Introduction, Objectives and Scope

VerSprite was asked to conduct a Technical Privacy Impact Assessment on behalf of GenDigital. The test took place between February 21st, 2024 and March 8th, 2024 with the consent and full knowledge of GenDigital 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 GenDigital, were adequately informed of the risks, level of effort, points of contact, and expected duration of the assessment. After the initial assessment, a first validation retest was performed on April 11th, 2024 followed by a second iteration on July 25th, 2024. From the results obtained during the validation retest, the final report was updated to reflect the current status of the original observations.

The main objective of this Technical Privacy Impact Assessment (TPIA) against 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.

Some specific objectives of this TPIA on Norton VPN were:

1. **Identify Privacy Risks**: The assessment seeks to identify potential privacy risks within the Norton VPN service. This includes examining how user data is collected, transmitted, stored, and used within the service to pinpoint areas where privacy vulnerabilities or issues may exist.
2. **Evaluate Data Protection Measures**: It assesses the effectiveness of data protection measures in place, such as encryption protocols, data retention policies, and access controls. The goal is to ensure that user data is adequately safeguarded against unauthorized access or disclosure.
3. **Ensure Compliance**: The TPIA ensures that Norton VPN complies with its stated privacy policies and relevant data protection regulations. It assesses whether the service is following its own privacy commitments and legal requirements.
4. **Assess Data Handling Practices**: The assessment examines how user data is handled throughout its lifecycle, from collection to deletion. This includes evaluating the transparency of data handling practices and user consent mechanisms.
5. **Identify Areas for Improvement**: It identifies areas where the Norton VPN service can improve its privacy practices. This involves recommending enhancements to privacy policies, security measures, or user education regarding privacy settings.
6. **Enhance User Trust**: By conducting a TPIA and demonstrating a commitment to protecting user privacy, Norton VPN can enhance user trust. Users are more likely to trust a VPN service that has undergone a thorough assessment of its privacy practices.
7. **Prepare for Regulatory Compliance**: Assessing and addressing privacy issues proactively can help Norton VPN prepare for regulatory compliance. Compliance with data protection laws is crucial to avoid legal consequences and fines.
8. **Enhance Reputation**: A successful TPIA can enhance Norton VPN's reputation as a privacy conscious service provider, attracting more users who value strong privacy protections.

This engagement was focused on conducting a Privacy Impact Assessment that is technical in nature and encompassing of the following efforts:

1. **Infrastructure-Side Traffic/ Data Analysis**: Capture VPN traffic from the multiple nodes of infrastructure that receive data communications, upstream from VPN client software.
    - VPN traffic via network infrastructure equipment (Routers, Core Switches, Firewalls) and namely the analysis would take place via sampling of live packet captures as well as infrastructure logs.
    - VPN traffic via other infrastructure such as forward proxies, WAFs, caching servers, load balancers via sampling of live packet captures as well as logs.
    - VPN traffic that is connecting to application servers that may be responsible for supporting any aspect of VPN client sessions. Examination of the level of data and the type of data that is captured will be examined.
    - VPN traffic and/ or any associated type of data that is stored for example on filesystems, relational database, non-relational databases, etc.

2. **Server-Side Data Assessment**: Review servers that are within the scope of the infrastructure supporting the overall VPN solution and analyze for static retention of VPN client connections, user information, geo-IP information or other pieces of information that could be considered as personal identifiable information. Infrastructure assets that will be evaluated as part of this phase of the engagement model include file servers, relational databases, non-relational databases, etc.

3. **Retention:** If there is data that could be associated with user connections, an evaluation on retention policies that are applied at a technical level will be evaluated to see how they are affected the retention of data that is knowingly/ unknowingly stored within the company infrastructure.

4. **Anonymization:** If data (personal identifiable information) is found to be stored, an evaluation to see how the data is preserved and anonymized will be collected by the VPN solution.

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 (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 performed.

It is important to note that there are not client side components in scope for this exercise, such as any VPN client.

Overall Findings

The overall privacy impact for the ***Norton Secure VPN Solution***, based on technical gaps found during the Technical Privacy Impact Assessment and the potential impact of discovered issues, is ***Low.*** This score takes into consideration the number of Critical, High, Medium, and Low Risk issues as well as technical gaps and security observations in relation to the Privacy Policies found across all phases of the assessment that had an impact on the privacy of the VPN final user.

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. While VerSprite assessment regarding business impact is based on experience interacting with entities across major enterprises, Gen Digital may adjust the severity levels as needed when prioritizing their remediation efforts.

VerSprite started this Technical Privacy Impact Assessment by familiarizing with the Norton VPN technology, the infrastructure involved and the identification of the main components of the solution in which the user behavior might be logged. As a result of this process, VerSprite identified the Edge servers as the primary components to review during this process along with the server deployment scripts developed for this purpose.

Gen Digital's Privacy Policies applicable to Norton VPN were reviewed based on publicly available information and additional documents that were provided by Gen Digital employees to understand its definition, 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 in a very straightforward manner how the Edge servers were set up, what applications and scripts were installed and what configuration changes were in place.

Next, VerSprite performed a review of a set of live Edge sample servers. For this purpose, Gen Digital provided access to servers in a staging environment that were created using the same Puppet 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 that information at hand, VerSprite started looking into the log retention policies implemented and the different mechanisms in place to avoid any unintended storage of user information. In the meantime, the network traffic was also intercepted and meticulously reviewed to get a clear understanding of any additional external component which the backend servers interact with.

Finally, VerSprite analyzed a set of production Edge servers to ensure the components, configurations and log file policies were followed in a similar fashion as the ones observed in the sample servers of the staging environment.

During this section of the assessment, in contrast with the staging environment, users were connected to the VPN solution of the reviewed Edge servers. The usage and traffic generated by the VPN clients generated log messages that were also reviewed. At this stage, VerSprite identified two potential privacy concerns. Although individual VPN users could not be directly identified from the observed log information, under certain conditions sensitive information could be logged which would certainly assist in identifying the VPN users.

During the validation retests performed on April 11th, 2024 and July 25th, 2024, VerSprite confirmed that changes were made to take care of the security observations mentioned above, and that the reported sensitive information was not being logged anymore.

As a result of this process, we found that there is a consistent way to handle information related to the user behavior while using the Norton VPN product among all the analyzed components of the solution and that it behaves in accordance with public privacy notice information.