PIQUE SOLUTIONS

Privacy: Windows 10 versus Google Chrome OS and Android

Feature and Functionality Comparison

PIQUE SOLUTIONS

April 2019

MICROSOFT SPONSORED THE DEVELOPMENT OF THIS WHITE PAPER.

THE UNDERLYING RESEARCH AND ANALYSIS WERE EXECUTED INDEPENDENTLY BY PIQUE SOLUTIONS.

795 Folsom Street, 1st Floor | San Francisco, CA 94107 | Tel.: 415.685.3392 | www.piquesolutions.com

Contents

Executive Summary

Privacy—or data protection, as it is referred to in the European Union—is not a new topic, and principles intended to drive consistent and trustworthy privacy practices have formed the basis of global laws and self-governing frameworks for many decades. The reason privacy has become such a pressing issue as of late is because the European Union has implemented rigorous regulation that impacts any company providing goods or services to individuals in the European Union, or that is monitoring or tracking personal aspects of EU citizens (e.g., demographics, hobbies, travel, social connections, shopping interests). The General Data Protection Regulation (GDPR) has set substantial fines for violations of the legally protected privacy rights of EU citizens. These privacy rights include the right of individuals to clearly understand how their personal information is being collected, used, and shared. The GDPR has profoundly broadened the scope of what is considered personal information, establishing numerous new types of information (e.g., device IDs, system configuration information, application usage, MAC addresses, network connections). As consumers provide information to obtain a particular service, the principles of data minimization and use limitation have established a keener focus on how and why certain data is being collected, whether or not the information is required for the provision of that particular purpose and, if not, then ensuring that the information is not collected unless consent has been obtained from the user.

The expression “the horse has already left the barn” is an understatement when it comes to the vast amount of personal information that has already been obtained (either directly or indirectly) from global consumers. The complex matrix of information sharing and data brokering that form the foundation of most information services that exist today has seen to this. The GDPR and other global laws are attempting to enable consumer control over the rampant collection, analysis, and prediction of information about them that has resulted from the explosion of social media, cloud computing, machine learning, the Internet of Things, and continually advancing mobile and wireless technologies.

In unison, recent headline-grabbing incidents of personal information misuse have heightened demand for personal privacy rights. Such incidents have stemmed from unexpected personal information collection, sharing, and profiling. Both laws and consumer demand are placing critical focus on the right to be informed of all data collection and how it is used. Brand reputations have been significantly impacted by such incidents and, now, by GDPR court actions that have emerged in recent months.

Pique Solutions was asked to evaluate the privacy features of various operating systems relative to these privacy requirements for transparency, user control, and compliance. The basic premise of transparency defined in privacy laws is to ensure that users—from potential buyers to existing customers—are aware of the personal data collection and usage that will transpire when they use a particular device or service. The process of providing notice about privacy practices is intended to occur at the point when personal data is about to be collected or as near to that time as possible. By virtue of the fact that this study is evaluating operating systems that are embedded in devices that are purchased by consumers, our focus will be on the information that is publicly available to potential buyers via the OS vendors’ privacy policies and related notifications regarding their privacy practices. This includes information provided during the installation of a new or upgraded operating system.

For this particular study, Pique was asked to define a set of “ideal scenarios” that comprise what are evolving as best practices related to the critical privacy requirements today. A side-by-side comparison of the privacy features of Windows 10 vs. Android and Chrome OS was then conducted based on publicly available information. This study did not involve any device testing.

Key Findings

Microsoft provides a substantial amount of information for users regarding their privacy options. From its home page, Microsoft uses a drill-down approach as the broad privacy topics are addressed in their policy, with links to additional information that specifically addresses the particular privacy topic within the context of Windows 10. Numerous references and links enable a user to research as granularly as desired before making a privacy choice.

Google uses a similar approach for their privacy policy; however, privacy controls for both Android and Chrome OS lack clarity due to overlapping descriptions of privacy settings that could be addressed at the browser, device, and Google account levels. Regarding Chrome OS, specific information is limited, although Google has recently augmented their January 2019 privacy policy with documentation published on March 12, 2019: “Google Chrome Privacy Notice” and “Google Chrome Privacy Whitepaper.” While the latter addresses a wide range of topics, the paper states, “[W]e touch only tangentially on Chrome OS,” which causes further confusion.

Microsoft requires logging in to an account to get to some critical information on the Privacy Dashboard, whereas Google provides their privacy information without the user having to log in.

Windows 10 enables viewing and deletion across almost all categories and provides specific information regarding the ability to download files to meet data portability requirements for information that is relevant. Data portability is only minimally addressed with Android.

Finally, while choices were identified very clearly in Microsoft’s documentation, the privacy settings information in Google’s documentation is less clear.

Assessment Methodology and Scoring

Traditionally, a corporate privacy policy is located at the bottom of the company's home page and is the initial starting point for a user to read about its privacy practices. Because this analysis was based on public information only, we opted to use each vendor's home page as our starting point.

To ensure an objective comparative analysis of the elements addressed in this study, Pique Solutions evaluated a common set of variables that would comprise an ideal scenario for privacy management and user control. Because this analysis was based solely on publicly available information and not on hands-on evaluations of privacy settings or control behaviors of the various operating systems, the objective comparative analysis has been based on whether each variable was evident in the documentation that is available to consumers by each vendor. The lack of evidence of a particular factor received a score of 0, which translates to "poor" in the rating scale. It should be noted, however, that a poor rating could result from either the apparent lack of a privacy control or a lack of available documentation about user controls, such as a privacy policy, granular privacy documentation, or privacy dashboards that enable consumers to be fully informed of the existence of these capabilities.

These ideal scenarios are based on the compliance requirements of the GDPR and other emerging and updated privacy laws, including those in California. The ideal approach to meeting the compliance requirements in each area is based on mechanisms that enable appropriate visibility and transparency for the consumer, corporate processes, and procedures that are evolving as the optimal ones to enable proper governance. Such procedures include related tracking, monitoring, and auditing of privacy governance controls and automated mechanisms that enable self-service customer privacy control and privacy preference management. While some manual processes are not inappropriate for the purposes of meeting GDPR requirements, the tight turnaround times (e.g., to provide information to a user under their Data Subject Rights of access to their personal information, correction, or deletion) require governance procedures that can be eliminated through these near real-time response mechanisms. Pique has not negatively rated any nonautomated process during this analysis; however, it is important to note what is evolving into best practice in the privacy management space.

In such an ideal scenario, each operating environment would include the following:

- Transparency/Notice
- Control/Choice
- Access/View Data
- Delete/Clear Data
- Data Portability

The following scoring system was used, with a maximum possible total score of 25.

Scoring Category	Score	Scoring Methodology
Transparency/Notice	0 to 5	0 = Lack of evidence or existence of control/capability 5 = Existence of control/capability evident
Control/Choice	0 to 5	0 = Lack of evidence or existence of control/capability 5 = Existence of control/capability evident
Access/View Data	0 to 5	0 = Lack of evidence or existence of control/capability 5 = Existence of control/capability evident
Delete/Clear Data	0 to 5	0 = Lack of evidence or existence of control/capability 5 = Existence of control/capability evident
Data Portability	0 to 5	0 = Lack of evidence or existence of control/capability 5 = Existence of control/capability evident If user data is not considered that which a user would opt to transfer to another service provider, the rating for Data Portability will be a 5 to typify “not applicable.”

Any number within the range is due to strong implications of existence of the control; however, complete certainty could not be ascertained, for instance, due to terminology, clarity of description, or inconsistent references across vendor policies and/or documentation.

Assessment Criteria and "Ideal Scenarios"

Transparency/Notice

Informed choice requires that a user is aware of data collection practices, prior to providing his or her personal information, typically to obtain a new product or service. Evaluation of operating systems presents a unique challenge, as the individual is purchasing a device within which the operating system has already been installed. This evaluation is therefore limited strictly to the operating system privacy policies or notices and information that the user encounters upon configuration of a new device and during any subsequent upgrading of the operating system on that device.

Ideal Scenario

- Information about data collection/sharing by each specific feature or functionality is provided in a transparent, clear manner to the potential customer or current user.
- Information is publicly available and does not require a potential customer or current user to sign in to their vendor account (e.g., Microsoft, Google, Apple ID) to obtain information regarding the privacy policy and practices of the operating system or update.
- Any additional information that provides a deeper explanation of the privacy implications of the feature are also made evident and readily available.

Control/Choice

As already indicated, informed choice leads to the ability for users to be fully aware of the implications of providing, or allowing the collection, usage, or sharing of, their personal information as they use their products, especially those that encompass complex information services–based platforms. *Control* ensures that users have the opportunity to choose whether or not to allow the processing of their personal information in the manner that was described to them through the processes in the preceding section. Many of the current headline-making incidents have included the use of personal information that was considered beyond the realm of "reasonable expectations" of users. Some of the features and functionalities enabled by the operating systems can collect personal information that users would prefer not to share. Ideally, once this data collection has been disclosed in the policy documentation suggested earlier, the consumer is given a choice to opt out of the feature's data collection rather than foregoing the entire service altogether.

Ideal Scenario

- The user is provided the ability to opt in or opt out of a feature's specific data collection.
- The user is provided with a real-time mechanism to choose or change preferences.
- Features are not bundled together in such a way that a feature-specific choice is not truly made available to the user because there are implications on other independent features.
- Opting out of specific data collection should not have a detrimental impact on the user, unless the personal information is absolutely required to provide that particular product or service offering.

Access/View Data

Users should have the ability to understand what personal information has been collected, aggregated, or otherwise captured about them. There are limitations cited in various global laws regarding the type of personal information that consumers are allowed to access. Information regarding their account

profiles, past transactions history, and browsing and surfing histories appears to be evolving into the traditional scope of what information users are requesting to view. Consequently, this paper has limited its scope to this emerging standard set of information for purposes of comparative analysis. Although self-service is not a legal requirement, there are timing requirements for these various data subject rights, so dashboards are emerging as the preferred mechanism through which consumers can request and see this information. Archived information is typically sent via email after a request has been submitted.

Ideal Scenario

- ⊕ The process by which to request access or viewing of personal data is identifiable.
- ⊕ The mechanism by which to request access to view personal information that has been collected about a user is available.
- ⊕ A self-service mechanism, such as a dashboard, provides real-time or near real-time viewing of collected personal information.

Delete/Clear Data

EU users have the right, under Article 17 of the GDPR, to request that information about them is deleted, within certain legal parameters. Manual processes are appropriate if response times meet privacy regulations. One best practice is the use of privacy dashboards as the mechanisms for self-service deletion of personal information in accordance with these requirements, particularly as digital evidence can be preserved to document the completion of the request.

Similarly, consumer expectations, particularly when data has been tracked without an individual's knowledge, are driving the need for technology providers to include mechanisms to delete information in this manner. This comparative analysis does not intend to assess the broader processes and implications regarding "the right to be forgotten"; rather, its scope focuses on the deletion of consumer user data that is being requested and fulfilled via these self-service mechanisms in place today.

Ideal Scenario

- ⊕ The process by which to erase personal information, as appropriate, is identifiable.
- ⊕ The mechanism by which to request deletion of certain personal information, as appropriate, is available.
- ⊕ A self-service mechanism, such as a dashboard, provides real-time or near real-time deletion of collected personal information.

Data Portability

The GDPR establishes the requirement for individuals to be able to download or otherwise obtain information that they may want to implement using a different technology service provider (e.g., CSV, JSON). The most obvious scenario for this is the portability of music, contacts, calendars, and so forth. Therefore, consumers should have the ability to receive this information in a manner that can be transferred. Technology providers may also offer options to directly transfer the information to the new provider, if the customer prefers.

Ideal Scenario

- The process by which to request relevant personal information in a portable format (or transferred directly by technology provider) is identifiable.
- The mechanism by which to request relevant personal information in a portable format is available.
- A self-service mechanism by which to request and receive a download of relevant personal information is available.

Application Access

While the scope of this comparative analysis is on the native applications of the operating systems, a critical privacy vulnerability exists in the independent application ecosystems enabled through the app stores of the various vendors. Policies defining compliance requirements that application developers must meet in order to participate in the app stores continue to be finetuned to include privacy-related aspects; however, validation processes differ among vendors and caveat emptor remains a guiding principle for many wary users. Mechanisms to block access to various features and functionalities by nonnative apps have been gradually introduced, with varying degrees of granularity, at the device level. This prevents the oft-referenced and true privacy scenario in which free flashlight applications were surreptitiously obtaining access to contact lists, microphones, and more.

One increasingly common approach ensures that users have the ability to define their preferred application permissions on their devices, and then, when an application requests or requires access to a particular feature, the user is alerted if their privacy setting is prohibitive. A relative rating has been determined based on whether or not these control capabilities appear to be in place, as well as on the breadth of controls that can be blocked at the device level. A “missing” component does not necessarily translate into a negative rating, particularly as categories of features and functionalities have not aligned to a common taxonomy. If the existence of a component control could not be determined, it was noted in this analysis only to indicate that, for a consumer, this represents a lack of visibility or transparency as to whether the blocking capability existed for that particular component. As this analysis did not involve a hands-on product evaluation and information was only gleaned from publicly available information from the vendors, it was not possible to determine what comprised the entire list of capabilities to which an application would seek access.

Ideal Scenario

- The user can choose to block access by applications to any features or functionalities.
- The user can modify his or her choice at any time.
- The user can make application-specific requests for access, ideally with granular choices.
- A permission request notification and/or mechanism alerts the user to access settings that have been blocked.

Detailed Comparative Analysis: Feature and Function Comparison

Location

Windows 10: Microsoft addresses location privacy across the various sections of its privacy policy, referred to as their "Privacy Statement." The statement clearly indicates what type of information is considered location data and how it is acquired. Then users are directed to the Microsoft Privacy Dashboard to learn more about how to control, view, and clear location data. On the dashboard, there is another link to the document "Windows 10 Location Service and Privacy," which provides even more information for understanding privacy settings and options. Location history can be downloaded in JSON format via the Activity History page.

Chrome OS: Chrome location settings can be chosen by selecting the "Ask before accessing" option. When selected, every site will ask for permission to access location. The default setting is for permission to be asked.

Android: The Google privacy policy prominently addresses location data collection and provides a link to the instructions "Turn your Android device's location on or off." Location accuracy is also an option that is provided. Another link provides information about location history, which can be collected if location reporting has been enabled and can be viewed and deleted on the history page through the user's Google account. Location history can be downloaded in JSON format via the Google Dashboard Download Your Data link.

Table 1. Scoring Results for Location

OS	Notice of Data Collection	Choice to Opt-Out	View Collected Data	Delete Collected Data	Data Portability
Windows 10	●	●	●	●	●
Chrome OS	●	●	○	○	●
Android	●	●	○	○	●

Poor ○ ◔ ◑ ◕ ● *Excellent*

Advertising

Windows 10: Microsoft prominently features a section on advertising with information regarding how to opt out of interest-based advertising. It further provides a link to an Opt Out page, where users may indicate their preferences. This page further explains the value of personalized advertising while also reiterating Microsoft's prioritization on user privacy. Windows 10–specific information is provided to guide the user through the steps of opting in or out of interest-based ads.

Chrome OS and Android: The Google privacy policy addresses Ad Settings, which requires that a user is signed in to his or her Google account. Ad personalization can be turned off in the Data and Personalization panel in a user's Google account. Google has added a "Why you're seeing an ad" page, with additional links to information on how to control certain ads. Clearer information is apparent on the Google Safety Center page related to Ad Settings.

Table 2. Scoring Results for Advertising

OS	Notice of Data Collection	Choice to Opt-Out	View Collected Data	Delete Collected Data	Data Portability
Windows 10	●	●	N/A	N/A	N/A
Chrome OS	●	●	N/A	N/A	N/A
Android	●	●	N/A	N/A	N/A

Poor ○ ◔ ◑ ◕ ● *Excellent*

Search

Windows 10: Microsoft addresses search in its privacy statement, including advising the user of the ability to go to the Privacy Dashboard to control, access, and delete search history. The Privacy Dashboard offers two additional links, one called "View and change your search settings," which offers extensive information and options for granular choices related to search. The second link provides more information about how to use InPrivate Browsing to avoid the collection of search history altogether. Search history can be viewed and cleared on the Activity History page. An archive of the user's search history can also be downloaded in JSON format on this page.

Chrome OS: The *Google Product Privacy Guide* addresses how to view and delete search activities, and the Chrome Privacy Statement further addresses that browsing history will be retained if a user is signed in to his or her Google account. The browsing history can be deleted using the My Activity section in the user's Google account. It also highlights the ability to search using Incognito mode.

Android: Information on how to clear history on an Android-based device is provided in the Google Help Center. Additionally, the center addresses how a user can delete search history saved while logged into via the My Activity section.

Table 3. Scoring Results for Search

OS	Notice of Data Collection	Choice to Opt-Out	View Collected Data	Delete Collected Data	Data Portability
Windows 10	●	●	●	●	●
Chrome OS	●	●	●	●	○
Android	●	●	●	●	○

Poor ○ ◔ ◑ ◕ ● *Excellent*

Browse

Windows 10: The Privacy Statement directs users, under the section "How to Access and Control Your Personal Data," to the Privacy Dashboard to control, view, and delete browsing data. It also includes a section advising the user how to turn off browser-based cookies for further privacy control. Browsing

data can be viewed on the Privacy Dashboard and cleared. It can also be downloaded in JSON format on the Activity History page.

Chrome OS: The *Google Product Privacy Guide* addresses how to view and delete browsing activities, and the Chrome Privacy Statement further addresses that browsing history will be retained if a user is signed in to his or her Google account. The browsing history can be deleted using the My Activity section in the user's Google account. It also highlights the ability to browsing using Incognito mode.

Android: Information on how to clear history on an Android-based device is provided in the Google Help Center. Additionally, the center addresses how a user can delete search history saved while logged into via the My Activity section.

Table 4. Scoring Results for Browse

OS	Notice of Data Collection	Choice to Opt-Out	View Collected Data	Delete Collected Data	Data Portability
Windows 10	●	●	●	●	●
Chrome OS	●	●	●	●	○
Android	●	●	●	●	○

Poor ○ ◔ ◑ ◕ ● *Excellent*

Speech, Inking, and Typing

Windows 10: Microsoft's Privacy Statement addresses how voice and speech data is collected through the use of various products with links to the Privacy Dashboard, where the user can learn more about options related to voice. Speech recognition that does not use the cloud-based engine is not retained; however, voice history that has been saved can be accessed, cleared, and downloaded in JSON or MPEG format on the Activity History page. The document "Speech, Inking, Typing and Privacy" further informs users of their options.

Chrome OS and Android: Information is provided in the March 2019 "Google Chrome Privacy Whitepaper" regarding information sent by Android to Google. It states, "Here we're focusing on the desktop version of Chrome; we touch only tangentially on Chrome OS." It does address the ability to opt in to the Google Assistant "Ok Google" feature if Voice and Audio is enabled under Data and Personalization in the user's Google account. The user also can see a list of their voice inputs and the date of recording. All recordings that are displayed deletion is possible. Android's statement regarding Chrome OS remains unclear.

Table 5. Scoring Results for Speech, Inking, and Typing

OS	Notice of Data Collection	Choice to Opt-Out	View Collected Data	Delete Collected Data	Data Portability
Windows 10	●	●	●	●	N/A
Chrome OS	◕	●	●	●	N/A
Android	●	●	●	●	N/A

Poor ○ ◔ ◑ ◕ ● *Excellent*

Applications/Activity History

Windows 10: Microsoft's Privacy Statement prominently addresses activity tracking and provides a link to more specific information in its "Windows 10 Activity History and Your Privacy" document. It provides specifics about how to manage activity history settings. Additionally, the Privacy Dashboard offers the ability to view and clear application history. Application usage history can be downloaded in JSON format on the Activity History page.

Chrome OS: Information about activity tracking is provided, and a toggle button enables the user to choose whether or not to include Chrome history and activities from sites and apps. Activity may be viewed and deleted on the Manage Activity page. (This is combined with web browsing activity, described earlier).

Android: Information regarding web and app activity can be controlled on the My Activity page. They are combined as "Websites and Apps You Use." This information is not saved unless the "Include Chrome history and activity from websites" button is selected.

Table 6. Scoring Results for Applications/Activity History

OS	Notice of Data Collection	Choice to Opt-Out	View Collected Data	Delete Collected Data	Data Portability
Windows 10	●	●	●	●	●
Chrome OS	●	●	●	●	○
Android	●	●	●	●	○

Poor ○ ◔ ◑ ◕ ● *Excellent*

Product and Service Performance/Diagnostics

Windows 10: Microsoft's Privacy Statement prominently informs the user of the diagnostic information that Microsoft collects. Substantial additional documentation is provided in the document "Diagnostics, Feedback and Privacy in Windows 10." Microsoft does not allow a user to opt out of basic diagnostic data collection, but the user does have the option of providing full diagnostic data to tailor their experience. Precise descriptions of the data collected under both categories are provided in the lengthy documents "Windows 10, 1809 Basic Level Windows Diagnostic Events and Fields" and "Windows 10,

version 1709 and New Diagnostic Data for the Full Level." Some "Product and Service Performance" data can be cleared (but not viewed) on the Privacy Dashboard. To view the diagnostic data, a Windows application for versions 1803 and 1809 is available—the Diagnostic Data Viewer.

Chrome OS: The March 12, 2019, Google Chrome Privacy Notice mentions usage and crash data with links to directions on how to turn off diagnostic and usage data. It states that crash reports will not "usually include" personal information but lists that the reports might include Chrome settings, locations where a user clicks, websites where speech was used instead of text, and personal information that might be included if Chrome crashes while a user is using it, "depending on what was happening at time of crash."

Android: Very limited information regarding diagnostic data is provided in any Google support document. There are instructions regarding how to turn off usage and diagnostics in the device settings; however, the limited examples of the types of diagnostics include battery level, how often an app is used, and network connectivity.

Table 7. Scoring Results for Product and Service Performance/Diagnostics

OS	Notice of Data Collection	Choice to Opt-Out	View Collected Data	Delete Collected Data	Data Portability
Windows 10	●	◕	◕	◕	N/A
Chrome OS	◕	○	○	○	N/A
Android	◔	●	○	○	N/A

Poor ○ ◔ ◑ ◕ ● *Excellent*

Application Access

Windows 10: Microsoft Windows 10 enables user control over whether or not an application may access location information via the privacy settings on the device. In the Privacy Dashboard, each application that is accessing a feature is listed. The document "Windows 10 and Your Online Services" has a link called "To see and control which of these apps have access to features like camera, microphone and location services, go to Settings > Privacy." The link goes to a new March 20, 2019, document called "Change Privacy Settings in Windows 10"; however, specific information regarding application access is not available.

Chrome OS: Information is provided in Google Chrome Help articles regarding how to turn camera and microphone settings off and on for particular applications.

Android: The support document "Control Your App Permissions" provides information regarding the features that can be accessed by applications if the user grants permissions. It also indicates that apps might seek access to other features, as well. App permissions can be turned on or off on the device in Application Manager. Further information, such as the list of features available to applications on an Android, was not easily found in the Google documentation.

Conclusions

Microsoft provides a significant amount of information to guide the user in awareness and usage of its privacy controls. With the trend to network more devices, as well as to enable cross-device information sync, this level of specific information regarding Windows 10 will enable a user to have a clear view of how the privacy policies and controls of the various elements will impact desired outcomes.

The Privacy Dashboard required logging in to learn more about the various options, as well as to access viewing and deleting options. To provide potential buyers or people without Microsoft accounts with the ability to learn as much as possible prior to purchasing a Windows 10–based product, extracting the nonconfidential information from behind the firewall of the log-in screen would be of value to the consumer.

Google appears to be launching a series of updated privacy documents, as evidenced by the recent Chrome Privacy Notice and "Chrome Privacy Whitepaper." This will be important for new and existing consumers, as the complexity among Chrome as a browser, Chrome OS as an operating system, and Android can be confusing. For instance, during the course of this study, the security page for Chrome indicated, under the Android heading, that a Chromebook was in use (which was being utilized at the time). Therefore, when discerning privacy controls "between" Android and Chrome OS, Google documentation does not provide the clarity or segmentation between the two environments.

As evident from the summary of scores across all categories of assessment in **Table 8**, Windows 10 scored higher than Google in all categories except for Notice of Data Collection for Chrome OS and Choice to Opt Out for Android, where all operating systems achieved parity. The most notable differences were observed in the Data Portability assessment category, in which Microsoft has the largest lead over Google.

Table 8. Cumulative Scoring Results for All Categories

OS	Notice of Data Collection	Choice to Opt-Out	View Collected Data	Delete Collected Data	Data Portability
Windows 10	●	●	●	●	●
Chrome OS	●	◕	◕	◕	◑
Android	◕	●	◕	◕	◑

Poor ○ ◔ ◑ ◕ ● *Excellent*

Based on our assessment, Windows 10 provides greater transparency and more granular controls than both Chrome OS and Android with respect to data privacy, especially as related to the collection and use of diagnostic data. Finding relevant information provided by Microsoft on the impact of the different privacy settings in Windows 10 on the user was less time-consuming, and the information presented was more concise and consistent than was the case for Google.