network, devices, data and identity. 4. Parental control information and settings are used to enforce the rules and policies defined by the user for their controlled profiles, help the user detect any misuse of Personal Data associated with such profiles and communicate with the user and controlled profiles. Additionally, Symantec will use aggregated, de-identified, anonymized or otherwise non-identifying data derived from collected data such as statistics for the purposes of: • Pursuing general cybersecurity research; • Improving the detection of malware and cyber-threats e.g. through file sample analysis; • Tracking and publishing reports on security and identity theft risks/trends; • Conducting statistical analysis of product deployment, including analysis of trends and comparisons in our aggregated user base; • Monitoring and improving product performance in terms of availability and response times; • Understanding frequency of product-related communications to optimize overall user experience; and • Gaining other non-user-specific business and market insights relevant to improving the performance of our operations.

Norton Safe Search, Norton Home Page, Norton Safe Web

Product/Service Description	Data Access and Collection	Data Processing
Norton Safe Search is a search engine website that helps protect the user from unsafe websites by filtering search results and providing website safety ratings to the user to provide a safer web browsing experience. It is also a browser extension that provides access to the Norton Safe Search website in various means. Different versions of this extension can on the user's choice either: a) override the browser's default search engine to the Norton Safe Search website or; b) override the browser's default search engine setting to the Norton Safe Search website AND override the browser's default homepage + new tab settings to the Norton Home Page. Norton Home Page is a browser extension and default homepage enabling the Norton Safe Search website. Norton Safe Web is a browser extension that the user chooses to use in order to monitor browsing activity and web page content. It uses reputation services and web page content analysis to help protect the user from malicious website content, phishing, and other threats.	1. Subscriber information and device and software data, including: Web browser name, version and preferred language; Operating system, version or platform; User device IP address 2. Service usage data including: Web links in social media and webmail; Website browsing activity; Web search terms; Default inputs in different search boxes managed by the Norton products; Search engine results 3. Cookies, pixel tags, scripts or similar technologies placed on the computer or device by the Norton Safe Search website and Norton Home Page website	1. Subscriber information and device and software data are processed by Symantec for the purposes of: • Enabling and optimizing the performance of the Service; • Performing license administration; • Understanding product usage and preferences to personalize and improve user experience; • Guiding the user during the software installation process; • Delivering Product and Service enhancements, better to protect the user, the user's network, device, data, and identity; and • Improving customer satisfaction from services provided via owned and third-party call centers. 2. Service usage data is processed by Symantec and on behalf of Symantec for the purposes of: • Informing the user on site safety; • Blocking browsing to unsafe websites; and • Analyzing Service usage. The user's search query requests made through our Norton Safe Search product will be directed to our Third-Party Search Partners Oath/Yahoo! (for US and Canada) and IACI (for non-US/Canada) in order for the query research to be delivered to you. . Our Third-Party Partners may also collect information directly from you pursuant to your activity on Norton Safe Search. Our Third Party Partners will collect such data as data controllers for the purpose of processing your search query. Such collection of data is governed by the Privacy Policy, Statement and Notice of the Third Party Partners. In order for the Norton Safe Search to be delivered to you, your search query request will be directed to our Third Party Partner (i.e., not a Symantec company), where such Third Party Partner will process your request. The Third Party Partner may also collect information directly from you through your activity on Norton Safe Search (collectively, "Third Party Data"). The Third Party Partner will be the data controller for the purpose of processing your search query, Therefore, it is our Third Party Partner, rather than Symantec, who decides how your Third Party Data will be collected, used, disclosed, retained, or otherwise processed. Your Third Party Data is subject to the Third Party Partner's privacy statement(s) for the processing of your data to carry out the search query. Please refer to the privacy statements of our Third Party Partner. 3. Cookies and similar trackers are processed for the purpose of following feature usage preferences and history. For more information about cookies, please refer to the section above titled, "Tracking Technologies, Cookies and Do-Not-Track" section of the Symantec - Norton Global Privacy Statement. Anonymized IP addresses and product usage information are processed by Google Analytics' Measurement Protocol for the purpose of critical error statistical analysis and management. Click here for information about Google Analytics data safeguards. Additionally, Symantec will use aggregated, de-identified, anonymized or otherwise non-identifying data derived from collected data such as statistics for the purposes of: • Pursuing general cybersecurity research; • Improving the detection of malware and cyber-threats e.g. through file sample analysis; • Tracking and publishing reports on security and identity theft risks/trends; • Conducting statistical analysis of product deployment, including analysis of trends and comparisons in our aggregated user base; and • Monitoring and improving product performance in terms of availability and response times.

Norton Security Toolbar

Product/Service Description	Data Access and Collection	Data Processing
Norton Security Toolbar has two variants, a) an add-on to Microsoft Internet Explorer and b) a browser extension for Google Chrome. Both variants are used by the user to monitor the user's browsing activity and web page content. They use reputation services and web page content analysis to help protect the user from malicious website content, phishing, and other threats. The Internet Explorer variant allows access and use of Norton Identity Safe vault information within the browser user interface. It also provides a search box to perform searches on the Norton Safe Search website. The Google Chrome variant provides a search box to perform searches on the Norton Safe Search website.	1. Device and software data, including: Web browser name, version and preferred language; Operating system, version or platform; User device IP address 2. Product usage data including: Website browsing activity; Limited website browsing history; Web search terms; Default inputs in different search boxes managed by the Norton products; Search engine results 3. Cookies, pixel tags, scripts or similar technologies placed on the computer or device by the Norton Safe Search website and Norton Home Page website	1. Device and software data are processed by Symantec for the purposes of: • Enabling and optimizing the performance of the Service; • Performing license administration; • Understanding product usage and preferences to personalize and improve user experience; • Guiding the user during the software installation process; • Delivering Product and Service enhancements, better to protect the user, the user's network, device, data, and identity; and • Improving customer satisfaction from services provided via owned and third-party call centers. 2. Product usage data is processed by Symantec and on behalf of Symantec for the purposes of: • Informing the user on site safety; • Blocking browsing to unsafe websites; and • Analyzing Service usage. 3. Cookies and similar trackers are processed for the purpose of following feature usage preferences and history. For more information about cookies, please refer to the section above titled, "Tracking Technologies, Cookies and Do-Not-Track" section of the Symantec - Norton Global Privacy Statement. Additionally, Symantec will use aggregated, de-identified, anonymized or otherwise non-identifying data derived from collected data such as statistics for the purposes of: • Pursuing general cybersecurity research; • Improving the detection of malware and cyber-threats e.g. through file sample analysis; • Tracking and publishing reports on security and identity theft risks/trends; • Conducting statistical analysis of product deployment, including analysis of trends and comparisons in our aggregated user base; and • Monitoring and improving product performance in terms of availability and response times.

Norton Identity Safe

Product/Service Description	Data Access and Collection	Data Processing
Norton Identity Safe has two variants: a) a component of Norton Security and b) browser extensions for all major browsers except Internet Explorer. All variants are a password manager which manages usernames, passwords, and other information useful for performing online activities.	1. Subscriber information and device and software data, including: Web browser name, version and preferred language; Operating system, version or platform; User device IP address; *Other Personal Data disclosed by the user, which may include usernames, passwords, websites addresses, physical addresses, payment account numbers, expiry information and free form text 2. Service usage data including: Website browsing activity; Web search terms; Default inputs in different search boxes managed by the Norton products; Search engine results	1. Device and software data are processed by Symantec for the purposes of: • Enabling and optimizing the performance of the Service; • Performing license administration; • Understanding product usage and preferences to personalize and improve user experience; • Guiding the user during the software installation process; • Delivering Product and Service enhancements, better to protect the user, the user's network, device, data, and identity; and • Improving customer satisfaction from services provided via owned and third-party call centers. 2. Product usage data is processed by Symantec and on behalf of Symantec for the purposes of: • Informing the user on site safety; • Blocking browsing to unsafe websites; and • Analyzing Service usage. Anonymized IP addresses and product usage information are processed by Google Analytics' Measurement Protocol for the purpose of critical error statistical analysis and management. Click here for information about Google Analytics data safeguards. Additionally, Symantec will use aggregated, de-identified, anonymized or otherwise non-identifying data derived from collected data such as statistics for the purposes of: • Pursuing general cybersecurity research; • Improving the detection of malware and cyber-threats e.g. through file sample analysis; • Tracking and publishing reports on security and identity theft risks/trends; • Conducting statistical analysis of product deployment, including analysis of trends and comparisons in our aggregated user base; and • Monitoring and improving product performance in terms of availability and response times.

Norton Family Premier

Product/Service Description	Data Access and Collection	Data Processing
Norton Family Premier helps protect protected users and their devices whom the subscriber chooses to protect with parental controls applied through subscriber-defined and subscriber-managed protection settings and features. For additional details about Norton Family Premier, please refer to the section below labeled “Norton Family Premier Additional Information”	*1. Subscriber information such as: Administrator contact information including, but not limited to the subscriber’s name, email address, and password to protect the subscriber’s account; Personal Data provided by the subscriber during configuration of the Service or any other subsequent service call; 2. Device and software data including: Installation status of the Norton Family client software on subscriber or protected user device; Software configuration, product details and installation status; License status, license entitlement information, license ID and license usage; Device name, type, OS version, language, location (Global Position System, GPS), browser type and version; Device hardware, software and application inventory; Application and database access configurations, policy requirements and policy compliance status, and application exception and workflow failure logs; *3. Protected user information which the subscriber chooses to disclose to Symantec, including: Name, gender, age and year of birth; Avatar images; The last six digits of official identification numbers related to the protected user (e.g. where available: Social Security Number, national identification number), e-mail address, mobile phone number, school name or any other information which the subscriber would like to protect; Machine login account details, country and time zone; 4. Protected user networking activity information which the subscriber instructs Symantec to monitor, including per the subscriber’s sovereign choice: Online and mobile device activities and locations; websites that the protected user tries to visit and those that the Product blocks the protected user from visiting; Online search terms that the protected user uses; Applications which the protected user installs or uninstalls on their device, if the subscriber has activated application monitoring; The protected user’s device usage time; *the protected user’s profile name, profile URL, age, Facebook profile ID and videos visited; Videos the protected user watches on YouTube.com and/or from Hulu if the subscriber has activated video monitoring.	1. Subscriber information is processed by Symantec for the purposes of: • Enabling and optimizing the performance of Norton Family; • Providing support or debugging assistance; • Sending to the subscriber promotional information, in accordance with the subscriber’s permission or as otherwise permitted by applicable law; and • Setting up the subscriber’s Norton Account. 2. Device and software data are processed by Symantec for the purposes of: • Ensuring the proper functioning of the Product and delivering the Services requested by the subscriber; • Performing license administration; • Evaluating and improving the Product’s installation success rate; • Research and development to improve Symantec’s products and services and better to protect the subscriber’s and protected users’ network, devices, data and identity; 3. Protected user information is processed for the purposes of: • Identifying and authenticating the subscriber and the protected user to Symantec; • Helping the subscriber detect any misuse of the protected user’s Personal Data; and • Communicating with the subscriber, and per the subscriber’s permission, with the protected user to provide the Service. 4. Protected user activity information is processed for the purposes of: • Helping the subscriber to supervise the online activities of the protected user’s device; • Limiting damage done by installed malware; • Helping to enforce subscriber-defined rules on online activities of the protected user’s device; • Enabling the subscriber to detect if the protected user is exposed to threats via online or SMS/MMS communications; and • Helping the subscriber to safeguard the protected user from such threats. Additionally, Symantec will use aggregated, de-identified, anonymized or otherwise non-identifying data derived from collected data such as statistics for the purposes of: • Pursuing general cybersecurity research; • Improving the detection of malware and cyber-threats e.g. through file sample analysis; • Tracking and publishing reports on security and identity theft risks/trends; and • Conducting statistical analysis of product deployment, including analysis of trends and comparisons in our aggregated user base.

Norton Family Premier Additional Information

If the subscriber chooses to activate the service, Norton Family will not allow the protected user to make their Personal Data public.

Where and to the extent permitted by the laws applicable in the country or region where the subscriber is located, Symantec may provide a **Text Message Supervision** service that enables to subscriber to block or monitor text ("SMS") and multimedia ("MMS") messages delivered to and from the protected user's mobile phone as well as a **Location Monitoring service**. Monitoring SMS and MMS exchanges and/or location and the use of any record of such monitoring may be restricted or prohibited by local laws applicable to the subscriber. The subscriber should by all means inquire with local authorities before activating this feature.

When the subscriber enables the Location Monitoring service, Norton Family will perform the subscriber's instruction to use GPS to track and collect the geolocation of the mobile device designated by the subscriber. The subscriber's consent, and as the case may be, the consent of the user of the mobile device, or the consent of the holder of parental responsibility for such a user is required for Norton Family to track, collect, use, or disclose the designated device's geolocation. The relevant consent or consents are collected through the Norton online portal, or and as the case may be in the product and confirmed when the subscriber enters their payment card information to purchase this Service with Symantec online. You may revoke any consent you have given at any time. For more information on how to do so, please see the "Your Privacy Rights" section of the Symantec - Norton Global Privacy Statement. After termination of the Service, the subscriber's account information relating to this Service will be deleted.

Once the subscriber downloads the application on the designated mobile device, Symantec may collect the geolocation of that device even when the application is not in use. We will only disclose such geolocation information to the subscriber, so that the subscriber can locate the device, and we will only process it for the operational purposes of delivering the services and functionalities requested by the subscriber. The subscriber may not use the Product's Location Supervision service to monitor the data, location, activities or any other aspects related to any individual for whom the subscriber does not hold parental responsibility. Subscribers in the European Economic Area should talk with protected users under their parental responsibility, especially if they are above 13 years of age, and take all necessary measures to ensure that the protected user concerned understands what the subscriber's use of the Product and associated Services entail. When electing to use the Product and associated Services, the subscriber is solely responsible for abiding by all laws and regulations applicable to the subscriber's relations with, and parental responsibility over the protected user.

Text Message Supervision

By default, Text Message Supervision is turned off. The subscriber must separately turn on the Text Message Supervision feature and install Norton Family onto the mobile device designated for such supervision. When activated, the Text Message Supervision collects the following information from the designated device:

- The mobile phone number of the device being monitored and the mobile phone numbers of other devices with whom the device exchanges SMS and MMS communications;
- The content of the SMS messages received or sent by the designated device (for MMS exchanges, Symantec will not record or capture any multi-media content exchanged, only the fact that an MMS exchange occurred);
- If available, the address book name associated on the designated device with the mobile number which sends SMS and MMS communications to the designated device, or receives such communications from it;
- The date/time stamp of the conversation;
- The location of the designated device;
- An event log of blocked SMS/MMS messages, including phone numbers of the parties, and associated names if any are available in the address book of the designated device.

Before starting to monitor SMS or MMS messages that a mobile device designated by the subscriber sends and/or receives, Symantec will send an SMS alert to the designated device, alerting the user of the device that the Product is about to execute the instruction of the subscriber to record and monitor the content of the SMS or MMS messages that are exchanged on the designated device. If, after receiving this SMS alert, the exchange of SMS or MMS messages continues on the designated device, the recording and monitoring of the messaging for the purposes described in this Notice will commence as per the subscriber's instructions. Symantec will reiterate the same SMS alert to the designated device once a month, or every time there is a new conversation.

If the subscriber chooses to block all SMS or MMS messages or messages with a specific counterpart, we alert the user of the designated device and send a text message to the counterpart indicating that messaging is blocked and that the message cannot be delivered.