PIQUE SOLUTIONS

Privacy and GDPR Compliance: Windows 10 versus macOS High Sierra and iOS 11

Comparison of Privacy Policies and Capabilities and Compliance with the GDPR

PIQUE SOLUTIONS

April 2018

THE DEVELOPMENT OF THIS WHITE PAPER WAS SPONSORED BY MICROSOFT. THE UNDERLYING RESEARCH AND ANALYSIS WERE EXECUTED INDEPENDENTLY BY PIQUE SOLUTIONS.

Contents

Pique Solutions is a competitive research and market analysis firm supporting Fortune-500 companies in the information technology sector. Pique is based in San Francisco, California.

Executive Summary

Pique Solutions conducted a comparative analysis of the level of privacy, transparency, and compliance provided by Microsoft Windows 10 and Apple macOS High Sierra and iOS as it relates to the European Union's General Data Protection Regulation (GDPR), effective as of May 2018.

Based on a side-by-side comparison of features, functionality, and policies related to each platform, we found that Microsoft's privacy terms are more transparent than those of Apple. Microsoft also provides a more unified and comprehensive approach to managing and ensuring user privacy, with a more effective and easier-to-use set of controls, in comparison to Apple.

In the enterprise, privacy and compliance impact both personal and corporate data. Software and service providers have become large consumers of personally identifiable information (PII) including consumer habits. The type of data collected extends beyond PII to also include information such as location, application usage, associations, interests, and in some cases even records of personal conversations.

To address the needs for privacy and compliance in the enterprise, Microsoft has taken the approach of providing transparency and information control within Windows 10 with tools that allow administrators to control privacy settings enterprise-wide. In contrast, macOS and iOS lack a centralized method to allow enterprises control of the level of information shared across Apple devices. This means that enterprises must manage privacy settings for macOS and iOS on a per-device basis. Because managing privacy on a per-device basis is simply unrealistic, enterprises run the risk of noncompliance by allowing end users to choose what information they share, be that through OS configuration or application settings, both intentional or unintentional.

Apple's privacy settings are device-based with limited privacy controls. Apple claims to bypass certain aspects of privacy requirements by removing association of the user ID to requests made with Siri (Apple's digital assistant), Dictation, and Location. Anonymity of separating user ID from requests does not provide the end user or organization the control of or the visibility into historic data, which is an area where Microsoft excels and leads the industry.

Microsoft provides full transparency and control of end-user and organizational data, enabling enterprises to meet a large set of GDPR requirements using first-party, native controls. In contrast, enterprises that implement Apple operating systems will face dependence on third-party controls to meet GDPR requirements, as Apple lacks native cloud-based privacy control tools for both macOS and iOS. Integrating, managing, and using these third-party tools will have a direct negative impact on total cost of privacy management and employee productivity.

Introduction to Privacy

The axiom “if you have nothing to hide, you have nothing to worry about” is used too often in defending cyber privacy overreach by companies and software vendors alike. While the saying might be true in a small subset of use cases, it represents a very narrow way of looking at privacy, especially given the array of privacy problems mixed up in data collection and used beyond analytics and disclosure.

Privacy of data and images includes concerns about making sure that individuals’ data is not automatically available to other individuals and organizations and that people can exercise a substantial degree of control over that data and its use. Furthermore, with the explosion of big data, enterprises need a robust data privacy solution to help prevent breaches and enforce security in complex IT environments. One of the best strategies for controlling access to information or physical space is having a single access point, which is much easier to secure and control than managing many such access points. The fact that big data is stored in such widely spread places runs against this principle. Its vulnerability is far higher because of its size, distribution, and broad range of access. In addition, many sophisticated software components do not take security seriously enough, including parts of companies’ big data infrastructure. This opens a further avenue for potential attack. As a result, it becomes increasingly important to demand a heightened level of security through vehicles such as terms and conditions, service level agreements, and security trust seals from organizations collecting and using big data.

Based on consistent estimates of the Big Four accounting firms, Fortune 500 companies are about to spend between 7 and 8 billion U.S. dollars to ensure they are compliant with the GDPR, effective in May 2018. Yet the cost of noncompliance with the GDPR is estimated to be 2.7 times greater than the cost of achieving compliance. While the U.S. government might be less compelled to fine companies for encroaching on people’s privacy, the European Union’s governing body, the European Commission (EC), has shown no restraint in this area. One example is the EC recent fining of Google for $2.9 billion for denying “consumers a genuine choice" when shopping online. This leaves U.S. consumers’ privacy more dependent on privacy controls offered by vendors that collect their private information, as there is less regulatory oversight and intervention by the government.

Because of the extraordinary cost and business implications for companies such as Google, with a business based on monetizing private data, the GDPR makes data privacy a hot topic and impacts every company that collects data from its customers. The way this data is handled and managed, and the transparency of that process, will likely become an important differentiator in the technology realm and will shift the market power in favor of companies that provide greater transparency and privacy to their customers with respect to their personal information. In addition, we believe that the GDPR and the way leading technology vendors respond to it will have a significant impact on employee collaboration and productivity.

What can companies do to protect personal information? Most enterprises use third-party security controls to protect privacy, such as encryption, access control, intrusion detection, backups, auditing, and additional corporate procedures that can prevent data from being breached and falling into the wrong hands. As such, more security can promote more privacy. At the same time, heightened security can also hurt privacy: It can provide legitimate excuses for companies to collect private and potentially sensitive information, from accessing an employee’s web surfing history on work computers, to fully enabling keystroke loggers and network traffic sniffers. In such cases, there is a fine line between ensuring security and violating the privacy of the user.

Assessment Methodology

The overall assessment methodology followed by Pique Solutions was as follows:

1. Based on product documentation and other publicly available data, we determined the privacy features and capabilities provided natively across Windows 10, macOS, and iOS.

2. We conducted interviews with privacy subject matter experts to verify assumptions and respective capabilities.

3. We manually confirmed the natively supported privacy features and those that required third-party tools to achieve parity.

When scoring the relative feature and functionality of the three platforms, Pique Solutions applied the following scoring methodology. The baseline was calculated as the maximum score attainable, multiplied by the number of features evaluated in each category.

Feature	Functionality
1 - Requires 3rd-Party SW	1 - Not Intuitive
3 - 25% Integrated	3 - Slightly Intuitive
6 - 50% Integrated	6 - Moderately Intuitive
9 - 100% Integrated	9 - Highly Intuitive

To assess Windows 10, macOS, and iOS, Pique Solutions researched the privacy policies, features, and functionality across two main categories.

1. Privacy and Transparency

For the privacy and transparency category, we assessed the following:

- User control for ads, assessment, location, and personalized experiences
- Device-feature controls (e.g., microphone, camera, contacts)
- Control over shared data
- Ability to delete history

2. GDPR Compliance

For the compliance category, we researched based on the GDPR. The research compared the following versions of the operating systems:

- Microsoft Windows 10 (Pro, Enterprise, and S)
- Apple macOS High Sierra 10.13.3
- Apple iOS 11.2.6

Key Findings

In our analysis, both macOS and iOS fell short of Windows 10 in their ability to provide a centralized and effective control of privacy settings. This complicates privacy and compliance of the entire Apple device ecosystem (e.g., MacBook, iPhone, iPad), as privacy cannot be centrally managed for those devices without the use of third-party tools. While Apple is reasonably transparent on the data they collect, it lacks the ability to provide historic data and the ability to delete data. Unlike macOS and iOS, Windows 10 makes privacy controls very easy to find and is generally more transparent than Apple about their use of personal information. The following are the key findings that led us to this conclusion.

Windows 10 provides more details than macOS and iOS on the following data privacy aspects:

- Types of personal data it collects
- How it uses personal data
- Reasons for collecting personal data
- Ways users can access and control sharing their personal data

In addition, macOS and iOS collect significantly more user information than Windows 10 for the following services:

- Information from services such as YouTube, and internet history
- Telephony information including SMS messages
- Email information
- Location information
- Local storage information, which might include personal information

During the analysis, Pique Solutions learned that while Apple does communicate clearly the data types collected by macOS and iOS, each OS requires the end user to manually opt in or out of sharing different types of PII and other data in privacy settings. This is done on a per-device basis, with no detailed information as to what information is collected. One of the examples of Windows 10 providing better transparency over iOS and macOS is location information. While Windows 10 displays the historical data related to location information and allows users to delete it, macOS and iOS do not.

Data privacy policies require users to read them and understand their implications. Microsoft is clear in stating that administrators of Windows 10 have full control of and visibility into the individual users' information and that it does not collect personal information from devices. Apple also does not collect personal information from devices except for analytics, which requires the user to opt in.

In terms of the personal information that Apple collects, they do not provide the end user with the ability to delete certain aspects of voice queries and location history. Apple is also limited with their privacy control to either opt in or opt out of sharing upon installation of said application. As a result, when it comes to privacy and control of personal data, Microsoft provides fuller transparency and control of user privacy. In addition, unlike Apple, Microsoft clearly states its data retention policy and usage of information, such as browser history, IP, and location. Apple's data retention policy is limited to Siri and Dictation information, which Apple keeps for at least two years.

Privacy and Transparency

- Both Microsoft and Apple equally provide detailed information on the type of data collected and the use of that data. macOS and iOS are limited in their ability to provide user-centric capabilities to view and delete any queries made for web history.
- Apple does not provide users with any control for viewing and deleting voice requests made via Apple Siri or Dictation, as those requests are cached on a server to which users do not have access. Apple strips the User ID from any Siri or Dictation request.
- Microsoft leads the industry in privacy, transparency, and control settings. This is evident in dedicated and comprehensive cloud-enabled privacy controls that tie to User ID regardless of which device is in use.

GDPR Compliance

- Windows 10, macOS, and iOS do not achieve the entirety of the GDPR, but they are able to achieve several tenants of the GDPR, which are detailed in "Feature and Functionality Comparison," later.
- Apple's lack of native centralized control of a user's privacy places enterprises at a cost and productivity disadvantage, because it requires them to us third-party solutions to centrally manage privacy to meet compliance.

The following comparison of features and functionality across key categories relevant to privacy and GDPR compliance is based on our review of publicly available information, as well as on hands-on testing of Windows 10, macOS, and iOS.

Feature and Functionality Comparison

Privacy and Transparency

The following table summarizes the results of our hands-on testing of privacy and transparency provided by Microsoft and Apple. With 45 being the baseline score for both feature and functionality, Microsoft scored higher than Apple in all categories, with a notable advantage over Apple in functionality, especially for macOS.

Testing Scores	Baseline	Feature	Functionality
Windows 10	**45**	**45**	**45**
macOS	**45**	**29**	**13**
iOS	**45**	**29**	**22**

Microsoft and Apple both provide detailed privacy terms. At the highest level, they both outline what type of information is collected, how the information is used, and how a user can access and update privacy settings. The collection of users' personal data is obtained using applications such as email (@icloud.com, @me.com, and @mac.com or O365), web searches, and voice queries. It is important to note that Apple's email offering is consumer-grade only, unless O365 is used on an Apple device.

Both Microsoft and Apple allow similar levels of control over the use and storage of location information, specifically in the areas outlined below.

Location Awareness Privacy

Location Tracking	Microsoft	Apple
Opt-in	Yes	Yes
Per-app setting	Yes	Yes
Sent to cloud	Yes	Yes
Location history	Yes	Yes
Anonymity of user	No	Yes
Can be disabled	Yes	Yes

Windows 10 only stores location history locally, and the data is kept for a maximum of 24 hours or until a system reboot. Apple does not store the location history within the user's Apple account but rather in the Apple infrastructure after removing the User ID associated with the location. The only caveat is when a user logs into a device in a different location. While this can be disabled by enterprise policy, the information remains on the Apple servers for more than two years, without your ability to delete it. Location tracking for Windows 10 devices follows the same policy for macOS and iOS). It is possible for applications, when allowed access, to send location data also to third-party applications and services.

Transparency

Enterprises have many different privacy concerns depending on their industry and the nature of their business. Apple's stated goal is to be clear about the information it collects. Apple provides the following guidance:

- Apple records users' activity, such as past searches, associated with user accounts when using Apple services. Except for Apple Siri and Dictation, these controls can be managed, including the ability to control whether certain activity is stored in a cookie or similar technology on users' devices when they use Apple services while signed out of their accounts. For Apple Siri and Dictation, users have no access to those queries.
- Enterprises can view and edit user preferences related to ads, cookies, tracking, and other settings on a per-device level. This can be done using the privacy settings within any given Apple device.
- Users can control with whom they share information through their Apple account, but this is limited to location and photo sharing on the device.

In comparison to Apple, Microsoft displays greater transparency about its privacy practices, including sharing where user data is stored, affirming that their data is used only to provide them with online services. In the consumer segment, Microsoft gives users full control of what they want to disclose to Microsoft. Windows 10 allows users to perform the following configurations and actions related to privacy:

- View and clear browser data that Microsoft collects when Cortana and Edge are used.
- View and clear location information that Microsoft collects when Microsoft products and services are used.
- View and delete information about Bing search activity.
- Manage what information Cortana stores to provide personalized recommendations.
- Manage apps and services that can access personal data.
- Choose whether or not to see interest-based advertising.
- Edit who can see their profile in Skype and other privacy settings by signing into their account at Skype.com.

In the enterprise, these settings can be configured via Group Policy and/or mobile device management.

The preceding configurations and actions are just some examples of the modifications that end users can make to protect their privacy in a corporate environment. In contrast, when setting up an Apple profile for the first time on a desktop system, users are given a set of union rules that are dictated by the corporate IT organization. In this case, users click the Accept button to, for example, gain access to their email or calendar. What the users do not realize, however, is that by doing so they also permit all browsing performed with the Apple (macOS and iOS) browser to be logged by corporate IT when using a third-party tool.

In comparison to Apple, Microsoft uses stricter controls natively to govern access to customer data, granting the lowest level of access required to complete key tasks and revoking access when it is no longer needed.

Apple (for both macOS and iOS) does not offer an easy way to manage the data that applications can or cannot access. The consumer user will receive a disclaimer when he or she first installs each app, but the only option to not divulge personal data is to uninstall the application. Apple does not allow user access to Siri and Dictation search history, and it does not provide the ability to delete Siri and Dictation requests. To justify this, Apple claims that it does not tie those requests to a specific user when the data is collected, thus ensuring anonymity. With Windows 10, users can easily control access to data such as location, contacts, messaging, calendar, and other personal information on a per-app basis in the Privacy section of its Settings menu. Compared to Apple, Microsoft offers much more granular privacy controls and supports many more customer use cases of privacy control from individual to enterprise user.

Diagnostics

Apple's diagnostics and monitoring features are visible and controllable by the consumer end user in the privacy settings on a per-device basis (e.g., MacBook, iPad iPhone). According to Apple, when users open a specific application, they are given the control to allow or block GPS, as well as allow or deny access to video or photo albums. Apple claims that it will not use any of this information to identify the user and that the collected information is only used to improve the performance and usability of macOS and iOS, respectively. In addition, Apple allows users to opt out; however, the information collected by Apple is accessible by developers in the Apple ecosystem of third-party applications, who follow their own privacy practices.

In contrast, Microsoft's Windows 10 management platform, Enterprise Mobility + Security (EMS) for IT administrators, offers multiple diagnostic features that are designed to assist the user by performing a series of checks to make sure that the system is running correctly. It provides an interactive user experience that does not leave the user uncertain about the information he or she discloses, in addition to providing information about the device's operational state and health.

Among other tools available to the Windows 10 user for increased diagnostics and transparency is the Windows Diagnostic Data Viewer. Available to everyone via the Microsoft Store, the Diagnostic Data Viewer is separate from the Microsoft Privacy Dashboard and allows users to see, search, and act based on the diagnostic data. The Diagnostic Data Viewer allows users to see the following:

- Common data, like the operating system's name, its version, Device ID, Device Class, diagnostic level selection, and more.
- Device connectivity and configuration, such as device properties and capabilities, preferences and settings, peripherals, and device network information.
- Product and service performance data that shows device health, performance and reliability data, movie consumption functionality on the device, and device file queries. It is important to note that this functionality is not intended to capture users' viewing or listening habits.
- Product and service usage data includes details about the usage of the device, the operating system, applications, and services.
- Software setup and inventory such as installed applications, install history, and device update information.

The Windows Diagnostic Data Viewer provides even greater transparency to all the diagnostic data received from Windows 10, in addition to providing users with features such as view, search, and filter of the diagnostic data, as well as the ability to provide feedback about the viewer. Combined with the Microsoft Privacy Dashboard, users can manage their data and change what data is collected by adjusting the privacy settings on their device or browser at any time.

Lastly, the Microsoft Privacy Dashboard provides a new Activity History page, which provides users clear and easy navigation to see the data that is saved in the Microsoft account. This dashboard allows users to manage their data and change which data is collected by adjusting the privacy settings on the device or browser at any time. The diagnostic data provides users with transparency into what information Microsoft collects, as well as control over that data. In the case of Apple, privacy settings are found in System Preferences on the MacBook and in Settings on the iPhone, which are built for the consumer and still require end user control if the enterprise supports Apple’s bring-your-own-device program. When a user finds the privacy controls, he or she is presented with a series of radio buttons to enable or disable the collection of privacy information.

Apple provides the following menu of items under Privacy Settings:

Sign-in and Security

- Signing in to Apple
- Apps with account access

Personal Information and Privacy

- Personal user information
- Contacts
- Management of user’s Apple activity
- Ad settings
- Control of content

Microsoft’s privacy settings and control can be accessed within a user’s Microsoft account. Navigating, viewing, and changing privacy settings only requires a couple of clicks, and this is much more intuitive compared to Apple. Apple also allows users to control their data but only in the form of “warnings” of what data they share and related pop-ups that allow users to opt in or opt out of sharing specific personal information. Depending on whether a user is using macOS or iOS, he or she can choose to opt out of location sharing and clear the web browser cache locally. This data, however, cannot be deleted at an account level.

Location Awareness

As most users quickly learn, both Microsoft and Apple focus on location awareness. While Microsoft takes a more direct approach to user location tracking and only reports it when queried, Apple takes a more passive approach and provides mapping and pin drops as it pertains to the user’s location. Both macOS and iOS have location awareness tracking, and mapping services are not enabled in policy by default. Starting with the Fall Creators Update, Microsoft is extending this experience to other device capabilities for apps that users install through the Windows Store. They will be prompted to provide permission before an app can access key device capabilities or information such as camera, microphone, contacts, and calendar, among others. This way, users can choose which apps can access information from specific features on their devices. Again, this capability is hard to attain in an Apple environment, given the fragmentation of the Apple ecosystem.

Windows 10 location controls within EMS are somewhat more passive in nature. When a user is outside of the designated geolocation on a global scale, the administrator with the ability to allow user access from foreign locations is alerted and given GPS coordinates and basic country and network block information. Granted, should the administrator desire to know the exact location of the user, he or she could do so by using GPS coordinates.

The key difference between Microsoft and Apple is that, while they both track the user's location when enabled, Windows 10 does not actively present the administrator with a map populated by all the locations that the user visited, as some of those locations might be related to personal matters. While workers are often asked by their employers to make themselves available while on personal travel via email and mobile devices, Windows 10 users are truly protected when location sharing is disabled, whereas macOS and iOS users are not.

Device Feature Controls

Windows 10, macOS, and iOS all provide device-feature controls that are either tied to the operating system and/or applications. The following is a list of the various device features that users can enable or disable across all three platforms:

- Microphone
- Camera
- Contacts
- Calendar
- Messaging
- Making phone calls (limited to Apple)

All three platforms provide easy and intuitive access within the settings of the operating system to enable or disable those features. There is not much difference in the level of device control in the privacy settings across the three platforms; however, Windows 10 provides the most granular controls for deleting web history, digital assistant history via Cortana, and location information. This can be accomplished within Windows 10 or online. Apple also allows users to delete their web history and location information, but Dictation history and queries made via Apple's Siri are not accessible and cannot be deleted by the user. Just like Apple's web browser, it will tailor user experience by serving up ads based on his or her search history. Similarly, Siri will also use voice queries for ads that might be of interest to the specific user.

GDPR Compliance (Compliance and Control)

Based on our hands-on testing and an in-depth review of public documentation, Windows 10 scored higher than macOS and iOS for GDPR compliance, as depicted in the following table.

Testing Scores	Baseline	Feature	Functionality
Windows 10	**9**	**9**	**9**
macOS	**9**	**6**	**6**
iOS	**9**	**6**	**6**

The GDPR imposes a wide range of requirements on organizations that collect or process personal data, including a requirement to comply with the following key principles:

1. Ensure transparency, fairness, and lawfulness in the handling and use of personal data. Organizations must be clear with users about how they use their personal data and are required to have a "lawful basis" to process that data.

2. Limit the processing of personal data to specified, explicit, and legitimate purposes—that is, organizations cannot reuse or disclose personal data for purposes that are not "compatible" with the purpose for which the data was originally collected.

3. Minimize the collection and storage of personal data to that which is adequate and relevant for the intended purpose.

4. Ensure the accuracy of personal data and enable it to be erased or rectified—that is, take steps to ensure that the personal data an organization stores is accurate and can be corrected if errors appear.

5. Limit the storage time of personal data. Companies must ensure that they retain personal data only for as long as it is necessary to achieve the purposes for which the data was collected.

6. Ensure security, integrity, and confidentiality of personal data. Organizations must take steps to keep personal data secure through technical and organizational security measures.

7. The systems organizations use to create, store, analyze, and manage data can be spread across a wide array of IT environments, personal devices, on-premises servers, cloud services, IoT devices, and so on. This means that most of the IT landscape of any organization could be subject to the requirements of the GDPR.

Many of the security controls to prevent, detect, and respond to vulnerabilities and data breaches required by the GDPR are like the controls expected by other data protection standards, such as the ISO 27018 cloud privacy standard. Rather than track the controls required by individual standards or regulations on a case-by-case basis, a best practice is to identify an overall set of controls and capabilities to meet these requirements.

Microsoft just recently released a new information protection strategy. The intelligent compliance solutions in Microsoft 365 help users assess and manage their compliance risks and leverage the cloud to identify, classify, protect, and monitor sensitive data residing in hybrid and heterogeneous environments to support GDPR compliance.

The recent updates in Microsoft 365 go a long way to help protect sensitive data and include the following:

- Compliance Manager general availability for Azure, Dynamics 365, and Office 365 Business and Enterprise customers in public clouds
- Compliance Score availability for Office 365
- Azure Information Protection scanner

In addition to the updates announced recently, capabilities in Microsoft 365 help enterprises and users to achieve the following:

- Protect sensitive data in apps and across cloud services
- Support data protection across platforms
- Provide a consistent labeling schema experience (in preview)

With the new updates, Microsoft 365 further enhances the privacy protection capabilities of Office 365, Windows 10, and EMS. It also integrates them into a rich set of solutions that help users assess and manage their compliance risks by leveraging artificial intelligence to protect their most important data. Since 2016, Microsoft Azure has included the Information Protection service, which checks for sensitive information in an organization's emails and attached documents. With the recent update, a scanner-tool addition—the Azure Information Protection scanner—can be used to discover sensitive files at an organization's premises when they are stored on Windows Server or network-attached drives, as well as at SharePoint Server data stores. For SharePoint Online and Exchange Online, Microsoft offers a scanning service through its Office 365 Data Loss Prevention solutions.

Microsoft also has plans to make its information protection labeling consistent across the Azure Information Protection service and Office 365 services. The idea behind this "unified labeling" concept is that a label created for one service will be available for others. The support of hybrid cloud and its impact on privacy and data protection is yet another important differentiator of Microsoft versus Apple that, again, relies on third-party partnerships to support hybrid cloud capabilities and requirements. For example, to protect sensitive data on-premises, Azure Information Protection scanner allows users to configure policies to automatically discover, classify, label, and protect documents in their on-premises repositories. The scanner can be configured to periodically scan on-premises repositories based on company policies. There is no native equivalent of this capability by Apple.

Lastly, Microsoft has made impressive efforts in supporting the privacy of all major devices and non-Windows platforms and is now supporting the privacy of Office 365 applications on Mac without plug-ins, as well as expanding support for the privacy of PDF files in partnership with Adobe.

Conclusions

Based on Pique Solutions in-depth comparative review of Microsoft's and Apple's policies related to the types of user data collected in Windows 10, macOS, and iOS, as well as the usage of that data, we conclude that Windows 10 provides more transparent privacy controls for both the enterprise and the consumer markets. Because Apple focuses mainly on the consumer market, it relies on third-party tools to provide the level of functionality and granularity of privacy controls required by the enterprise that Microsoft provides natively. We also found that Windows 10 offers more extensive data privacy and protection tools for centralized management of privacy and compliance. By centralizing the management of privacy control, Windows 10 reduces the cost of managing privacy and compliance in the enterprise.

With the GDPR, privacy is becoming increasingly important for both end users and enterprises. Both Microsoft and Apple clearly outline their policies related to the collection of private information and the disposal of said information. They also both provide easy access to those policies. However, while Microsoft extends this transparency with specific privacy controls in Microsoft 365, which provides the enterprise and the user with native access to managing, diagnosing, and monitoring privacy in a central location regardless of device type, this is only possible via third-party tools in Apple macOS and iOS. There are many third-party controls designed to address the misuse and dissemination of information including encryption, access control, intrusion detection, backups, and access auditing. However, while third-party controls reduce data leakage to ensure privacy, they require an additional layer of tools and technology, thus increasing the complexity and the cost of their integration and management. This constitutes a tremendous advantage for Microsoft because it contributes to a lower total cost of ownership for Windows 10 compared to that of macOS and iOS. In addition to the higher cost and complexity of privacy management for Apple, there is also a greater risk of privacy breaches associated with introducing third-party products and the need to effectively operationalize them in the workflow.

In summary, after an in-depth, side-by-side comparison of Microsoft's and Apple's privacy, transparency, diagnostics policies and tools, and the control given to users over the usage of their personal information, Pique Solutions has found that Windows 10 and the complementary integrated and native tools offered under the Microsoft 365 umbrella provide a more comprehensive set of controls when compared to macOS and iOS in every aspect reviewed. Microsoft's approach to collecting personal information is more transparent and provides a centralized and easier-to-administer set of tools for protecting privacy and information including tracking of data usage. Lastly, the built-in privacy controls provided natively in Windows 10 enable organizations to comply with a large set of GDPR requirements, while the native privacy controls offered in macOS and iOS fall short in several important aspects.