PIQUE SOLUTIONS

Privacy and GDPR Compliance: Windows 10 versus Chrome OS and Android 8

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 Google Android 8 and Chrome OS 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 Google and that Microsoft also provides a more unified approach to managing and ensuring user privacy, with a more granular and easier-to-use set of controls, in comparison to Google.

Unlike Google, Microsoft has little economic reliance on personal data. This allows Microsoft to not only be more transparent about use of personal data but also more genuinely committed to the privacy of its customers. In other words, while privacy is a potential source of competitive advantage for Microsoft, it directly threatens Google's core business. With GDPR, we will see increased pressure on companies to change the way they collect and use data. On the other hand, with the increased application of big data and machine learning, the evolution of IoT, and the adoption of cloud, privacy and security risks will increase. It remains to be seen how successful governments can be in enforcing tougher privacy standards, but we believe that customers will increasingly demand transparency of the use of their personal data, as well as greater control over what personal data companies collect from them and how they use it. Based on our analysis, Microsoft has a significant lead over Google in both of these aspects, and that lead will likely increase as privacy becomes a source of competitive advantage.

Recently, customers raised the issue of why Chrome Cleanup Tool (CCT), a malware scanner that is integrated into the Chrome browser, not only can scan the files in the Documents folder without explicit permission of the user but also cannot be turned off, unlike the corresponding tool in Windows 10, the Windows Defender. While the concerns about Google's disposition of the data collected by CCT might be exaggerated, it is an example of Google's opaque transparency policies and insufficient level of control provided to the end user.

Our analysis found evidence of inferior transparency and insufficient privacy controls provided to end users by Google as compared to those of Microsoft. When comparing the granularity of features and the functionality of privacy controls of Windows 10 versus those natively offered in Chrome OS and Android, Windows 10 consistently scored higher in all the following categories of comparison: privacy, transparency, location awareness, diagnostics, and GDPR compliance. Besides the deficiencies found in Google's own approach to privacy and transparency, Google's ubiquitous sharing of personal data with third parties further jeopardizes the privacy of their customers.

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, as there are serious repercussions for not meeting the GDPR. The penalties for non-compliance of the GDPR carry fines of up to €20M or up to 4 per cent of total global revenue of the preceding year, whichever is greater. Other fines and penalties can range around €10M or up to 2 per cent of total global revenue of the preceding year, whichever is greater. 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, Chrome OS, and Android 8.

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, Chrome OS, and Android, 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)
- Google Chrome OS 62
- Google Android 8 (Oreo)

Key Findings

During our analysis and testing, Pique Solutions learned that Google collects significantly more PII than Microsoft, and that the privacy controls in Windows 10 are easier to find and use than those in Chrome OS and Android. While Google discloses the data types collected by Chrome OS and Android, 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 per-device basis that can be tied to either an enterprise account or a consumer account.

Although Google's privacy policies may seem transparent at first, after an in-depth review, it becomes apparent that Google nebulously collects and stores sensitive information that potentially makes organizations vulnerable to intellectual property and personal information breaches. Moreover, Google's privacy policies are not necessarily followed by developers of its ecosystem of third-party applications who become privy to personal information without necessarily having to adhere to Google's data privacy policies. Throughout the analysis, we found that Microsoft is generally more transparent than Google about the use of personal information.

Specifically, Windows 10 provides more details than Chrome OS and Android 8 in 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, Chrome OS and Android 8 collect significantly more user information than Microsoft, namely:

- 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

Until recently, most individuals did not read privacy statements and End-User License Agreements in much detail. Although Google's privacy policies might seem transparent at a superficial glance, after an in-depth review, it becomes apparent that Google nebulously collects and stores sensitive information that potentially makes organizations vulnerable to intellectual property and personal information breaches. Although Google claims that it protects personal information, the type of information it stores should be alarming to both enterprises and consumers. Moreover, Google's privacy policies are not necessarily followed by developers of third-party applications, and they become privy to personal information without having to adhere to Google's data privacy practices.

As mentioned above, a data privacy policy requires the end user to read it in its entirety and understand its implications. Microsoft is clear in stating that administrators of the Microsoft environment have control and visibility into the individual users' information and that it does

not collect personal information from end-user devices. The only caveat that Microsoft states is that it will share information if it believes said information is criminal. In terms of the personal information that Google collects from users' devices, Google does not provide the end user with the ability to delete or control that data. As a result, when it comes to privacy and control of personal data, Microsoft provides a fuller transparency and control of user privacy. In addition, unlike Google, Microsoft clearly states its data retention policy and usage of information such as browser history, IP, and location.

Windows 10 provides similar details vs. Chrome OS and Android 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

Google collects significantly more user information than Windows 10 when one includes Android for the following services:

- Information from services such as Google Search (internet history) and Google Hangouts, to name a few
- Telephony information including SMS messages
- Email information
- Location information
- Local storage information, which might include personal information

Privacy and Transparency

- Microsoft provides a superior per-app control of the use and storage of personal information as compared to Google.
- Microsoft uses stricter controls than Google to govern access to customer data.
- Microsoft is more transparent than Google with respect to providing detailed information on the type of data collected and the use of that data.
- Both Microsoft and Google track user location; however, unlike Chrome OS and Android, Windows 10 does not actively present the administrator with a map of all the locations visited by the user. Also, location tracking and the use of location data can be managed on a per-app basis in Windows 10 but not in Chrome OS and Android.
- Both Microsoft and Google provide the ability to view history and delete any queries a user made with web searches and by a digital assistant.
- Both Microsoft and Google provide the ability to view and delete all location information.

GDPR Compliance

- Neither Microsoft nor Google achieve the entirety of GDPR, but they are able to achieve several tenants of GDPR, which are detailed in the feature and functionality comparison below.
- To obtain a GDPR-compliant solution from Google, one needs to make a request using a “super admin” account. This makes the process ambiguous and cumbersome.
- Microsoft’s stronger support of hybrid cloud scenarios enables users to more effectively manage their compliance risks and leverage the cloud to identify, classify, protect, and monitor sensitive data residing in hybrid environments. This translates into better support of GDPR compliance for companies using hybrid cloud deployments.

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 Google. While Google and Microsoft provide comparable features, Microsoft displayed a notable advantage over Google in functionality.

Testing Scores	Baseline	Feature	Functionality
Windows 10	**45**	**45**	**45**
Android 8	**45**	**45**	**25**
Chrome OS	**45**	**45**	**25**

Microsoft and Google 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 (Gmail or O365), web searches, and voice queries.

As evident from the following table, Microsoft provides a slightly higher level of control of the use and storage of location information, specifically by natively offering a per-app setting, which Google lacks.

Location Awareness Privacy

Location Tracking	Microsoft	Google
Opt-in	Yes	Yes
Per-app setting	Yes	No
Sent to cloud	Yes	Yes
Location history	Yes	Yes
Anonymity of user	No	No
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. Just like Microsoft stores this information in MSA, Google stores the location history within the users' Google account. While this can be disabled by enterprise policy, the time frame can be for more than 12 months. Location tracking for Android devices works on the same policy as Chrome OS. It is possible that applications, when allowed access, send location data also to third-party applications and services. This is true also for Windows 10 devices; however, in the case of Chrome OS and Android, which rely heavily on third-party applications, controlling the privacy settings can become cumbersome and overwhelming, as the user is required to read the privacy and service agreements of those specific third-party apps and services and make the necessary configurations on those apps in addition to Google's native privacy settings.

Transparency

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

- Google records users' activity, such as videos watched on YouTube and past searches, associated with user accounts when using Google services for both enterprise and consumer segments. These controls can be managed, including whether certain activity is stored in a cookie or similar technology on users' devices when they use Google services while signed out of their accounts. G Suite administrators can also restrict which videos are viewable.
- Enterprises can view and edit user preferences related to Google ads shown to the users on Google.com and across the web, such as which categories might be of interest to the users. This can be done using the Ads Settings. Users can also visit the specific page to opt out of certain Google advertising services.
- Users can control with whom they share information through their Google account.
- Users can take information associated with their Google account out of many of Google's services.
- Users can choose whether their profile name and profile photo appear in shared endorsements that appear in ads.

Google G Suite tracks users' locations, search history, and Tailored Ads and places similar cookie-tracking technology on end-points.

In comparison to Google, Microsoft displays greater transparency about its privacy practices, including sharing where user data is stored, both online and offline. Microsoft gives users full control of what personal information they want to disclose to Microsoft. In the consumer segment, 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 within the Microsoft privacy dashboard.
- 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 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 a Google 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 using the Chrome OS browser to be logged by corporate IT.

Microsoft uses stricter controls than Google 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.

By default, Google collects the URLs of pages one visits to provide alternate suggestions when one cannot reach a specific website. It autocompletes searches and URLs based on one's browsing history and related searches, and it preloads web pages (including their tracking cookies) for web links that one might click. A visit to Chrome OS settings lets the user disable each of these options; however, if the user's enterprise policy is being enforced, that option is taken away.

Unfortunately, Chrome OS does not offer an easy way to manage the data that applications can access. Users will receive a disclaimer when they first install each app, but their only option if they are uneasy about personal data collection is to uninstall that specific application. 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 Google, Microsoft offers much more granular privacy controls and supports many more customer use cases of privacy control from the individual user to an executive enterprise user.

Diagnostics

Google's G Suite for enterprise is a platform that can be accessed via both Chrome OS and Android. It includes two types of diagnostics and monitoring: The first one sends information to the enterprise and the second one to Google. According to Google, when usage and diagnostics are turned on, those devices send information to Google about the usage and performance of specific features. For example, the device can send information such as battery level, application usage patterns, and the quality and length of network connections (e.g., mobile, Wi-Fi, Bluetooth). Google 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 Google Android and Chrome OS, respectively. However, the information collected by Google is accessed by developers in the Google ecosystem of third-party applications, who follow their own privacy practices.

In contrast, Microsoft's Windows 10 management platform, Microsoft Enterprise Mobility + Security (EMS), offers multiple diagnostic features that are designed to assist IT administrators 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 Google, finding privacy settings is much more difficult and time-consuming. When one does find the privacy controls, he or she is presented with a series of pop-up questions that ask users to rate the ease of use and effectiveness of the privacy settings. This series of pop-ups indicates that Google realizes that the level of transparency and control are not easily obtained and is perhaps working on improving them.

Google provides the following menu of items under Privacy Settings:

Sign-in and Security

- Signing in to Google
- Device activity and security events
- Apps with account access

Personal Information and Privacy

- Personal user information
- Contacts
- Management of user's Google activity
- Ads settings
- Control of content

Users can access their Google privacy settings in their Google account. They can then manually go through each privacy setting, which involves multiple screens, subsettings, and clicks. Google does offer the option to click Privacy Checkup, but this option provides a limited view of privacy settings for the consumer segment and the same manual work is required to change settings through multiple steps. 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 Google.

Location Awareness

As most users quickly learn, location awareness is natively offered within all three operating systems. While Microsoft takes a more passive approach to user location tracking and only reports it when queried, Google takes a more active approach and provides mapping as it pertains to the user's location. Both Chrome OS and Android 8 have location awareness tracking and mapping services enabled in policy by default for geographical tracking purposes. On the outside, this does not appear to be intrusive, as geographic policies are supposed to track a user's location; however, it is important that users receive transparency and control over which applications can access their location information. Most users are accustomed to being prompted for permission to use location data when using a map or other location-aware application. 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 a Google environment, given the fragmentation of the Google 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 Windows 10 and Google is that, while they both track the user's location, 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, Google's active location tracking can often be an overly invasive tracking method when deployed on a BYOD-enrolled device. With Google, even though a user might opt out of sharing their location, they still populate their login information with location. The location information of Microsoft users, on the other hand, is truly protected when location sharing is disabled.

Device Feature Controls

Windows 10, Chrome OS, and Android 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

All three platforms provide easy and intuitive access within the settings of the operating system to enable or disable those features. For instance, Google Android prompts the user upon installation by asking for permission to grant access to an application to make a phone call on his or her behalf. There isn't much difference in the level of device control in the privacy settings across all 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. Google also allows users to delete their web history, location information, and any queries made by Google's digital assistant. Just like Google's web browser, it will tailor user experience by serving up ads based on the user's search history. Similarly, Google's digital assistant will also use voice queries to 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 versus Chrome OS and Android for GDPR compliance, as depicted in the following table.

Testing Scores	Baseline	Feature	Functionality
Windows 10	**9**	**9**	**9**
Android 8	**9**	**7**	**4**
Chrome OS	**9**	**7**	**4**

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 designed 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.

Currently there are two GDPR-compliant solutions in the marketplace: Microsoft 365 Enterprise and Google G Suite Enterprise. The key issue is choosing the solution that best fits the organization's privacy policies and requirements. To obtain a GDPR-compliant solution from Google, one needs to make a request using a "super admin" account. This makes the process ambiguous and dubious. Microsoft, on the other hand, is completely transparent about the process of gaining compliance, and provides users with detailed information related to how the process works.

Lastly, 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 general availability (GA)

In addition to these updates, 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 Google that, again, relies on partnerships (e.g., with Cisco) 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 Google.

Lastly, Microsoft has made formidable effort 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

Countermeasures such as encryption, access control, intrusion detection, backups, auditing, and other corporate procedures can prevent data from being breached and falling into the wrong hands. While security can enhance privacy, heightened security can also hinder it, as it can provide legitimate excuses to companies for collecting private employee information.

One of the leading reasons behind privacy violations is that enterprises and the user community are continuing to blindly trust companies that clearly state in their privacy statements that they can effectively pull personal information from mobile and laptop devices, upon the acceptance of their terms, without a detailed understanding of the details related to the use of that data.

While both Google and Microsoft collect personal information from users, we believe that Microsoft's protection of user anonymity is greater than that of Google, as Microsoft keeps all collected data anonymous unless given explicit user permission and does not share the collected information with third parties as Google does. Given Google's great reliance on the ecosystem of third-party applications, user privacy becomes inherently more difficult to protect, as each third-party provider has their own set of privacy rules that may or may not be transparent or adequate.

While there is a fine line between potential privacy violation and the need to collect data from users to improve user experience and the quality of products, we believe that Microsoft is more transparent than Google when it comes to disclosing the exact use of the different types of collected data, is more effective in providing users with a unified platform to manage data privacy settings across any device category and, finally, provides users with more effective controls for protecting their privacy. Finally, with Azure, Microsoft provides superior hybrid-cloud privacy protection capabilities that enable companies to protect their sensitive data with more confidence.

In summary, after an in-depth, side-by-side comparison of Microsoft's and Google's privacy, transparency, diagnostics policies and tools, and the control given to users over the usage of their personal information, Pique Solutions concludes that Microsoft is superior to Google in each of those aspects. Not only is Microsoft's approach to collecting personal information more transparent, but it also provides IT organizations and end users with more effective and easier-to-use tools for protecting their personal information and determining its use.