12-2022

Watching the Watchmen: An Ethical Evaluation of the Behavior of Modern Software Applications

Joshua Graves
Northeastern Illinois University, jgraves@neiu.edu

WATCHING THE WATCHMEN:

An Ethical Evaluation of the Behavior of Modern Software Applications

A Thesis Presented to
the Faculty of the University Honors Program
Northeastern Illinois University

In Partial Fulfillment of the Requirements
of the NEIU Honors Program
for Graduation with Honors

Joshua Graves
December 2022

HONORS SENIOR PROJECT

ACCEPTANCE AND APPROVAL FORM

Joshua Graves

Watching the Watchmen: An Ethical Evaluation of the Behavior of Modem Software Applications

This senior project has been reviewed by the faculty of the NEIU Honors Program and is found to be in good order in content, style, and mechanical accuracy. It is accepted in partial fulfillment of the requirements of the NEIU Honors Program and graduation with honors.

Peter Kwasniewski 11/28/22

Faculty Advisor Date

Rouniana Stankova 11.28.2

Faculty Reader Date

Denise Cloonan Cortez 01-05-2023

Honors Curriculum & Standards Board Date

Jon Hageman 11 Jan 2023

Coordinator, University Honors Program Date

ABSTRACT

Software has become a ubiquitous element of modern life around the world. An unprecedented amount of power is bestowed upon the companies that own and operate that software. The obvious question arises: “Do these companies operate in an ethical manner regarding their software?” We derive an ethical code via synthesizing the ethical codes of both the IEEE and the ACM, disregarding principles that cannot be examined by an outside observer. We utilize this ethical code to examine five leaders in the software industry, namely Facebook, Google, Microsoft, Twitter, and Amazon. For each company, we examine four incidents in which they had the opportunity to either adhere to or disregard ethical practices. We then tabulate and analyze the data, noting common trends and outstanding results. From this analysis, we conclude that the majority of the companies act in an ethical manner, but improvements must be made in the management of user information to keep what should be confidential information confidential, and to mitigate harm caused by breaches of that confidential information more effectively.

TABLE OF CONTENTS

LIST OF FIGURES

INTRODUCTION

It is nigh-impossible to engage with the modern world without the use of modern technology. As the invention of the printing press introduced the idea of widespread literacy, and thus the infinite capabilities of reading, the invention of user-friendly software has introduced the general population to entirely new avenues for all things. One can communicate with individuals across the planet in real time, translate the greatest works written in a foreign language, operate their own thermostat, and order whatever item may catch their fancy for delivery within hours, all from the comfort of their own room through the help of devices utilizing modern software. Software that is younger than the majority of the Earth's population. Software that defines a new frontier for an industry, and brings with it all of the highs and lows that a new frontier represents.

As the Industrial Revolution exposed, rampant progress brings about new practices that have developed so quickly as to run amok unchecked. Workers have never been so exploited as they were in that era, and there are obvious fears that the software revolution that has been ongoing ever since the turn of the millennium carries with it that same spirit of exploitation, this time turned on the clients and end-users.

This study examines particular instances wherein prolific software companies were given the opportunity to act in an ethical manner. For each instance we determine whether the companies adhered to or disregarded the ethics outlined in Figure 1.

LITERATURE REVIEW

As the intention of this research is to determine the ethical standing of commonly used software applications and their intended purposes, it is imperative that a specific code of ethics that can be broken or adhered to is defined. Using the codes employed by different reputable software engineering organizations, such as the Institute of Electrical and Electronic Engineers (IEEE) and the Association of Computing Machinery (ACM), a concise definition of ethical behavior for the purposes of this study can be created.

Following the definition of an ethical code, it is imperative to outline particular cases and technologies that will be examined. For the software being examined we examine (1) its storage of private user data for profiling and marketing purposes, (2) the effects of that software on people, and (3) its intended uses. These aspects will be extrapolated on in the Uses section of this study. How secure the software is in protecting its users' sensitive information from prying eyes, and what the software's intentions were in development will be the primary focus of the Software Development section.

Ethics

Like most trades and crafts that came long before it, software engineering possesses a code of ethics followed by many within the field. In fact, it sports several different codes, each from different organizations. The IEEE, one of the premier organizations of technical professionals, sports three core tenets, each with their own further values. They are as follows [1]:

1. To uphold the highest standards of integrity, responsible behavior, and ethical conduct in professional activities.
2. To treat all persons fairly and with respect, to avoid harassment or discrimination, and to avoid injuring others.
3. To strive to ensure this code is upheld by colleagues and coworkers.

The ACM has a much more detailed code [2] that explains its core beliefs in a much more intricate manner. The four categories of the ACM code of ethics are:

1. General ethical principles.
2. Professional responsibility.
3. Professional leadership principles.
4. Compliance with the code.

Each of these categories, with the exception of the fourth, contains principles that shall be incorporated into the definition of ethical behavior as defined by this study.

Through the synthesis of these two organizations' beliefs, this study arrives at the following ethical code, to be adhered to hereafter:

1. Act primarily with the public good in mind.
2. Avoid any harm that could befall the users of the software.
3. Respect user privacy.
4. Protect confidential information to the best of the available capabilities.
5. Act with a user's private information only in manners authorized by that user.

Figure 1: Categories of Ethical Behavior in Software Engineering

Because of its inclusion in the ethical code, the definition of private information must be clarified, alongside its counterparts: personal information and confidential information. Confidential information, for the purposes of this study, shall refer to information known to the user, the software they interact with, and any necessary parties that the software acts as an intermediary for. For example, a user's address, when given to an online storefront that hosts independent sellers, must be given to the seller, and constitutes confidential information. Personal information is information that could identify the user. Information such as names, email addresses, and phone numbers generally fall under this category. Lastly, private information is information given to the software by the user, without intending for that information to be used. Recovery emails and two-factor authentication tools fall under this category.

Other aspects that would be worth considering would be the adherence to the requirements of their employers and clients. However, this is not a practical undertaking, as it would involve the details of trade secrets unlikely to be divulged by any parties interviewed, or in the case of open-source projects to be examined, is completely impossible.

Software Development

In the article, *Ethics is a software design concern* [3], Ipek Ozkaya explains that the design of software itself is of concern in regards to ethics. Citing concerns with the progression of the prevalence of the internet in modern everyday life, Ozkaya likens the development of architecturally unsound software—software possessing critical vulnerabilities—to the construction of an architecturally unsound building; the consequences of that poor design fall on the users. The danger that deploying such

software poses to the general user would violate ethical principles.

An example of the results of such an insecurity would be data breaches. The Yahoo! data breach [4] that occurred in 2013 is the pinnacle of unethical behavior in software engineering. Personal information, including usernames passwords, dates of birth and phone numbers were included in the hack. Yahoo! became aware of the breach in 2016, years after the information had already begun being sold, did not disclose what data exactly was being distributed, and a year later, in 2017, they revealed that every Yahoo! account at the time was included in the hack.

For our consideration, unethical software development is an unethical reaction from the developers, upon being made aware of unintentional violations of the code of ethics. In contrast, unethical software usage entails the intentional disregard of the code of ethics when utilizing the software.

Uses

In contrast to developmentally unethical software, software that is unethical by its usage must be intentionally utilized in an unethical manner. The most obvious example of this is ransomware—software designed to restrict access to something on a device unless certain demands are met. However, malware and other Blackhat [5] activities (e.g., keylogging, spyware) are clear violations of general ethics and the law, as they represent acts such as theft or the destruction of private property.

This research seeks to examine software that end-users, the typically less technologically inclined population when compared to developers, intentionally use. As such, a more fitting example to examine would be online profiling software. Facebook [6], for example, keeps permanent logs of every account creation and deletion, every advertisement the user interacts with, every contact the user has ever

made Facebook aware of, and more. This information was stored with the intent to sell the information to advertising companies, which would then use it to target individuals with advertisements tailored to that particular user.

On the face of it, this may not appear to be a violation of any particular ethical principal, sans that of the respect for user privacy, which the user abdicates through agreeing to the terms of service. However, these individuals' profiles are shockingly accurate, and in theory, any entity capable of purchasing the information contained in them is capable of doing anything they wish to with it. A study [7] conducted by Ullah et al, which described how a targeted advertisement could be created, also explains that a bad actor could easily use the information to fool someone into some course of action.

METHODOLOGY

Data Collection

We consider four incidents in which each company was given the opportunity to employ the ethical code established by this study. Each incident represents a potential five points, representing adherence to each ethical principle outlined in Figure 1. These incidents are then weighed on their violation of or adherence to the ethical code. For every infraction, a single point was deducted. For every non-infraction, no points were deducted. Four incidents were examined per company, to reduce the possibility of score inflation via any company having a smaller or greater pool of opportunities. Each company begins with a total of 20 points, corresponding to the number of incidents and the maximum number of adherences to the code of ethics (Figure 1) possible.

The incidents chosen were chosen on the basis that they possess some quality that pertains to the ethical code, in order to keep all of the information relevant to this study's focus.

Analysis

Once the total scores for each incident were examined for each company, they were tabulated and analyzed by the categories defined in Figure 1 to compare and contrast the different companies and to note trends in behavior amongst them. We noted areas of issue alongside their most likely causes.

RESEARCH

Given the defined criteria for ethical behavior, shown in Figure 1, the past incidents of threats to user privacy, and therefore potential unethical behavior, can be examined and judged accordingly. Each incident will be compared to each of the five ethical standards, and every infraction will result in the deduction of one point from the final score of a given individual's ethical rating.

Facebook

Meta, the company formerly and colloquially known as Facebook, is one of the leading forces in social media. As the parent company of Facebook, Instagram, and WhatsApp, millions utilize Meta's infrastructure to communicate with friends, family, and even strangers. As a result, it is a massive target for would-be hackers and organizations that wish to harvest data for whatever purposes. Throughout its lifespan, Facebook has been the victim of many breaches, totaling approximately 18 of note as of October 2022. For the purposes of this study, we examine only 4 breaches, as they

offer sufficient perspective into the successes and shortcomings of Facebook's abilities and to protect users' confidential information.

Forced Conversion of User Profiles from Private to Public:

In 2009, while undergoing changes from a platform primarily intended for individuals to interact with their local peers into one in the general shape of the monolithic corporation we know today, Facebook changed user profile defaults to share with the broad Facebook community. These settings allowed for an individual's posts to be visible on search engines and available to anyone capable of finding their profile.

1. *Act Primarily with The Public Good in Mind* – Facebook did not intend to directly harm its users, but negligence of how actions can affect others is not an excuse for if those actions negatively affect them. A point was deducted from Facebook for this infraction.
2. *Avoid Any Harm That Could Befall the Users* – Simply not converting user profiles would have circumvented any privacy concerns; unfortunately, Facebook chose the opposite approach. A point was deducted from Facebook for this infraction.
3. *Respect User Privacy* –Users could change their profiles back to private if they chose, but neglecting to do so left their profile exposed. Any private profile was, until reverted back by its owner, visible to any interested party. A point was deducted from Facebook for this infraction.
4. *Protect Confidential Information to the Best of The Available Capabilities* – Any confidential information posted on an account that did not permit the

public availability of its information was no longer confidential. A point was deducted from Facebook for this infraction.

5. *Act With a User's Private Information Only In A Manner Permitted By The User* – Facebook changed users' privacy settings without their requesting they be changed. A point was deducted from Facebook for this infraction.

Shared Data with Advertisers, Including Users' Names, Locations, and When They Clicked on Ads [10]:

In 2010, it was discovered that Facebook was sharing usernames and internal user IDs with advertisers. Facebook claimed this was accidental. The information provided could easily be used to identify which individual user was interacting with a particular advertisement, and that identification could be used to gather sensitive data through unintended access and awareness of the user's profile. Facebook remedied this issue almost immediately after the Wall Street Journal sought their opinion on the matter.

1. *Act Primarily with The Public Good in Mind* – While the sharing of user information with those it was not intended for is an issue, due to the fact that this sharing of data was unintentional, a point was not deducted against Facebook for this infraction.
2. *Avoid Any Harm That Could Befall the Users* – Failure to protect the users of a software service is failing to avoid harm that could befall those users. This issue was caused due to Facebook's error in design; a released product with a security flaw. A point was deducted against Facebook for this infraction.
3. *Respect User Privacy* – Facebook shared user data with unauthorized entities. A point was deducted against Facebook for this infraction.

4. *Protect Confidential Information to the Best of The Available Capabilities* – The user data that was made available to the advertisers should have been considered confidential. In other words, only available to select individuals: the user, those the user themselves authorized with that data, and Facebook, which requires access to that data. Because they remedied the issue after being made aware of it, no point was deducted, as although they pushed out a faulty service and released confidential data, they did attempt to protect that data in the future.
5. *Act With a User's Private Information Only in A Manner Permitted by The User* – The user did not explicitly or implicitly consent to the sharing of any information with the advertisers. A point was deducted against Facebook for this infraction.

The Cambridge Analytica Scandal [11]:

In 2016, a political consulting firm known as Cambridge Analytica was found to be utilizing a massive dataset that they had purchased from a researcher at the University of Cambridge for the purpose of targeted political advertisements towards those profiled through the data. The data originated from a feature of Facebook's API that allowed for a third-party application to retrieve data from the friends of the users that interacted with the third-party application, with neither their knowledge or consent. While Facebook patched this feature out in 2015, and forbid the sale of any data gathered through this process in their Terms of Service, they tacitly approved of that behavior through inaction, as that data was utilized to create ads on Facebook's own platform. Facebook never notified any users of anything regarding this incident until news outlets began reporting on it.

1. *Act Primarily with The Public Good in* Mind – Facebook's failure to notify users about anything regarding the scandal, from the initial bug to its patching, or the sale of the data, or the fact that the political ads were heavily profiled and targeted, is definitively for the benefit of Facebook and to the detriment of the public. A point was deducted against Facebook for this infraction.
2. *Avoid Any Harm That Could Befall the Users* – Facebook's refusal to take action to inform users of the data's collection and usage prior to being outed by the media, and also allowing the bug to persist for several years under fairly loose usage conditions is strictly not avoiding harm. A point was deducted against Facebook for this infraction.
3. *Respect User Privacy* – By allowing this bug to persist in their API for any extended period of time, user privacy was completely disregarded and circumvented by third party developers. A point was deducted from Facebook for this infraction.
4. *Protect Confidential Information to the Best of The Available Capabilities* – Facebook noticed this issue in their API years prior to fixing it, and did nothing to prevent the sale of the information that would later be used by Cambridge Analytica, in spite of it being against Facebook's terms of service to sell the data in the first place. A point was deducted from Facebook for this infraction.
5. *Act With a User's Private Information Only in A Manner Permitted by The User* – The users never permitted Facebook to hand the advertisers their data, and Facebook never technically permitted the data to be collected on friends of users that interacted with the third-party application. A point was deducted from Facebook for this infraction.

Sold User Data to Companies Like Netflix and Spotify [12]:

In 2018, it was discovered that Facebook had been selling user data to other large tech companies. It provided information to these companies on a case-by-case basis, with Netflix and Spotify being allowed to read private messages between users, Microsoft being allowed to see the names of all of a user's friends through Bing, and Amazon to learn users' names and contact information through their friends. Facebook neglected to disclose that these companies would be using this information to their users.

1. *Act Primarily with The Public Good in Mind* – Selling user data to other individual companies does not benefit the public good; especially if it's information that a user might not want to share with these particular companies. A point was deducted from Facebook for this infraction.
2. *Avoid Any Harm That Could Befall the Users* – Placing data in the hands of extra unintended recipients opens up the opportunity for that data to be retrieved and intercepted by more sources than intended. This creates opportunities for harm where they otherwise would not exist. A point was deducted from Facebook for this infraction.
3. *Respect User Privacy* – Information the user did not provide was supplied to organizations the user did not explicitly authorize to use that information. A point was deducted from Facebook for this infraction.
4. *Protect Confidential Information to the Best of The Available Capabilities* – The confidential information in this case was not leaked or breached; it was given away. As a result, it was technically protected. No points were deducted for this infraction.

5. *Act With a User's Private Information Only in A Manner Permitted by The User* – No users were made aware of this process until the media reported on it. A point was deducted from Facebook for this infraction.

Google

Google is perhaps the most pervasive software company of them all. The Google search engine practically defines the public internet. Google Images is a best-in-class image-based search engine, Google Maps is one of the most thorough and implemented displays of maps around the world, Google Mail is an extremely popular email service, and YouTube is the most popular video hosting website worldwide. This is to say nothing of their now defunct services; the cloud gaming service Google Stadia, and the full social media platform Google+. The Android operating system, which occupies approximately 80% of the mobile phone operating system market share, is also developed by Google. Many websites earn revenue through Google Ad-Sense. Avoiding the company while using the modern internet is nigh-impossible. Consequently, any breach of user privacy related to Google has the potential to tell anything about those users. This study observed 4 breaches of user privacy related to Google and its many services, and assessed them according to the ethical code.

Malware Available Through the Google Play Store Infected Anywhere Between 200,000 and 1,000,000 Accounts [13]:

In 2015, an application called BrainTest, available through the Google Play Store, was discovered to be infecting devices it was installed into with rootkit malware. It prevented its own removal from the device through various watchdogs — code that ensures that certain criteria are met and acts in the event that they are.

Estimates for the number of devices infected range from 200,000 to 1,000,000 different devices. Google removed the application from the Play Store after being made aware of its true purpose.

1. *Act Primarily with The Public Good in Mind* – The Google Play store exists to serve Android users with high-quality applications; technically any Android application can be installed without going through the Google Play Store, and therefore the Google Play Store conveys an air of quality to the applications it hosts. By not properly vetting the applications that would be hosted on their Store, Google has acted contrarily to the public good, and a point was deducted from Google for this infraction.
2. *Avoid Any Harm That Could Befall the Users* – A proper vetting system would have been the preventative measure necessary to prevent harm; however, one as not in place. A point was deducted from Google for this infraction.
3. *Respect User Privacy* – While the fact that this malware made its way onto people's devices through Google's service is indeed negative, the fact that Google did nothing to prevent or monitor the download of an application, despite its danger to the user, is an act of respecting user privacy. No points were deducted from Google for this infraction.
4. *Protect Confidential Information to the Best of The Available Capabilities* – Google never supplied any confidential information, either intentionally or not, to the hacker. No points were deducted from Google due to lack of an infraction.

5. *Act With a User's Private Information Only in A Manner Permitted by The User* – Google never utilized user data in relation to this incident. No points were deducted from Google due to lack of an infraction.

Google+ Bug Made It Possible For Third Party Developers To View Private User Data [14]:

Similarly to Facebook, Google+—Google's now defunct social media platform—possessed a glitch in the permissions it made available to third party developers: if a user interacted with a third-party application, the developer of that application would also be able to retrieve the information of any friends of that user, so long as that friend had their account information visible to friends. Google suppressed any knowledge of this bug, as they became aware of it in 2018 while the Cambridge Analytica scandal was ongoing, and after being made aware of it, opted to terminate Google+. An estimated 500,000 accounts were affected.

1. *Act Primarily with The Public Good in Mind* – Google suppressed the knowledge of the bug due to the ongoing Facebook-Cambridge Analytica scandal, they did seek to immediately rectify this quietly, and informed users after the fact after finding no evidence of misuse, but a notification to those affected users would have been the right step to take for the sake of the public good. A point was deducted for this infraction.
2. *Avoid Any Harm That Could Befall the Users* – Google disabled all consumer functionality of Google+ to prevent this vulnerability from being utilized after discovering it. They also ensured that no data had been actually leaked anywhere. No points were deducted due to lack of infraction.

3. *Respect User Privacy* – The decision to publicly acknowledge the issue after assessing that there was no breach of user privacy is in Google's favor, alongside the fact that no data was actually breached. No points were deducted due to lack of infraction.
4. *Protect Confidential Information to the Best of The Available Capabilities* – The information, as far as Google is aware and has made public that they are aware of, was all kept confidential. No points were deducted due to lack of infraction.
5. *Act With a User's Private Information Only in A Manner Permitted by The User* – No user information was actually utilized by Google in this incident. No points were deducted due to lack of infraction.

Google Would Track User Locations Despite Users Disabling Location Tracking [15]:

Google offers a setting through which users can opt into location services on their Google accounts. In 2018, it was revealed that, even on accounts that had this setting disabled, Google would track users through certain app activities; storing snapshots of a user's current location for things like weather services, Google Maps navigation, and more. Google claimed that this was clearly conveyed, and that users could in fact shut down this tracking through the "web and app activity" setting.

1. *Act Primarily with The Public Good in Mind* – There is nothing good that can come from duplicitously gathering data on individuals against their wishes. A point was deducted from Google for this infraction.
2. *Avoid Any Harm That Could Befall the Users* – Because the data was kept internal at Google, technically speaking the users were in no harm that they

didn't place themselves in by using Google's services. No points were deducted due to lack of infraction.

3. *Respect User Privacy* – Circumventing a user's chosen privacy settings against their wishes is an absolute violation of user privacy. A point was deducted from Google for this infraction.
4. *Protect Confidential Information to the Best of The Available Capabilities* – In this particular case, the confidential information was gathered by Google themselves; if a user chooses to disable location tracking, then their location should be considered confidential. A point was deducted from Google for this infraction.
5. *Act With a User's Private Information Only in A Manner Permitted by The* User – Google was tracking users' locations despite their disabling of the labeled Location Services. A point was deducted from Google for this infraction.

Google Allegedly Gathered and Collected User Data from Minors [16]:

In 2019, Google was accused of gathering data on minors via the YouTube Kids service, a version of YouTube that is intended to only include content suitable for children. The data was gathered for the purpose of targeted advertising, as YouTube's purpose for gathering information typically is. This violates the United States' Children's Online Privacy Protection Act (COPPA). Google agreed to pay a $170 million dollar settlement, vowing to change their practices by cracking down on the detection of content intended for children.

1. *Act Primarily with The Public Good in Mind* – Gathering user data allows Google to improve their service, but that is acting with Google's benefit in

mind; better product means more users, and that means greater profit for Google. A point was deducted from Google for this infraction.

2. *Avoid Any Harm That Could Befall the Users* – No measurable harm came about or could reasonably come about and be linked back to Google's information collecting in this case. No points were deducted due to lack of infraction.
3. *Respect User Privacy* – Google violated both user privacy and United States federal law regarding the privacy of minors. A point was deducted from Google for this infraction.
4. *Protect Confidential Information to the Best of The Available* Capabilities – Minors' information is largely considered confidential in software development, both for legal and ethical reasons. Google's violation of this confidentiality did not protect that information, because it allowed it to be stored at all. A point was deducted from Google for this infraction.
5. *Act With a User's Private Information Only in A Manner Permitted by The User* – As the users in this case whose privacy was violated were minors, it falls on their parental figures to consent to the collection of their information; which Google never received. A point was deducted from Google for this infraction.

Microsoft

Microsoft is a technological giant. The developers of the Windows operating system, which holds the largest market share of all desktop operating systems by a wide margin. Windows has become the *de facto* operating system, as it also possesses the widest berth of available software applications compared to its alternatives, those

being MacOS and the plethora of Linux distributions. As a result, Microsoft is an old, respected, and foundational technological corporation. Breaches of Microsoft's security and customer information could, in a worst-case scenario, result in breaches of computers, corporations, and individuals around the world.

An Internet Explorer Flaw Gave Hackers Administrator Privileges on Private Websites [17]:

In 2010, a zero-day flaw in the newly released Internet Explorer 6 allowed for hackers to download malware to employee computers and steal information. Known victims included both Google and Adobe. Microsoft was aware of this flaw months prior, but had only scheduled to fix it months after it became known and had already been abused.

1. *Act Primarily with The Public Good in Mind* – Microsoft was aware of this bug prior and continued to release a version of Internet Explorer with this critical bug regardless, with no concern for their customers. A point was deducted from Microsoft for this infraction.
2. *Avoid Any Harm That Could Befall the Users* – Any harm could have been avoided if the release of Internet Explorer 6 was delayed while Microsoft worked to remedy this vulnerability. A point was deducted from Microsoft for this infraction.
3. *Respect User Privacy* – User privacy was never truly violated by or directly due to Microsoft; while bad actors did gain access to administrator privileges, nothing private was involved. No points were deducted due to lack of an infraction.

4. *Protect Confidential Information to the Best of The Available Capabilities* – By releasing Internet Explorer 6 while knowing this bug existed and what it could be used for, Microsoft failed to protect any information "to the best of the available capabilities". A point was deducted from Microsoft for this infraction.
5. *Act With a User's Private Information Only in A Manner Permitted by The User* – Microsoft never actually accessed any user information, and therefore could not have used it in an unauthorized way. No points were deducted due to lack of an infraction.

Approximately 3000 Xbox Live Users Had Private Information Leaked Online [18]:

In 2013, Microsoft hosted an Xbox Entertainment Awards poll, allowing users to vote on their favorite music, TV shows, games, and films of the year. It was discovered that submissions to the poll were published online, and it was possible for visitors to remove or edit existing entries. Submitters' names, gamer tags (online usernames for Xbox Live), email addresses, and birthdays were all made visible. This leak only effected Xbox Live users residing in the United Kingdom. Approximately 3000 accounts were exposed.

1. *Act Primarily with The Public Good in Mind* – The public good is a non-factor in this case. A simple publication setting error was the cause of this leak. No points were deducted due to lack of an infraction.
2. *Avoid Any Harm That Could Befall the Users* – Incompetence is not a valid reason for allowing harm to befall the users. A point was deducted from Microsoft due to this infraction.

3. *Respect User Privacy* – By publishing the information online rather than keeping it on some internal secure database, user privacy was not respected. A point was deducted from Microsoft due to this infraction.
4. *Protect Confidential Information to the Best of The Available Capabilities* – By keeping confidential user information on a website rather than an internal database, Microsoft failed to protect it to the best of their available capabilities. A point was deducted from Microsoft due to this infraction.
5. *Act With a User's Private Information Only in A Manner Permitted by The User* – While Microsoft did make the information public, they never acted with it in a manner that the user did not permit. Their storage of that information was authorized, it was the manner in which they stored it that caused an issue, no points were deducted from Microsoft due to lack of an infraction.

Over 500 million LinkedIn Accounts' User Information Was Scraped and Sold [19]:

In 2021 it was discovered that approximately 500 million LinkedIn profiles had had their information scraped from the website. A hacker had listed the data set for sale. The information was all publicly available, as it was listed on the victims' public LinkedIn profiles. It was also aggregated and combined with information taken from other sources. The information scraped from LinkedIn included account IDs, full names, email addresses, phone numbers, workplace information, genders, and links to other social media accounts tied to the users' LinkedIn profiles.

1. *Act Primarily with The Public Good in Mind* – Microsoft did not scrape this data, and therefore did not act for or against the public good. No point was deducted due to lack of an infraction.

2. *Avoid Any Harm That Could Befall the Users* – Microsoft never directly placed its users in harm's way. No points were deducted due to lack of an infraction.
3. *Respect User Privacy* – Microsoft themselves never directly utilized or accessed private user information. No points were deducted due to lack of an infraction.
4. *Protect Confidential Information to the Best of The Available Capabilities* – Microsoft could have put better stopgaps in place in order to prevent or mitigate web scraping, using many commonplace systems. A point was deducted from Microsoft for this infraction.
5. *Act With a User's Private Information Only In A Manner Permitted By The User* – Microsoft never acted in this scenario using private information. No points were deducted due to lack of an infraction.

A Microsoft Power Apps Setting Made Users' Company Data Public [20]:

Microsoft Power Apps is a platform that allows for companies to construct their own propriety applications, as well as share and store data. In 2021, it was discovered that a number of large corporations had failed to configure the applications made using Power Apps to make the information stored within their applications private. The information that was leaked as a result of this misconfiguration varied based on the type of company that fell victim to it, sometimes including information as sensitive and valuable as Social Security Numbers. Microsoft changed the default of the Power Apps privacy settings to make the information private following being made aware of this leak.

1. *Act Primarily with The Public Good in Mind* – Microsoft never acted in regards to this incident; it was a revelation of a policy/setting default. No points were deducted due to lack of an infraction.
2. *Avoid Any Harm That Could Befall the Users* – By setting the default privacy setting to public on a service designed for building private solutions for private enterprises, and excusing that behavior by stating that information about the setting is in the documentation, something end users are not particularly likely to read thoroughly if unnecessary, Microsoft made a decision that placed Power Apps users in unnecessary harm. A point was deducted from Microsoft due to this infraction.
3. *Respect User Privacy* – Microsoft did not publicize or interact with their clients' information despite this default setting. No points were deducted due to lack of an infraction.
4. *Protect Confidential Information to the Best of The Available Capabilities* – Permissions should always, by default, favor and protect the user's privacy whenever possible. Microsoft did not do this. A point was deducted from Microsoft for this infraction.
5. *Act With a User's Private Information Only in A Manner Permitted by The User* – Microsoft never utilized or had direct access to the private information of their clients. No points were deducted due to lack of an infraction.

Twitter

Twitter is one of the leading figures in social media. In 2022 it was purchased by Elon Musk for an estimated $44 billion. Nearly all individuals and publications of renown in the West are present on the platform, from politicians to celebrities to

fellow billion-dollar corporations like McDonald's and Coca-Cola. It is the most used social media platform for journalists, the third most used social media source for receiving news updates by adults behind Facebook and Google-owned YouTube [21], and is the second most used social media platform worldwide, behind only Facebook in this regard [22].

A Hacker Utilized a Brute-Force Password Guesser to Gain Access to A Twitter Administrator Account [23]:

In 2009, a hacker breached a Twitter administrator account using a brute-force password checker; it would randomly guess at passwords until it achieved a valid log-in. Modern systems have the ability to detect suspicious log-in activity, through location information on where the attempted log-in occurred, and the number of attempted log-ins. Using the administrator account, the hacker then compromised the accounts of multiple high-profile individuals.

1. *Act Primarily with The Public Good in Mind* – Twitter did not act in this event, and the unlimited password attempts could be viewed generously as being permissive towards their users. No points were deducted due to lack of an infraction.
2. *Avoid Any Harm That Could Befall the Users* – Even in the time that this hack occurred, barring accounts for suspicious log-in activity was a commonplace method of preventing brute-force password hacking. A point was deducted from Twitter for this infraction.
3. *Respect User Privacy* – Twitter never accessed user information in regards to this incident. No points were deducted due to lack of an infraction.

4. *Protect Confidential Information to the Best of The Available Capabilities* – Twitter's failure to implement proper password protection is a failure to protect confidential information. A point was deducted from Twitter for this infraction.
5. *Act With a User's Private Information Only in A Manner Permitted by The User* – Twitter never accessed user information in regards to this incident. No points were deducted due to lack of an infraction.

An Unspecified Bug Compromised 330 million User Passwords [24]:

In 2018, Twitter forced all users to change their passwords, after realizing there was an internal bug that left over 330 million user passwords exposed. They were being stored, unencrypted, within an internal log. Twitter stated the found no misuse of the information located in the log.

1. *Act Primarily with The Public Good in Mind* – Twitter forced all users to reset their passwords after being aware of the bug, and did not find any evidence that it had been misused. No points were deducted due to lack of an infraction.
2. *Avoid Any Harm That Could Befall the Users* – Twitter did its best to protect its users in this incident; only publicizing information about the bug after fixing it, and still mandating password changes after the fact. No points were deducted due to lack of an infraction.
3. *Respect User Privacy* – Twitter never accessed user information in regards to this incident. No points were deducted due to lack of an infraction.
4. *Protect Confidential Information to the Best of The Available Capabilities* – Twitter performed optimally in this incident; they caught the bug before it was made known to any bad actors, and still forced changes to user passwords so if

the bug was known to bad actors at all, the information obtained is now useless. No points were deducted due to lack of an infraction.

5. *Act With a User's Private Information Only in A Manner Permitted by The User* – Twitter never accessed user information in regards to this incident. No points were deducted due to lack of an infraction.

A Flaw In Twitter's Support Form Exposed Country Codes on Phone Numbers Associated With Accounts [25]:

In 2018 it was revealed that Twitter's support form had a bug that revealed the country code of the phone number associated with the account of whoever submitted one. Twitter was made aware of this bug in 2016, when a security researcher reached out to them regarding it, but dismissed the bug as a non-significant security risk. Twitter discovered that the bug may have been abused by both China and Saudi Arabia to scrape for users associated with particular locations.

1. *Act Primarily with The Public Good in Mind* – Twitter was aware of the flaw well before it became known to the public, and they had classified it as an insignificant issue. The well-being of the users is always the most pressing issue in terms of cybersecurity. A point was deducted from Twitter for this infraction.
2. *Avoid Any Harm That Could Befall the Users* – By not immediately fixing a privacy vulnerability as soon as they could, Twitter knowingly placed its users in harm's way. A point was deducted from Twitter for this infraction.
3. *Respect User Privacy* – Twitter did not directly violate user privacy in regards to this incident. No points were deducted due to lack of infraction.

4. *Protect Confidential Information to the Best of The Available Capabilities* – Choosing to not prevent the easy confirmation of a user's confidential location is not protecting their location to the best of the available capabilities. A point was deducted from Twitter for this infraction.
5. *Act With a User's Private Information Only in A Manner Permitted by The User* – Twitter never accessed the user's private data in regards to this incident. No points were deducted due to lack of infraction.

Twitter Accidentally Used Information Received for Two-Factor Authentication Purposes for Targeted Advertising [26]:

In 2019, Twitter revealed that the information given to them for the purposes of two-factor authentication was accidentally implemented in their "Tailored Audiences and Partner Audience" system, the designation for Twitter's targeted advertising system. The information being used included phone numbers and email addresses, which Twitter claims were matched against the marketing lists given to them by their prospective advertisers. Twitter came forward with this information three weeks after claiming to have prevented this unauthorized sharing of information.

1. *Act Primarily with The Public Good in Mind* – While this could be viewed as a mistake, Twitter knowingly designed their targeted advertising algorithms with the ability to harness the user's location and other private information. A point was deducted from Twitter for this infraction.
2. *Avoid Any Harm That Could Befall the Users* – The information, while it was used wrongly, was never in the hands of explicitly malicious entities. No points were deducted due to lack of infraction.

3. *Respect User Privacy* – Twitter gave away its users' private information for monetary gain. By Twitter's account it was accidental, but they still did so. A point was deducted from Twitter for this infraction.
4. *Protect Confidential Information to the Best of The Available Capabilities* – Designing the algorithm for targeted advertising without the necessary stopgaps to prevent it from accessing information distinctly marked as not to be given to Twitter and its advertisers is failing to protect that information. A point was deducted from Twitter for this infraction.
5. *Act With a User's Private Information Only in A Manner Permitted by The User* – Twitter handed the private information of its users to advertisers against their wishes. A point was deducted from Twitter for this infraction.

Amazon

Amazon is one of the most valuable companies in the world. Its very logo markets itself as the store that sells everything, from A-to-Z. It occupies a spot amongst the most influential and ubiquitous companies on Earth, boasting a number of subsidiaries that branch into nearly every conceivable field. Amazon Web Services is utilized across the internet for cloud computing. Twitch is the premier streaming platform. Whole Foods is a renowned organic grocer. But this goliath of a corporation's sheer size leaves it open to some of the most dangerous of attacks.

As of 2016, It Was Possible for Virtually Any Amazon Customer Service Employee to View Any Amazon Customer's Data [27]:

As an incredibly large company, Amazon has a number of different departments to cater to its different clientele. The inner workings of the mega-

corporation possess an element of obfuscation purely because finding any particular user's information, theoretically, would require knowledge of exactly where you want to look for it and exactly how to find it. However, as an Amazon employee, it was indeed possible to merely request to see the information of any particular user, and be given that privilege.

1. *Act Primarily with The Public Good in Mind* – While this is a definite security hazard, Amazon likely did this for a more efficient customer service. No points were deducted due to lack of infraction.
2. *Avoid Any Harm That Could Befall the Users* – Insider attacks are always a meaningful threat, and handing out all data to any individual that might remotely need it is practically asking for that information to be mishandled. A point was deducted from Amazon for this infraction.
3. *Respect User Privacy* – While the information was kept internally, it should only be visible to those that absolutely need to see it, and only when they need to see it. A point was deducted from Amazon for this infraction.
4. *Protect Confidential Information to the Best of The Available Capabilities* – The information was kept internally, and while it was given to far too many that did not explicitly require it, it was still kept internal. No points were deducted due to lack of infraction.
5. *Act With a User's Private Information Only in A Manner Permitted by The User* – The information was, in this incident, not explicitly utilized in any way; merely visible to those it should not have been visible to. No points were deducted due to lack of infraction.

A Hacker Posted Thousands of Kindle Accounts and Their Information [28]:

In 2016, a hacker posted a list of Amazon customer accounts, which reportedly included emails, passwords, location information, phone numbers, and more. The hacker requested $700, and when Amazon failed to comply, he posted the information. While a cybersecurity professional claimed that the information indeed looked legitimate, the passwords appeared to be encrypted, and the hacker claims that Amazon disabled all of the accounts after the leak was posted.

1. *Act Primarily with The Public Good in Mind* – Amazon, according to the hacker, deactivated all of the potentially effected accounts listed in the leak. No points were deducted due to lack of infraction.
2. *Avoid Any Harm That Could Befall the Users* – Amazon quickly discounted the veracity of the leak, before quietly deactivating the accounts. This may have been a tactic to get would-be malicious entities to ignore the leak while they dealt with it behind closed doors, but ultimately, as nothing came of the leak, it can be assumed that Amazon's strategy was effective. No points were deducted due to lack of infraction.
3. *Respect User Privacy* – Amazon did not invade or violate user privacy in regards to this incident. No points were deducted due to lack of infraction.
4. *Protect Confidential Information to the Best of The Available* Capabilities – None of the confidential information in the leak was ever, at least prolifically, utilized, and Amazon denies that there was a real leak to begin with. Even without a generous view on the situation, if Amazon did indeed deactivate all of the accounts, then they have protected those users' finances. No points were deducted due to lack of an infraction.

5. *Act With a User's Private Information Only in A Manner Permitted by The User* – Amazon did not utilize their customers' information in regards to this incident. No points were deducted due to lack of infraction.

A Third Party, AMZReview, Through Aggregation of Reviews and Seller-only Information, Compiled and Released Customer Data [27]:

In 2018, Amazon discovered the existence of the third-party website, AMZReview, which claimed to offer optimization tactics to Amazon sellers; that it would help to boost their Amazon seller rankings. In reality, AMZReview had compiled the information that Amazon would give to its sellers upon request in the hopes that they would analyze it internally and improve, and cross-referenced that information with information obtained from other websites. The result was a stockpile of names, mailing addresses, order histories, phone numbers, and even personal email addresses. AMZReview claimed to hold information on 16 million users, while Amazon confirmed approximately 4.8 million. Amazon audited all companies they had known to have abused their liberal dissemination of information, and now limits the information a seller may obtain significantly more.

1. *Act Primarily with The Public Good in Mind* – Amazon's offer to help sellers was with the best of intentions, but freely giving away user information simply on request with only good faith to assert that it will not be mishandled is not in favor of the public good. A point was deducted from Amazon for this infraction.
2. *Avoid Any Harm That Could Befall the Users* – Amazon handed out sensitive information to anyone that asked. A point was deducted from Amazon for this infraction.

3. *Respect User Privacy* – Amazon liberally disseminated user information, without the explicit consent of the user in any instance. A point was deducted from Amazon for this infraction.
4. *Protect Confidential Information to the Best of The Available Capabilities* – Supplying important information about their users without proper regard for how it could be used is not protection. A point was deducted from Amazon for this infraction.
5. *Act With a User's Private Information Only in A Manner Permitted by The User* – The information Amazon gave away was all relevant information to a seller that needs to send an item to a customer, While the companies that received that information used it without regard for the customer's wishes, Amazon only acted as they were authorized to. No points were deducted due to lack of infraction.

Amazon Employees Took Bribes in Exchange for Sabotaging a Seller's Competitors [27]:

In 2017, a seller had realized that an independent Amazon seller had begun selling a lower quality version of a product she had developed herself, mimicking her listing and even utilizing her original listing's photos. She was issued fraudulent copyright claims from strange sellers, and her account was suspended. Upon having it reinstated, her payments would occasionally find themselves sent to the competitor's account, and occasionally her customers would receive her competitor's product. This specific competitor, Krasr, had acted using this very same strategy before, and had been able to do so due to bribing insider Amazon employees. Krasr could bribe them to reinstate violating accounts and suspend legitimate ones, to send private Amazon

information on trending and popular products, and even customer information so that Krasr could attempt to bribe them to remove bad reviews.

1. *Act Primarily with The Public Good in Mind* – Taking a bribe in order to sabotage a legitimate salesperson is not in the public good's best interests, and actively harms smaller sellers. A point was deducted from Amazon for this infraction.
2. *Avoid Any Harm That Could Befall the Users* – The lack of a system in place to prevent the abuse of an insider on Amazon's storefront is a failure to avoid harm. A point was deducted from Amazon for this infraction.
3. *Respect User Privacy* – User information was never at stake or in use in regards to this incident. No points were deducted due to lack of infraction.
4. *Protect Confidential Information to the Best of The Available Capabilities* – The sabotage did not involve sellers' confidential information, only their public store. No points were deducted due to lack of infraction.
5. *Act With a User's Private Information Only in A Manner Permitted by The User* – Users were not impacted by Amazon in any way not in alignment with Amazon's typical user interaction. These typical methods were exploited, but they were still typical. No points were deducted due to lack of infraction.

RESULTS

The results of the ethical evaluation are detailed below, categorized by the ethical standards detailed in figure 1 (Public Good, Avoid Harm, Respect Privacy, Protect Confidential Information, Act as Authorized). The "Ethical Average" category in the following figures indicates achieving at least 50% of the available points, and therefore the standard expected to be reached by the companies being examined.

Public Good

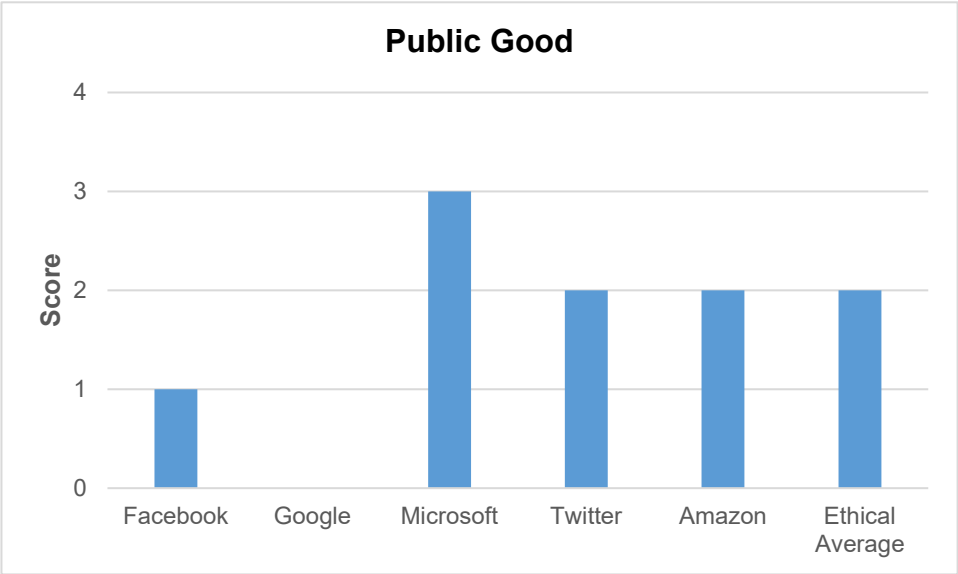

Figure 2: Comparison of the Infractions Against The Public Good

The only company that exceeded the Ethical Average in this category was Microsoft, which only received one infraction in the Public Good category. Google failed to avoid a single infraction in this category and thus had all four of its points deducted, while Facebook skirted by with a single point. Twitter and Amazon both met the average.

Avoid Harm

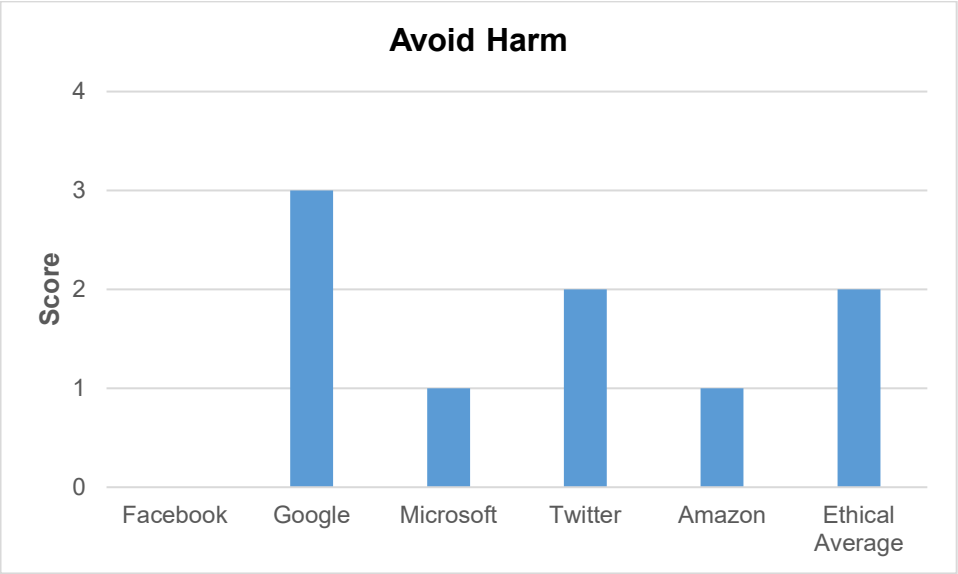

Figure 3: Comparison of the Infractions Against Avoiding Harm

In this category, the only company that exceeded the Ethical Average was Google. Twitter met the Average, while Microsoft, Amazon, and Facebook all failed to even meet the Ethical Standard. The latter of the three also failed to avoid any infractions in this category. This is the category in which the companies collectively performed the worst, with only one of them exceeding expectations and another one exactly meeting them.

Respect Privacy

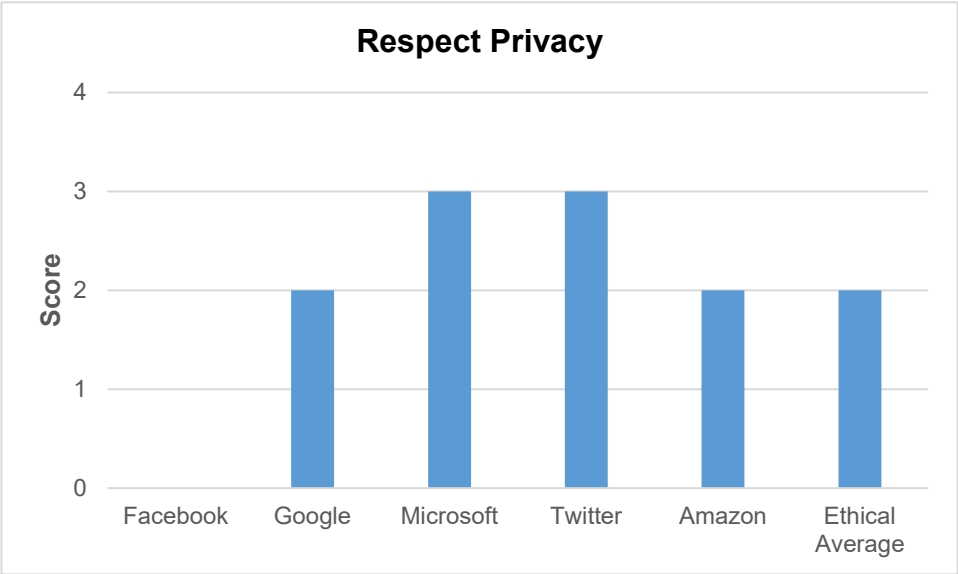

Figure 4: Comparison of the Infractions Against Respecting User Privacy

In this category, the only company that failed to meet the Ethical Average was Facebook, which scored zero points. All others either exceeded or met expectations.

Protect Confidential Information

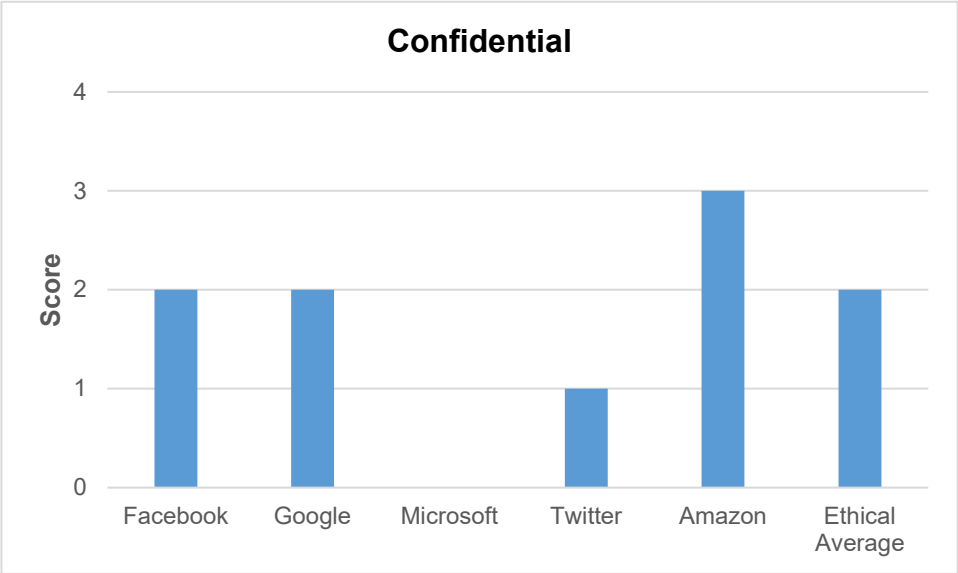

Figure 5: Comparison of the Infractions Against Protecting Information

In this category, only Amazon exceeded the expectations set by the Ethical Average. Facebook and Google both met this standard, but neither exceeded it. Twitter received only one point, while Microsoft received none.

Act As Authorized

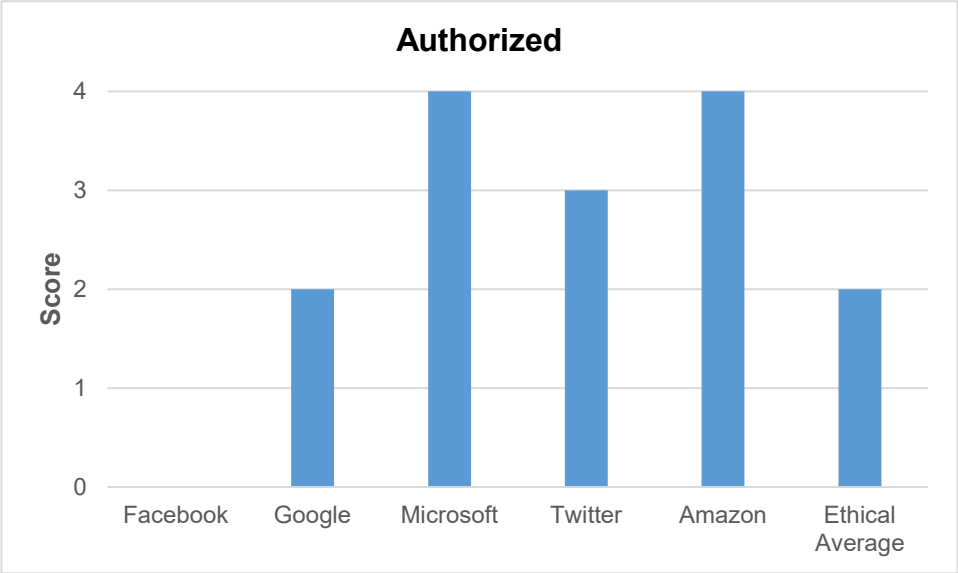

Figure 6: Comparison of the Infractions Against Acting as Authorized

In this category, every company except for Facebook managed to meet the ethical standard. The only one that failed to exceed it was Google. Microsoft and Amazon both faced no infractions, while Twitter only received one.

Overall Evaluation

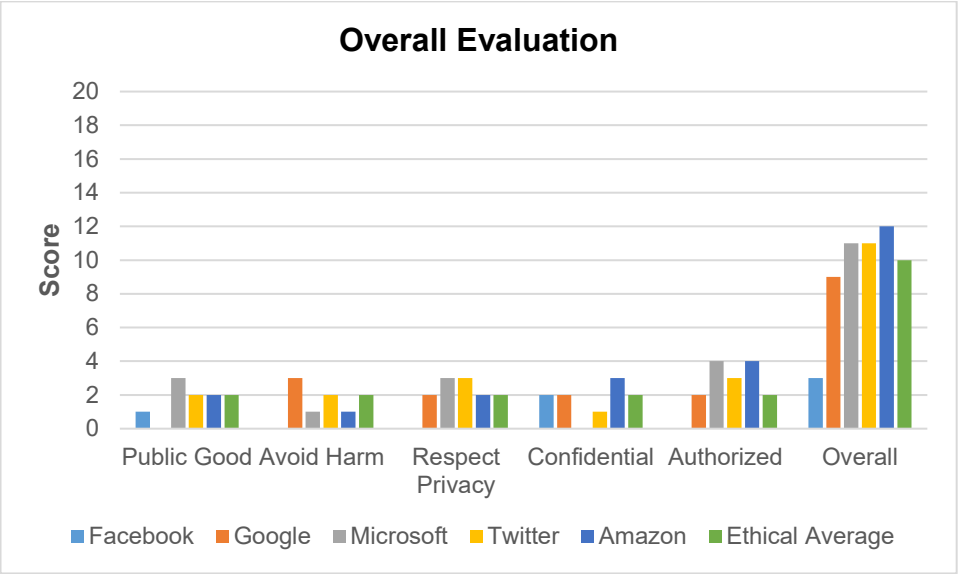

Figure 7: Comparison of All Infractions and Final Scores

Amazon, Twitter, and Microsoft all exceeded the overall Ethical Average. In accordance with the standards of this study, their conduct has been proven ethical. Google and Facebook both failed to meet the Ethical Average. Their conduct, on the whole, has been determined unethical, due primarily to their inability to act in favor of the public good and to only use information as authorized by the user.

CONCLUSIONS

The most prolific software companies often skirt the line of ethical behavior. They behave in ways that can often put their users at risk, either intentionally and with the motive of private gains, or unintentionally, through negligence or an incapability to protect from a particular type of threat. Amazon's greatest struggles are internal, due to the company's large size creating an inability to prevent a bad actor from gaining access to exploitable information. Facebook's greatest problem is its intense

desire to profit from its vast userbase by any means necessary, and its disregard for how the information they expose may be used can harm its users.

Despite this, overall, the companies acted ethically more often than not. While their behavior may not be ideal, these companies act in a largely ethical manner. The areas in which they struggled the most as a whole were the maintaining the confidential status of confidential information, and in the avoidance of harm befalling its users as a consequence of the company's actions. Both of these can be mitigated by the use of more effective cybersecurity measures; namely doling out information only to those who absolutely require it, and taking immediate action upon being made aware of any bugs or breaches that could compromise user information.

REFERENCES

[1] *IEEE Computer Society*. [Online]. Available: https://www.computer.org/education/code-of-ethics. [Accessed: 28-Feb-2022].

[2] "The code affirms an obligation of computing professionals to use their skills for the benefit of society.," *Code of Ethics*. [Online]. Available: https://www.acm.org/code-of-ethics. [Accessed: 17-Apr-2022].

[3] I. Ozkaya, "Ethics is a software design concern," *IEEE Xplore*. [Online]. Available: https://ieeexplore.ieee.org/document/8693077. [Accessed: 28-Feb-2022].

[4] "Yahoo triples estimate of breached accounts to 3 Billion," *The Wall Street Journal*, 04-Oct-2017. [Online]. Available: https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804. [Accessed: 17-Apr-2022].

[5] M. Terry, "Different types of hackers – and what they mean for your business," *Bridewell Consulting*, 25-Feb-2022. [Online]. Available: https://www.bridewellconsulting.com/different-types-of-hackers-and-what-they-mean-for-your-business. [Accessed: 17-Apr-2022].

[6] M. Laforgia, M. Rosenberg, and G. J. X, "Facebook's data deals are under criminal investigation," *The New York Times*, 13-Mar-2019. [Online]. Available: https://www.nytimes.com/2019/03/13/technology/facebook-data-deals-investigation.html. [Accessed: 17-Apr-2022].

[7] I. Ullah, R. Boreli, and S. S. Kanhere, "Privacy in targeted advertising: A survey," *arXiv.org*, 20-Jun-2021. [Online]. Available: https://arxiv.org/abs/2009.06861. [Accessed: 28-Feb-2022].

[8] “American schools gave kids laptops during the pandemic. then they spied on them | Jessa Crispin,” *The Guardian*, 11-Oct-2021. [Online]. Available: https://www.theguardian.com/commentisfree/2021/oct/11/us-students-digital-surveillance-schools. [Accessed: 17-Apr-2022].

[9] C. E. Lincoln Spector, “The windows 10 technical preview, keylogging, and you,” *PCWorld*, 03-Nov-2014. [Online]. Available: https://www.pcworld.com/article/435872/the-windows-10-technical-preview-keylogging-and-you.html. [Accessed: 17-Apr-2022].

[10] E. Steel and J. E. Vascellaro, “Facebook, Myspace confront Privacy Loophole,” *The Wall Street Journal*, 21-May-2010. [Online]. Available:https://www.wsj.com/amp/articles/SB10001424052748704513104575256701215465596. [Accessed: 02-Nov-2022].

[11] A. Chang, “The Facebook and Cambridge Analytica scandal, explained with a simple diagram,” *Vox*, 23-Mar-2018. [Online]. Available: https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram. [Accessed: 02-Nov-2022].

[12] G. J. X, “As Facebook raised a privacy wall, it carved an opening for tech giants,” *The New York Times*, 19-Dec-2018. [Online]. Available: https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html. [Accessed: 02-Nov-2022].

[13] Bferrite, “BrainTest - a new level of sophistication in Mobile malware,” *Check Point Software*, 21-Sep-2015. [Online]. Available:

https://blog.checkpoint.com/2015/09/21/braintest-a-new-level-of-sophistication-in-mobile-malware/. [Accessed: 02-Nov-2022].

[14] D. MacMillan and R. McMillan, “Google exposed user data, feared repercussions of disclosing to public,” *The Wall Street Journal*, 08-Oct-2018. [Online]. Available: https://www.wsj.com/amp/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194. [Accessed: 02-Nov-2022].

[15] “Google Records your location even when you tell it not to,” *The Guardian*, 13-Aug-2018. [Online]. Available: https://www.theguardian.com/technology/2018/aug/13/google-location-tracking-android-iphone-mobile. [Accessed: 02-Nov-2022].

[16] B. Brody and M. Bergen, “Google to pay $170 million for YouTube child privacy breaches,” *Bloomberg.com*, 04-Sep-2019. [Online]. Available: https://www.bloomberg.com/news/articles/2019-09-04/google-to-pay-170-million-for-youtube-child-privacy-breaches. [Accessed: 02-Nov-2022].

[17] K. Zetter, “Microsoft learned of IE Zero-day flaw last September,” *Wired*, 22-Jan-2010. [Online]. Available: https://www.wired.com/2010/01/microsoft-zero-day-flaw/. [Accessed: 02-Nov-2022].

[18] C. Donnelly, “Xbox Live users hit by Data Breach,” *IT PRO*, 20-Mar-2013. [Online]. Available: https://www.itpro.com/data-leakage/19470/xbox-live-users-hit-data-breach. [Accessed: 07-Nov-2022].

[19] K. Canales, “Hackers scraped data from 500 million linkedin users - about two-thirds of the platform's userbase - and have posted it for sale online,” *Business*

Insider. [Online]. Available: https://www.businessinsider.com/linkedin-data-scraped-500-million-users-for-sale-online-2021-4. [Accessed: 07-Nov-2022].

[20] B. Fung, "Data leak exposes tens of millions of private records from corporations and government agencies | CNN business," *CNN*, 24-Aug-2021. [Online]. Available: https://www.cnn.com/2021/08/24/tech/data-leak-microsoft-upguard/index.html. [Accessed: 07-Nov-2022].

[21] M. Jurkowitz and J. Gottfried, "Twitter is the go-to social media site for U.S. journalists, but not for the public," *Pew Research Center*, 29-Aug-2022. [Online]. Available: https://www.pewresearch.org/fact-tank/2022/06/27/twitter-is-the-go-to-social-media-site-for-u-s-journalists-but-not-for-the-public/. [Accessed: 07-Nov-2022].

[22] "Social Media Stats Worldwide," *StatCounter Global Stats*. [Online]. Available: https://gs.statcounter.com/social-media-stats. [Accessed: 07-Nov-2022].

[23] K. Zetter, "Weak password brings 'happiness' to Twitter Hacker," *Wired*, 06-Jan-2009. [Online]. Available: https://www.wired.com/2009/01/professed-twitt/. [Accessed: 08-Nov-2022].

[24] R. Sandler, "Twitter is telling everyone to change their password after a bug left 330 million passwords exposed," *Business Insider*. [Online]. Available: https://www.businessinsider.com/twitter-tells-all-330-million-users-to-change-their-password-after-bug-left-them-exposed-2018-5. [Accessed: 08-Nov-2022].

[25] Z. Whittaker, "Twitter warned of phone country code leak two years ago - but did nothing, security researcher says," TechCrunch, 18-Dec-2018. [Online]. Available:

https://techcrunch.com/2018/12/18/twitter-warned-country-code-form-leak-bug-security-researcher/?guccounter=1. [Accessed: 09-Nov-2022].

[26] L. H. Newman, “Never trust a platform to put privacy ahead of profit,” Wired, 09-Oct-2019. [Online]. Available: https://www.wired.com/story/twitter-two-factor-advertising/. [Accessed: 09-Nov-2022].

[27] W. Evans, “Amazon's dark secret: It has failed to protect your data,” Wired, 18-Nov-2021. [Online]. Available: https://www.wired.com/story/amazon-failed-to-protect-your-data-investigation/. [Accessed: 09-Nov-2022].

[28] M. Ehrenkranz, “A hacker claims to have leaked 80,000 Amazon users' passwords and personal information,” Mic, 08-Jul-2016. [Online]. Available: https://www.mic.com/articles/148207/a-hacker-claims-to-have-leaked-80-000-amazon-users-passwords-and-personal-information. [Accessed: 09-Nov-2022].

[29] M. X. Heiligenstein, M. A. F. Sr., C. Reed, A. Proctor, C. Kime, and R. Minton, “Cybersecurity News, Guides, & Resources,” Firewall Times, 07-Nov-2022. [Online]. Available: https://firewalltimes.com/. [Accessed: 15-Nov-2022].