Introduction, Objectives and Scope

VerSprite was asked to conduct a Technical Privacy Impact Assessment (TPIA) on behalf of Norton VPN. The test took place between June 9th, 2025, and June 27th, 2025, with the consent and full knowledge of Norton VPN officials. Before conducting the Technical Privacy Impact Assessment, a formal kick-off conference call was established to ensure that all members, from both VerSprite and Norton VPN, were adequately informed of the risks, level of effort, points of contact, and expected duration of the assessment.

An update to the original report was introduced to include the review of additional server instances performed between July 29th, 2025, and July 31st, 2025. The final report was delivered on July 31st, 2025. A validation retest was performed between August 25th, 2025, and August 26th, 2025, and this report was updated accordingly to reflect the results and current status of the original observations.

Considering that the technical gaps and security observations reported from the initial exercise were found as Remediated during the validation retest instance, the overall Privacy Impact Score for the ***Norton VPN Solution*** is ***None.***

This Score ranks the Privacy Impact as either *None*, *Low*, *Medium* or *High*, taking into consideration the number of Critical, High, Medium, and Low-Risk security issues and observations as well as the technical gaps in relation to the Privacy Policies found across all phases of the assessment that had an impact on the privacy of Norton VPN's final users. Furthermore, the Score reflects the likelihood of exposure and the overall business impact based upon VerSprite assessment of the criticality of the assets and data at risk.

Objectives

The main objective of this TPIA for Norton VPN was to comprehensively evaluate the service's privacy practices, identify potential risks, and take steps to improve privacy protection for users while ensuring compliance with relevant privacy regulations.

Scope

This engagement was focused on conducting a Privacy Impact Assessment, which is technical in nature and encompassed the following discovery efforts:

Backend Infrastructure Assessment

Infrastructure Traffic/Data Analysis

- Captured and analyzed VPN traffic from multiple backend infrastructure nodes that handle data communications upstream from VPN client software.
- Evaluated relevant network infrastructure components, including routers, core switches, firewalls, forward proxies, web application firewalls (WAFs), caching servers, and load balancers. This involved sampling live packet captures and reviewing infrastructure logs.
- Examined VPN traffic reaching application servers supporting VPN client sessions to assess data flow, data types, and potential privacy impacts.
- Identified any stored data related to VPN traffic within infrastructure data stores, including file systems, relational databases, and non-relational databases.

Server-Side Data Assessment

- Reviewed servers within the VPN backend infrastructure to evaluate static data retention related to client connections, user information, geo-IP data, or other potentially personally identifiable information (PII).
- Focused on backend infrastructure assets such as file servers, relational databases, and non-relational databases to assess data storage practices and associated privacy risks.

Retention and Anonymization Review

- Evaluated technical data retention policies related to VPN service data stored within backend infrastructure.
- Assessed whether any retained PII was anonymized or otherwise handled in a privacy-compliant manner.

Scope Limitations

- The assessment was strictly limited to the backend infrastructure supporting the VPN service.
- Client-side testing (e.g., Windows, Mac, iOS, Android) was excluded from the assessment.
- No performance testing, security penetration testing, or assessments of non-VPN services or applications were included.

If any data was found that could be associated with user connections, then an evaluation of retention policies that are applied at a technical level was performed to see how they affect the retention of data that is knowingly or unknowingly stored within the company infrastructure. Likewise, if sensitive data (such as Personal Identifiable Information) was found to be stored, an evaluation aimed to determine how the data is preserved and anonymized by the VPN solution was also performed.

Methodology

VerSprite started this TPIA by updating their understanding of the Norton VPN technology, the associated infrastructure, and the key components of the solution where user behavior might be logged. As part of this initial phase, VerSprite also reviewed some recent minor changes in the infrastructure. As a result of this process, the Edge servers were identified as the primary components to review, along with the server deployment scripts developed for this purpose.

Norton VPN's updated Privacy Policies applicable to the Norton VPN solution were also studied during this initial discovery phase, and additional internal documents that were provided by Norton VPN employees were also reviewed to understand their purpose, the data categorization, the log retention and rotation policies that had been set for the whole solution.

Moving forward, VerSprite analyzed the main components of the VPN solution. The first phase consisted of the review of the server deployment scripts developed by Norton VPN. These scripts showed us in a very straightforward manner how the Edge servers were set up, what applications and scripts were installed and what configuration changes were made to them.

Next, VerSprite performed a review of a set of live Edge sample servers. For this purpose, Norton VPN provided access to servers in the staging environment that were created using the same scripts that were previously reviewed. In these servers, the running processes and scheduled tasks were identified to discover the main components that were running on them. The settings for these components were analyzed alongside, and the log files that they created were identified as well.

With all this information at hand, VerSprite proceeded to examine the log retention policies in place, as well as the mechanisms designed to prevent the unintended storage of user information. Concurrently, VerSprite intercepted network traffic to gain a clear understanding of any additional external components that the backend servers interact with.

Finally, VerSprite analyzed a set of production Edge servers to ensure that the components, configurations, and log file policies were consistent with those observed in the sample servers from the staging environment.

Overall Findings

VerSprite's initial assessment identified two potential privacy concerns. While individual VPN users could not generally be directly identified from the observed log information, in some cases the stored data may reveal details about accessed resources and VPN client usage patterns. In one Edge server role, VerSprite found that, under specific error conditions, the VPN client's IP address could be logged. In the rare event that this condition overlaps with the first, it may be possible to correlate the data in a way that could identify the user and their associated traffic, thereby impacting privacy. It is important to note that these log entries were subject to the established log rotation policy, which is aligned with the Norton VPN Privacy Policy.

During the validation retest performed on August 25th, 2025, and August 26th, 2025, VerSprite could confirm that changes were implemented to successfully address these identified gaps.

Conclusions

As a result of these efforts, VerSprite confirmed that user behavior data is handled consistently with Norton VPN's Privacy Policies across all analyzed components of the solution. Although certain technical gaps and issues were initially identified, they were later found Remediated, thus the overall privacy impact of the ***Norton VPN*** solution is assessed to be ***None***.