**Microsoft Company Overview:**

Microsoft is a technology company most famous for their personal computer operating systems. Founded in 1975 by Bill Gates and Paul Allen, the company has over 115,000 employees worldwide and made just under $96 billion of revenue in their 2015 fiscal year (Facts About Microsoft). The company made a name for itself in the 1980’s with the development of the MS-DOS operating system, which was followed by their Windows operating system shortly thereafter (Facts about Microsoft). The company went public in 1986 and is currently valued at $403.2 billion. It currently ranks 31st on the list of Fortune 500 companies (Fortune). Microsoft is based here in the Puget Sound, with the majority of their employees working out of the Microsoft campus in Redmond, WA.

The company is segmented by business functions and engineering groups. Business functions include: Business Development Group, Corporate, External, and Legal Affairs, Corporate Strategy & Planning, Finance Group, HR group, Marketing Group, and Operation. The Engineering Groups include: Applications and Services Engineering Group, Cloud and Enterprise Engineering Group, Windows and Devices Group, and Technology and Research (Facts About Microsoft).

In addition to the long line of Microsoft Windows operating systems for which the company is so famous, they branched out into hardware products in the early 2000’s with the development of the Xbox, the Windows line of mobile phones, and the Microsoft Surface tablet. Other software products include Skype (acquired in 2011) and cloud services. They also continued to update and improve their Microsoft Office Suite of applications, which includes the likes of Microsoft Word, PowerPoint, Excel, and Outlook. As of November of 2014, 1.5 billion people use a Microsoft Windows operating system every day and 1.2 billion people use Microsoft Office (Microsoft by the Numbers).

As our project is focused on the privacy policies behind Microsoft’s most recent version of their Windows operating system, Windows 10, it would be prudent to discuss the history and context of that project in further detail. Windows 10 was released in the summer of 2015 and given to users of Windows 8 as a free upgrade. According to Microsoft, Windows 10 was designed to run on all modern Windows devices including: Windows PC’s, tablets, phones, Window’s Internet of Things products, Microsoft Surface Hub, Xbox One, and Microsoft HoloLens (Myerson). It was also touted as being the “most secure platform ever, including Windows Defender for free anti-malware protection, and being the only platform with a commitment to deliver free ongoing security updates for the supported lifetime of the device” (Myerson). Microsoft announced that there were roughly 14 million downloads of Windows 10 in the first 24 hours after the new operating system was launched and one month later, it was estimated that between 50 and 67 million people were using the product (Wilson). The company’s ultimate goal is to have Windows 10 running on one billion devices within two to three years (Ralph).

**Summary of the information issue**

Microsoft Windows 10 has been in the eye of the storm of numerous protests for the manner in which personal information is gathered. Of course, Microsoft has been collecting personal data for years now, but since the introduction of Windows 10, a deluge of information has become available and accessible to the company. The timing could not have been more appropriate. At a juncture when Big Data has debuted on the business, science and administration scenes in an enormous way, Windows 10 seems poised to beat every information gathering agency hollow. With more than 200 million devices running Windows 10, Microsoft may well be the best information vendor of the decade. How all this information is used is not fully understood, except certain euphemistic explanations by the company (Microsoft Privacy Policy). Microsoft explains it ‘’will access, disclose and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive) when we have a good-faith belief that doing so is necessary to:

1. Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies;

2. Protect our customers, for example, to prevent spam or attempts to defraud users of the services, or to help prevent the loss of life or serious injury to anyone;

3. Operate and maintain the security of our services, including to prevent or stop an attack on our computer systems or networks; or protect the rights or property of Microsoft, including enforcing the terms governing the use of the services - however, if we receive information indicating that someone is using our services to traffic in stolen intellectual or physical property of Microsoft, we will not inspect a customer's private content ourselves, but we may refer the matter to law enforcement’’ (Microsoft Privacy Policy).

The company’s “good faith” has elicited mixed responses ranging from derisive to acquiescent, but most of it questions the need for gathering so many data. Moreover, the company makes no bones about the fact that third parties may make use of personal data made available to them as they feel fit. Ostensibly, Microsoft uses personal information such as location or your picture to improve the user experience. This may be acceptable because Android and iOS also do the same. However, Cortana, a new feature which serves as a personal assistant, demands an uncomfortable amount and range of information. Of course, one can always choose to not use it, but for the average user, it is difficult not to try out these brand new features.

Many have criticized the ‘opt-out’ instead of the ‘opt-in’ settings that do not always allow users to realize that they may be passing on important and very private information. Microsoft’s language in one or two settings is very vague, which means it’s hard to tell when it is or isn’t collecting data related to some settings. The “Getting to Know You” setting is particularly vague and problematic. Most casual users will never even look at these settings. It has led to major concerns regarding “keylogger” issues, that is, whether Microsoft gets hold of every word that is typed (Matthews). The clarification issued apparently denies anything of the sort, asserting that ‘typing and inking’ information is gathered merely in order to improve language by checking spelling and other errors, and to improve customer experience (Sarkar). Yet, niggling doubts still prevail over the vague language Microsoft uses. The company clarifies, “The data is put through rigorous, multi-pass scrubs to ensure it does not collect sensitive or identifiable fields (e.g., no email addresses, passwords, alphanumeric data, etc.). Data is also chopped into very small bits and stripped of sequence data so it cannot be put back together or identified. The data samplings collected are limited; Microsoft is not capturing everything you write, nor is it capturing data every time” (Gordon)**.** As mentioned earlier, the language leaves enough scope for multiple interpretations. In fact, even diagnostic data one sends can be used to access important information such as how long you spent on a particular web page or how often you use a particular app.

Windows 10 comes built in with a number of settings that can help one preserve privacy. For instance, one can turn off Cortana, or text prediction, reminiscent of Google Search. The most contentious, “Getting to know you” can also be turned off, as can the Cloud Info. But if you are very particular about sharing personal information, you will also have to disable Sync, which will sync all information on all your Windows 10 PCs. Yet, whatever you do, data is bound to go to Microsoft from Windows as the company claims that it is essential for consumer protection and of course, for advertising.

Windows has been into the business of data collection for two decades, then why is there so much outcry now? One of the main reasons for this is the impact of whistleblowers like Edward Snowden, Julian Assange, and Bradley Manning. Techtarget.com defines ‘The Snowden effect’ as “ the increase in public concern about information security and privacy resulting from disclosures that Edward Snowden made detailing the extent of the National Security Agency's (NSA) surveillance activities” (WhatIs). Citizens have become more concerned about how, when, and why their data is being collected by government or non-government agencies. Certain studies to measure the impact of Snowden revelations have been carried out. The Internet poll conducted by the Center for International Governance Innovation showed that 60 percent of respondents spanning across 24 countries knew about the Snowden revelations (Rouse).

Studies have been conducted to quantify some of the effects as indicated by changes since the Snowden revelations. An Internet poll conducted by the Center for International Governance Innovation showed across 24 countries that, overall, 60 percent of respondents were aware of Snowden. Germany was at the top with 94 percent. Sweden, Brazil, China and Hong Kong all were in the mid-to-low eighties. US and Canada were 76 percent and 64 percent respectively. The poll also showed changes in the behavior of people. 43 percent of the people participating in the poll said that they have grown more careful while surfing. Also, 49 percent of the respondents said that they change their passwords more often after knowing about Edward Snowden(Rouse). Thus, we can see that whistleblowers have brought a social and technological change that has completely transformed the ethical issue of data collection.

**Current Bibliography:**

Arce, Nicole. "Windows 10 Spies On You By Default: Here's How To Opt Out." Tech Times RSS. 2 Aug. 2015. Web. 13 Jan. 2016. <<http://www.techtimes.com/articles/73725/20150802/windows-10-spies-on-you-by-default-heres-how-to-opt-out.htm>>

Brandon, John. “Microsoft Responds to Windows 10 Privacy Policy Concerns.” Computerworld. 4 Aug. 2015. Web. 25 Jan. 2016.

<<http://www.computerworld.com/article/2956773/emerging-technology/microsoft-responds-to-windows-10-privacy-policy-concerns.html>>

Brown, Aaron. “It looks like Windows 10 is storing more data than first thought, and this is why.” Express. 7 Jan. 2016. Web. 18 Jan. 2016.

<<http://www.express.co.uk/life-style/science-technology/632080/Windows-10-Microsoft-Data-Collection-Statistics>>

Bright, P. “Microsoft has a new mission statement, and it’s basically the same as its old one.” Arstechnica. 25 Jun. 2015. Web. 21 Jan. 2016. <<http://arstechnica.com/information-technology/2015/06/microsoft-has-a-new-mission-statement-and-its-basically-the-same-as-its-old-one/>>

Burlacu, Alexandra. “Microsoft vs. Privacy: Windows 10's Controversial Tracking Tools Hitting Windows 7, 8.” TechTimes. 8 Sep. 2015. Web. 27 Jan. 2016.

<<http://www.techtimes.com/articles/82619/20150908/microsoft-vs-privacy-windows-10s-controversial-tracking-tools-hitting-windows-7-8.htm>>

CISO Office. "Privacy Brief: Opt In Versus Opt Out." *Office of the CISO*. Web. 25 Jan. 2016. <<http://ciso.washington.edu/resources/privacy-briefs/privacy-brief-opt-in/>>

Dent, Steven. "Microsoft Promises That Windows 10 Doesn't Violate Your Privacy." *Engadget*. 29 Sept. 2015. Web. 25 Jan. 2016. <<http://www.engadget.com/2015/09/29/microsoft-privacy-policy-statement/>>

Fortune. “Fortune 500.” Fortune.com. 31 Dec. 2015. Web. 23 Jan. 2016. <<http://fortune.com/fortune500/> >

Gordon, Whitson. “What Windows 10's "Privacy Nightmare" Settings Actually Do.” Lifehacker.com 05 Aug. 2015 26 Jan 2016.

<<http://lifehacker.com/what-windows-10s-privacy-nightmare-settings-actually-1722267229>>

Lopez, Napier. "Cortana Now Scans Your Email to Make Sure You Fulfill Your Commitments." *TNW Network All Stories RSS*. 25 Jan. 2016. Web. 25 Jan. 2016

Mathews, L. “Microsoft clears the air on Windows 10 “keylogger”” Geek.com. 7 Oct 2015. Web. 23 Jan. 2016. <<http://www.geek.com/microsoft/microsoft-clears-the-air-on-windows-10-keylogger-1606160/>>

Microsoft. 2015. “Privacy & Cookies.” October 2015. Web. 24 Jan 2016. <<https://www.microsoft.com/en-us/privacystatement/default.aspx?tduid=(d418114651157b54a9ffdcf0b582c0d1)(256380)(2459594)(TnL5HPStwNw-wNkBg.n0Ye2.LqLF5PzvRA)()>>

Microsoft. “Facts about Microsoft.” News.Microsoft.com. 2 Dec. 2015. Web. 23 Jan. 2016. <<http://news.microsoft.com/facts-about-microsoft/>>

Microsoft. “Microsoft by the Numbers.” News.Microsoft.com. 13 Nov. 2014. Web. 23 Jan. 2016. <<https://news.microsoft.com/bythenumbers/ms_numbers.pdf> >

Microsoft. "Microsoft Privacy Statement." Microsoft.com. 1 Oct. 2015. Web. 13 Jan. 2016. <<https://www.microsoft.com/en-us/privacystatement/default.aspx>>

Morey, T., Forbath, T., & Schoop, A. (2015). Customer Data: Designing For Transparency And Trust. Harvard Business Review, 93(5), 96-105.

Myerson, Terry. “Hello World: Windows 10 Available on July 29th.” Blog.Windows.com. 1 Jun. 2015. Web. 23 Jan. 2016.

<<https://blogs.windows.com/windowsexperience/2015/06/01/hello-world-windows-10-available-on-july-29/> >

Popa, B. “Microsoft Edge Sends Browsing History to Microsoft - How to Block It.” Softpedia. 2 Sep. 2015. Web. 26 Jan. 2016. <<http://news.softpedia.com/news/microsoft-edge-sends-browsing-history-to-microsoft-how-to-block-it-490684.shtml>>

Ralph, Nate. “Microsoft by the numbers: 110M Windows 10 users, 1B visitors to the Windows 10 app store.” CNet.com. 6 Oct. 2015. Web. 23 Jan. 2016. <<http://www.cnet.com/news/microsoft-by-the-numbers/> >

Sarkar, Samit. “How to stop Windows 10's prying eyes” Polygon.com 23 July 2015, 25 Jan 2016.

<<http://www.polygon.com/2015/7/31/9075531/windows-10-privacy-how-to>>

Sieber, T. “Is Microsoft Gathering Data From You in Windows 7 and 8?” Makeuseof. 8 Sep. 2015. Web. 23 Jan. 2016.  
<<http://www.makeuseof.com/tag/microsoft-gathering-data-windows-7-8/>.>

Sikes, J. “Upgrade Windows 10.” Walking Dead Forums. 9 Aug. 2015. Web. 22 Jan. 2016. <http://www.walkingdeadforums.com/forum/f97/upgrade-windows-10-a-138342.html. August 09>

Sultan, Owen. “Windows 10 Spying Controversy - Canadian Authorities Start Investigation.” HackRead.com. 11 Sep. 2015. Web. 27 Jan. 2016.

<<https://www.hackread.com/canada-looking-into-windows-10-spying/>>

Summers, Nick. "Torrent Tracker Bans Windows 10 over 'terrible Privacy Policy'" *Engadget*. 25 Aug. 2015. Web. 25 Jan. 2016. <<http://www.engadget.com/2015/08/24/torrent-trackers-ban-windows-10/>>

Thaler, Richard. “Opting-in vs. Opting-out.” The New York Times (Online). 26 Sept. 2009. Web. 25 Jan. 2016.

<<http://www.nytimes.com/2009/09/27/business/economy/27view.html?_r=0>>

Trent, R. “Microsoft is NOT Tracking Your Every Waking Moment with Windows 10*.*” WindowsIT Pro. 7 Oct 2014. Web. 23 January 2016. <<http://windowsitpro.com/windows-10/microsoft-not-tracking-your-every-waking-moment-windows-10>>

Rashid, F. 2015. “Windows 7, 8, and 10: Now all collecting user data for Microsoft.” 1 Sep. 2015. Web. 23 Jan. 2016. <<http://www.infoworld.com/article/2979054/windows-security/windows-7-8-10-now-all-collecting-user-data-for-microsoft.html>>

Rouse, M. “Snowden Effect.” Whatis.com. Oct. 2015 (Web). 20 Jan 2016.

<<http://whatis.techtarget.com/definition/Snowden-effect>>

Wilson, Mark. “How Many People are Using Windows 10?” BetaNews. Aug. 2015. Web. 23 Jan. 2016

<<http://betanews.com/2015/08/20/how-many-people-are-using-windows-10-watch-real-time-stats/> >

Wilson, Mark. 2016. “If you're fine with Microsoft's approach to privacy in Windows 10, you're out of touch.” BetaNews. Jan 2016. Web. 20 January 2016. <http://betanews.com/2016/01/08/if-youre-fine-with-microsofts-approach-to-privacy-in-windows-10-youre-out-of-touch/>.

Write, Mic. "The Windows 10 Privacy Issues You Should Know about." *TNW Network All Stories RSS*. 29 July 2015. Web. 25 Jan. 2016. <<http://thenextweb.com/microsoft/2015/07/29/wind-nos/>>