5-2021

# Brave New World Reboot: Technology's Role in Consumer Manipulation and Implications for Privacy and Transparency

Allie Mertensotto

# Brave New World Reboot: *Technology's Role in Consumer Manipulation and Implications for Privacy and Transparency*

**By**

**Allie Marie Mertensotto**

**Advisor: Dr. Molly Rapert**

**An Honors Thesis in partial fulfillment of the requirements for the degree Bachelor of Science in Business Administration in Marketing.**

**Sam M. Walton College of Business**
**University of Arkansas**
**Fayetteville, Arkansas**

**May 8, 2021**

**INTRODUCTION:**

Most consumers are aware that our data is being obtained and collected through the use of our devices we keep in our homes or even on our person throughout the day. But, it is understated *how much* data is being collected. Conversations you have with your peers – in a close proximity of a device – are being used to tailor advertising. The advertisements you receive on your devices are uniquely catered to your individual person, due to the fact it consistently uses our data to produce efficient and personal ads. On the flip side, our government is also tapping into our technology to learn more about us as well. Generation Z refers to this as "the FBI agent living in our phone." There is a phenomenon surrounding this topic and it is becoming common knowledge that our devices are listening to us. Whether or not people want this to happen, it is inevitable.

While this appears incredibly daunting: "our phones routinely collect our voice data, store it in a distant server, and use it for marketing purposes" (Komando, 2019). There are many fuzzy areas when it comes to the legality of technology and the transmission of our personal information to third parties. Fundamental privacy rights, liability, and constitutional issues are just to name a few. While GDPR is an example of data privacy law that is tackling the issue comprehensively abroad, there is surprisingly not a satisfactory legal framework currently in place within the United States (Green, 2018).

This research project is designed to explore the range in which consumers deem this phenomenon acceptable and where the tipping point lies in terms of this being beneficial or creepy. I have developed a three-stage approach to this research. Because data privacy issues are rampant, listening devices are ever present, and there is a lack of extant literature in this domain, I feel it is important to extend the traditional business research approach to include a multifaceted exploration of the domain. Accordingly, I will conduct a literature review in three core areas: the rise of technology, technological devices and transparency as a whole, and global landmark situations. Within this literature review, I will evaluate legal cases surrounding the matter and accumulate all relevant information concerning our technology's underlying purpose within the privacy realm. Finally, I will build on these foundations to develop a survey of consumer expectations, utilizing existing academic scales of privacy, expectations, preferences, comprehension and protection (Maser, 2020; Naeini et al, 2017; Custers et al, 2014;) the research design will target cross-generational respondents to explore subgroup differences that I will analyze and deliver results on. Additionally, this research was supported through funding provided by the University of Arkansas Honors College and the State Undergraduate Research Fellowship program.

**THE RISE OF TECHNOLOGY**

When you are sitting at home or a restaurant – driving in the car, traveling or just simply at work – it is assumed that there will be a device within an arm's reach of your person. Devices such as smartphones, tablets, computer/laptops, smart speakers, smart TVs and MP3 players are becoming customary in everyday life. According to the Pew Research Center, 81% of American adults own their own smartphone (Pew Research Center, 2020). By the Marriam Webster definition, the term "smart" in front of this phone indicates it is a cell phone that includes additional software functions such as email or an internet browser (Merriam-Webster). This ever-present device is usually always on our person, when decades ago the closest telephone would be your landline plugged in at home. As generations emerged and science became more advanced, our world has gradually shifted to become the 'era of technology.'

Before diving into how smartphones are the driving force of modern times, it is essential to understand the context of technology and it's past and current status. Technology defined by Merriam Webster dictionary captures the essence of the term by stating it's "a manner of accomplishing a task especially using technical processes, methods or knowledge" (Merriam-Webster). Before life was "handed to us on a silver platter" – individuals decades ago built the foundation of where we are today in regard to the technological realm. Technology technically originated with the "first tools" just as sharp flakes of stone to resemble knives or even hammers. These tools were made nearly 3.3 million years ago. As time went on, mechanical clocks, printing, steam engines, railways and steamboats were all invented before the 1800s. Photography entered the scene in the early 1820's when Nicéphore Niepce used "light-sensitive solution to make copies of lithographs onto glass, zinc and a pewter plate." Towards the end of 1820s he made an "eight-hour-long exposure of the courtyard of his house" which was known to be the first 'photograph' (Gregersen). Within a 30-year gap in the 1800s, Samuel Morse created the electric telegraph and by the end of said gap, the telephone was created by Alexander Graham Bell. The improvement from merely written to actual voice communication was revolutionary. Following the telephone, one of the last grand inventions before the 1900s was the automobile, by Karl Benz in 1885. The first radio was developed by Guglielmo Marconi after a long experiment to send transmission over long distances. The Wright brothers made their appearance next in 1903 with the invention of an airplane, flying from 120-852 feet. The 1900s began to kick off the incredible frontier of the technology we know and use consistently today. Philo T. Farnsworth created the television and approximately a decade later John Atanasoff designed the first electrical digital computer. Yet, be careful not to mistake this 1937 design for the personal computer we know and use today. It wasn't until 1974 when the first personal computer was invented. These devices were gigantic and eventually worked down to be smaller yet all the more powerful. That same year, the internet was invented by Vinton Cerf and Robert Kahn. It was stated that "the IP became the basis for how data is transmitted over the Internet" (Gregersen). Artificial intelligence entered the scene for the first time in 2017 via a program called AlphaGo. To explain further, "Go" is a game that has very simple rules but in turn, many possible positions. It was said that "through machine learning, AlphaGo became better at the game than any human" which is astonishing and overwhelming all at once.

World's before Apple maps and GPS systems could get us anywhere and everywhere, people relied solely on atlases. These spiral-bound books enclosed over one hundred pages of maps, road information and highway details for the entire country (Larkin, 2019). Before you could pull out your cell-phone to capture the moment with your loved ones, you would take a photo on a camera and it would take a week for film to develop. Before you could send a note to

a friend a thousand miles away via a quick text or email, your penmanship was on full display through handwritten letters that could be sent from post offices to destinations all across the world. In a similar realm, after the telephone was invented there was even more improvements within the structure as you can now not only just call and write to your loved one if they are far but see their face through your device in 'live time.' Facetime and other video chat platforms such as Skype and Zoom are heavily relied upon to stay in touch with those near, far and even across the world. The Internet wasn't always wireless as there used to be a manual phone line required to connect to the Internet. Older generations reflect on this period and recall their many struggles with the dial-up internet system. Christopher Burke wrote on a Quora site that "you had to make sure nobody else in the house picks up the phone to dial while you're connected to the internet or your connection would drop." That thought is unfathomable to many younger generations as we view our multiple devices simultaneous connection as customary. Within the Internet realm, a few decades ago – to study you had to go to a library and check out encyclopedias and textbooks, but now with a click of a button, you can have all the information you need right at your fingertips in the comfort of your own home or simply wherever you have a connection.

Continuing on this walk down memory lane – to see a movie you had to go to a DVD store such as Blockbuster, Hollywood Video or even just catch it at the right time at your local movie theatre. Now there are endless capabilities to stream any show or movie on a device within mere seconds. Blockbuster rental company actually went out of business and filed for bankruptcy in 2010 "after Netflix's popularity continued to grow" resulting in the accumulation of $1 billion of debt (Olito, 2020). These streaming platforms are a prime example of how technology has evolved to become easier, more efficient for the consumer to "accomplish" a task – as mentioned in the technology definition earlier. There are many platforms you can stream on as this does not stop at just Netflix. Hulu, Disney +, Paramount +, HBO Now, Amazon Prime are just to name a few of the subscription packages you can sign-up for. These are all video streaming service packages that an individual must "subscribe to" in order to access. This is also seen in how some cable companies allow digital video recordings, commonly referred to as DVR to record movies or series that air during a specific time, for you to go back and watch later at your convenience. These are both quick ways that technology snuck onto the movie/digital scene of normal business practices to 'get ahead.' In a similar realm, books are starting to be replaced by Kindles, Nooks and other e-readers. Technology is stepping in and taking the place of many old, traditional items that were around the house. You can read any magazine, news article or novel on your e-reader, tablet or iPad in a matter of seconds. It has simply become more convenient than driving to the store to buy continuous new copies. Newspapers have since stopped being delivered regularly to neighborhoods since most retain their news from their applications on their devices, the Internet or through social media platforms such as Twitter. The transition of news from print to television/radio to digital spaces caused a lot of disruptions to the "traditional news industry" according to Pew Research Center. Roughly 86% of US adults claim to get their news from their smartphone/tablet/computer. This has become the new common way to receive news and has been the ultimate game changer within the news industry (Shearer, 2021).

In addition, old traditional watches that have been around for decades are being traded in for all forms of smart watches which now have capabilities to make phone calls, send text messages, track fitness analytics, send notifications, use apps – the list goes on. You're essentially wearing a 'tiny phone on your wrist. There are many different brands that design and

sell these watches such as Apple, Samsung Galaxy, Fossil, etc. If you don't have a smart watch, there are still fitness trackers to be worn such as a FitBit - that allows you to self-monitor your activities and meet fitness goals and tracking your metrics such as heart rate, calorie consumption and keeping track of your distance. This is a realm of technology that didn't necessarily "replace" anything but was invented anew, to aid individuals through everyday life. With more recent applications such as CashApp, a mobile payment service developed by Square, Inc., allowing users to transfer money to one another using a mobile phone app (Cash App) or Venmo, another mobile payment service application owned by PayPal that allows individuals to transfer funds to one another via a mobile device within the US (Venmo).

Author Francine Cefola wrote in her book 'Tell It to the Future' that "if we don't know where we come from, how can we know where we are going?" She then goes on to explain that "we learn from the past." We have learned, prospered and steadily grown through each technological change, and mistake, while seamlessly entering into the "era of technology." Every invention and idea that was set before us centuries ago have developed into our customary, every day essentials. Our 'traditional society' is and has been built upon technology and it's only growing from here.

Circling back to smartphones, it is significant to notice the magnitude of what they can do for us as individuals. This incredible piece of technology provides many benefits such as keeping your loved ones who live miles away close, quick & accessible maps, instant communication, web surfing capabilities, entertainment applications, reading the news, educating yourself, having a camera on hand, and countless opportunities to stay connected (Munoz, 2018). These devices are getting "smarter and smarter every day" and it's like having a personal computer fit in your pocket, aiding you at any moment necessary. Over half the population own a smartphone as this is an integral part of their daily lives. According to a 2016 Survey by Bank of America, 93% of millennials said smartphones are more important than a toothbrush and deodorant (Munoz, 2018).

Understanding the context of technology is crucial but knowing that the rise of this is at the expense of our personal information being leaked/compromised, is not so comforting. While technology and devices such as smartphones playing a lead role in our everyday lives is beneficial, it is imperative to also conceptualize that this means our lives are on full blast, at all times. When using any device or platform that I previously mentioned, we usually have to give our personal information to the server. With this knowledge, it is chilling to think that our personal information is "more accessible than ever." It's not assuring to hear that this is "at the expense of our privacy." The time an average audience spends on technology (i.e. desktop, smartphone, tablet) resulted in being 90 hours and 49 minutes for the month of February and 102 hours and 29 minutes for the month of March in 2020. Roughly 80% of their time spent on devices was on a smartphone (Nielsen, 2019). It's important to understand the context of technology and how there has been a huge rise in the use of digital devices in the past 40 years. Just like Big Brother predicted, the eerie comparison of 1984 to the current paranoia we live in today is the same: consistently worried that the government is listening to everything we say. George Orwell wrote in his fictional world that technology that tracks your every move and we live in an era today that the internet does just that (Wiggins, 2016). Back in the time period of this book, technology still had a long way to go. Only 8% of households had a personal computer and the World Wide Web still had a few years to grow at this point. Looking back at the year I was born, 1998 – 61% of households did not have internet. 18 years later in 2016, over 70% of consumers had not just internet in their homes, but a broadband that is high-speed and connects

all computers together. This is massive improvement in the context of how fast technology came to the scene and dominated. Similarly, in 1998, 62% of people did not own a cell phone. By 2007, 71% of Americans had a "dumb" phone and by 2016, 75% own a "smart" phone. The cell-phone has had over 27 remodels to the 'brilliant' technology it has become (Fischer-Baum, 2017).

Within this realm, it is also necessary to call out that there are multiple issues involving our technology/devices causing identity theft. This can be done in both "low-tech and high-tech ways." According to Norton, thieves are aiming to exploit your information and this is a topic of discussion that I will expand upon shortly (Norton Online). Overall, because our smart phones can access the internet, take photos/videos and have voice assistants such as Siri enabled on them – they are revolutionary and becoming a staple for most humans. A feature that these phones have are voice-activated software's and are "personal assistants" to you. In that realm, people are purchasing products such as iPhones, Amazon Alexa, Google Home, etc. that don't have to be plugged in/ 'told to start' to hear a command from their user – in which confirms the fear that they are "always listening." Such devices listen for "wake phrases" and our commands are routinely recorded to be held in a personal data base (Komando, 2019). This is commonly found in smartphones, meaning you always have a recording device listening into your conversations within an arm's reach of your person.

Coronavirus Disease 2019, commonly referred to as COVID-19, is described as an infectious disease that is caused by a new coronavirus called 'severe acute respiratory syndrome coronavirus 2' (SARS-CoV-2). When this outbreak occurred in Wuhan City, Hubei Province, China in December of 2019 it was originally reported to the WHO and quickly became a "global health emergency." As this virus began to spread rapidly across the globe, infecting and killing millions, the WHO declared COVID-19 as a "global pandemic." A global pandemic is essentially an epidemic that "occurs worldwide, crossing international boundaries and affecting large amounts of people" (Medscape, 2021). In March, the entire world essentially went on "lockdown" but referred to this period as "quarantine." The definition states that it's a "state, period, or place of isolation in which people that have arrived from elsewhere or have been exposed to infectious or contagious disease are placed." It was mandatory – since the virus was so new and no one knew the details surrounding it yet – to have "normal life" go on pause for an intermediate period. It is currently March of 2021, a year later, and we are still technically in "quarantine" because the pandemic hasn't been entirely controlled – but there is a vaccine that is in the process of being rolled out. But in March of 2020 the world had to take an unforeseen pause and this caused places of business, schools/Universities, the entertainment industry, travel, and anything deemed "normal" to go into immense panic. Teachers especially were thrown off as all their students were sent home for the remainder of the semester, not to return to in-person classes in the foreseeable future. Due to the entire population under an isolation period to help "protect the public by preventing any exposures" – life felt like it was falling a part in the beginning. Luckily, with the technology of modern times this didn't hinder performance for businesses to get their work done and for students to finish out their semester. Due to the millions having to stay home, there needed to be "virtual" ways for individuals to stay involved with their field. Enter: Zoom, in how this "cloud-based video communication app" saved the day by "allowing you to set up virtual video and audio conferencing, webinars, live chats, screen-sharing and other collaborative capabilities" (Antonelli, 2020). All platforms can connect and access this means of technology which allowed lectures, meetings, business calls, trivia nights, connecting with loved ones, happy hours, attending conferences, etc. to go on! Zoom has risen to

the top thanks to the "intense separations measures" and a "profound resonance within this new social distancing culture." It was stated by CNBC, that "daily downloads of the Zoom app have increased 30x year-over-year" and the app spiked from 10 million to 200 million downloads in just *three* months, back in March 2020 (Evans, 2020). Zoom has quickly become the video communication platform of choice for "federal governments, tech startups, religious communities, and individuals who miss seeing their friends and family" (Antonelli, 2020). Its growth is on track to continue at a "rapid pace amid the vaccine rollout" due to the fact this company has become a "household name" amidst the pandemic lockdowns (Armental, 2021). This is just an example I wanted to tie into how the context of technology has evolved and changed so much since its origin. The technology has created a comfortable environment to continue working and visiting with colleagues, coworkers, peers & family amidst ever-changing, unprecedented times. Zoom has changed the normalcy of office life and education as we know it. In plain words, it has become our "new reality" quoted by Chief Executive Officer Eric Yuan. He went on to state that remote/working from anywhere is the new future and it's "here" (Armental, 2021).

Technology is ever-present, rapidly evolving and changing therefore it's up to our ability to adapt and maintain within the flow because our future truly lies in its hands.

## PRIVACY & TRANSPARENCY –GLOBAL LANDMARK SITUATIONS, LEGAL CASES & CONCERNS

The average consumer lives in a state of oblivion when it comes to the privacy rights they are signing over when they purchase a device. There is an internal battle when receiving/purchasing any type of new technology due to the fact that you could be signing away your privacy rights – just like that. 61% of businesses surveyed think that data privacy regulation improves customer trust and in order to create a comprehensive data privacy framework, the United States needs to follow the path of many successful countries such as the EU.

When researching what the EU has in place - GDPR, General Data Protection Regulation, I found that this was the strictest data privacy law in the world. Specifically, they have gone the farthest in terms of privacy within the technology realm, leading many to believe that GDPR is an example of a data privacy law that is tackling the issue comprehensively. The stark reality is that lawmakers have simply left the American public behind. By definition, this regulation imposes obligations onto organizations anywhere in the world if they are targeting or collecting data related to anyone in the EU. This regulation was officially put in place on May 25th, 2018. This is a legislation that imposes heavy fines against those that violate the security/privacy standards put into place (GDPR, 2018). Also, "while other countries have enacted consumer privacy protections", a topic I will be exploring, "the United States has no satisfactory legal framework in place" (Green, 2018.) There are no well-established regulations on how companies or the government uses our personal data. In 1986, our Congress passed the 'Stored Communications Act' in aims to protect individuals' private content held in electronic storage by third parties. While this seems like this is a step in the right direction, courts today have "struggled to apply the SCA consistently" due to different technologies. It is said that many want Congress to revisit this act to create a 'technology-neutral' standard that offers this once promised protection (Thaw, 2015). Implementing regulation that closely resembles GDPR is crucial during a time that people are trusting their personal data with cloud services and breaches are becoming a daily occurrence (GDPR, 2018).

On another note, there are many fuzzy areas when it comes to the legality of technology and the transmission of our personal information to third parties. Fundamental privacy rights, liability, and constitutional issues are just to name a few. There have been legal cases involving a voice-controlled device (i.e. Amazon Alexa) having its own legal protections and learning how it abides with our Amendment rights. The protection of speech by a digital assistant rises so many ethical/privacy questions and there are [murder] cases such as *State of Arkansas v. Bates* which involve law enforcement "seizing and issuing a search warrant" over their Amazon Echo to retrieve audio recordings during the 48-hour windowed time of death (Silvestro, 2017). In another example, Alexa "witnessed" an alleged Florida murder as the device held "crucial information" within the devices' recordings. The individual was charged with murder of his girlfriend's death and they were seeking ways to hear these Amazon Echo recordings in court, according to NBC News (Burke, 2019). It is wild that devices that are merely just sitting in our homes, can turn into "witnesses" in a matter of seconds when it comes down to the wire. If you think what you are saying in your home is private – think again. With such devices, you now have someone constantly eavesdropping and it could be used for/against you in court one day. But is this allowed? Does this go against the privacy policy that Amazon has in place? This is the ultimate test of the "devotion to your privacy" (Sauer). People can easily offer up these recordings but the question at stake is can companies such as Amazon or Google be *forced* to share the information with law enforcement? This act of betrayal through the state of Arkansas police *demanding* the collection of recordings from the murder suspects' Echo. Yet, it since had to go through many "legal hoops" to ensure the data being collected cannot be obtained elsewhere, specific yet integral to the investigation and pass a test in private with the judge before deciding if the information should be disclosed in court. This isn't a new area of concern within law, as individuals right to privacy has been tested before. In the 1967 *Katz* v. *United States* Supreme Court case – it was ruled that the "FBI's use of an electronic eavesdropping device (affixed outside of a telephone booth) was an invasion of privacy" and therefore could not be offered as evidence within the trial. This set up the boundaries within investigations and set precedents for future cases within this realm.

Amazon's efforts to protect the data are applaudable but then questions the reasoning for storing this data in the first place if it's so hard to access. After research, it was discovered that for example if an individual is meeting with their attorney and somehow confesses to having committed a crime/an affair with someone with a wake word such as Alexa, it would be legal to use in court, no matter how unethical – in "one party consent states." California is an example of a state that requires "permission from both parties" before recording, but not all states have this luxury enacted in their regulations (Sauer). It is important to note from a legal standpoint, that millions of users are welcoming digital assistants into their lives without a clue of the "potential havoc this Trojan horse can bring" (Sauer).

Consumer privacy is a differentiator, not just a compliance risk (Balis, Larson & Saverice-Rohan, 2021). Within a research experiment at Northeastern University – 17,000 of the most popular apps were found to record the phone's screen and send that information out to third parties." Google Chrome has intentions and the plan to phase out third party cookies by 2022 and this process will take two years to fully transition. To start, let's define what third party cookies are. They are created by domains that are not the website that you are visiting. The purpose solely is tied back to online-advertising purposes and are placed onto the website through adding scripts or tags. They are accessible on any website that can load the third-party server's code (Clearcode, 2021). You will notice the difference between first party and third-party cookies via

the origin. First party is created by the host site while third party doesn't match the domain. So, if you see the URL that doesn't match, it means it has been left behind by a third-party advertising provider. An example of this would be ad.doubleclick.net. Due to the motive to remove third party cookies, users should start to see less ads on sites that are not the one they originally clicked on. This is an effort to stop targeting ads, advertiser's effectiveness of mastering their image of us precisely, and fraud. Since the way they track individuals' personal browsing has "long raised privacy concerns" it has been ruled to phase third party cookies out by 2022 (Schechner, 2021). It went on to say that "protecting user privacy and promoting online competition can sometimes be at odds because one of tech's most popular business models is targeting advertising at individuals based on their online behavior" (Schechner, 2021). Google is receiving backlash and overarching "scrutiny" over third-party cookies in multiple countries, not just in America. It was released that the UK's top anti-trust regulator, U.K.'s Competition and Markets Authority, has also opened a formal probe into the "phasing out of third-party cookies" (Schechner, 2021). This results in companies having to prioritize first- and second-party data "more effectively" to prevent "declining in value" (Balis, Larson & Saverice-Rohan, 2021). Giving individuals control and choices when involving their data is becoming a new precedent and quite frankly a requirement under the law. The appropriate next step would be to: "create a more navigable and *transparent exchange* with customers" due the number of individuals who find privacy policies unclear. This cookie-less environment is the perfect opportunity for brands to differentiate themselves for putting privacy "at the core of their experience and values" and holding a strong commitment to this statement (Balis, Larson & Saverice-Rohan, 2021).

As previously mentioned, the GDPR – General Data Protection Regulation for EU, is the strongest data protection regulation in the world. This law "gives consumer more choices and protections about how their data is used" – and within this law it is easier to ask companies to delete their data, if they desire. Failure to comply can result in steep fines which will target and pull from their revenue. This law has drawn attention to the fact that their data is being used and has increased the incentive to want to re-gain control on their privacy rights and protections (Anant, Donchak, Kaplan, & Soller, 2021). 2020 started by implementing the California Consumer Privacy Act (CCPA) in January. This allowed consumers to be fully and consciously aware of their rights. This also allows individuals to prevent the sale of their data (Anant, Donchak, Kaplan, & Soller, 2021). This act immensely built trust which in turn made the businesses happier because it, in turn, improved their "data processing efficiency" (Velez, 2021). This Act was voted to be expanded in the past election, so the updated law is now called "California Consumer Privacy Rights and Enforcement Act, commonly referred to as CPRA. This development is moving closer to align with the European Union's General Data Protection Regulation (GDPR) that I mentioned earlier. It is to be assumed that other states will soon follow, while dozens have "pending legislation seeking to address data privacy." Maine, Nevada, New York, Oregon and Washington have also enacted their own data privacy legislation.

While state data privacy laws are on the rise, federal data privacy may be enacted within 2021 (Dillion). The only federal laws that the United States have in place currently are sector laws such as HIPAA in healthcare and GLBA in finance (Velez, 2021). The US Federal Trade Commission (FTC) has handed out the largest fine for "mishandling data" thus far. Privacy laws are beginning to drive more "stringent" data privacy best practices – which is enforcing organizations to "re-think" their approach to how they manage data to produce greater efficiency (Divatia, 2020). Companies are slightly beginning to have major reorganizations/discussions with third parties, service providers and contractors due to state laws coming onto the scene. For

example, the most comprehensive and stringent being CPRA (Dillion). There will be momentum to follow shortly for a national privacy referendum similar to GDPR. Responsibly enhancing trust within the customer and businesses is the best policy to head towards right now as the nation is shifting to attempt to protect our privacy, as it should. A uniform federal data privacy legislation will "help allow US businesses to better compete in the global market, given the other countries' established privacy laws" (Dillion).

Countries and governments outside of Europe have data-privacy regulations as well. Some examples include Brazil, in their Lei Geral de Proteção de Dados, or LGPD (General Data Protection Law). This example is also one in which started with sector-based guidelines but then became a nationwide law (Anant, Donchak, Kaplan, & Soller, 2021).

In a similar realm, there was global scrutiny on the use of data for the ever-rising 'contract tracing' applications enforced by governments around the world. It was stated by Pollyanna Sanderson from the Privacy Council at the Future of Privacy Forum – "many countries including the United States have opted for centralized approaches that allows individuals to share their GPS location with a contact tracer." Then she went on to say that data consortiums that share certain types of data are gaining momentum right now especially Apple and Google (although they already face antitrust scrutiny) via their contact-tracing collaboration and how this is a blueprint for future data sharing efforts.

Companies tapping into our data is not considered illegal by any means and these tactics will only become more refined unless the laws or the online advertising ecosystem is miraculously changed (Pettijohn, 2019). Due to the nature of ads geared to "benefit users" when in actuality it is greatly benefiting the advertisers by storing all these statistics and data about their everyday consumers. If you have ever made a purchase on a credit or debit card using your technology on Wi-Fi, then you're at risk for having your data shared and stored. The risk of putting your data on a viewable basis to a third party is possible via hacker's ability to connect into public Wi-Fi networks to watch your every move (ARAG, 2017). This information is incredibly daunting and I don't think many people know that this is the case when you study in a library, coffee shop or any public space. It is crucial to be aware to what passwords and account information you enter while you are connected to a public source of internet, in this realm it is actually safer to use your 3G/4G networks (ARAG, 2017).

Seeking out protection for your devices, if that is something that currently isn't set up, is also a crucial way to staying on top of your privacy concerns. Sometimes, smartphone apps can be the "culprit" of identity-stealing viruses. Even downloading identity theft protection apps, after proper research on the front end, is always a good idea. Parents or guardians of those with small children should be warned that sometimes "innocent" gaming apps, calculators or even flashlights can be designed to steal your personal information (Kree, 2020). The terrifying part of it all is that once a hacker is in – they have access to all your deeply personal information such as passwords, banking information and all your photos. According to 4News, FBI Agent Tomas Armendariz said a "red flag" could be as simple as evaluating if the app is using an excessive amount of cellular data. Children are extremely susceptible to falling into this trap because they don't venture into the terms and conditions to see what the app has access to upon downloading. A safety precaution is to go through your smartphones settings and disable camera and microphone from the apps that simply don't require it.

Our phones can lead to identity theft in multitudes of different ways. According to Norton, ways this can occur include: your old phone being 'disposed of 'unsafely, no lock screen security, non-updated apps, public Wi-Fi for sensitive transactions, typing passwords in public,

sharing your devices freely, no remote locking program, no anti-virus program installed, etc. (Norton Online). Another important aspect to note is that it is increasingly harder to identify a scam via a smartphone if it comes through an app, text or email (ARAG, 2017). They warn not to wait until a "threat strikes" but proactively ensure you're safely using your technology to help prevent your identity from being embezzled. In the Netflix documentary "The Great Hack" it is revealed that via Facebook – if one of your friends authorized an app on *their* account, they can still harvest some of *your* data points. The scariest part of this is that this can potentially be scaled to impact elections and policies in countries as a whole (Pettijohn, 2019).

An example is that hackers use a scam called "vishing" – which is defined in Oxford Languages as "the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers." When hackers are able to do this on your smartphone, a simple phone calls worth of information can be gathered to use against you in the future – pretending to know you, or in most cases pose as your bank. This is an increasingly important issue that is becoming more common and relevant. It must be understood that personal information is never good to give over the phone. Additionally, privacy concerns around the popular Zoom app, mentioned previously, have been on the rise since the pandemic due to the astonishing number of users. The scrutiny with this app includes an action referred to as "Zoom-bombing" and this is where a malicious user will purposefully join a Zoom meeting that they weren't invited to and show explicit or disturbing content/images. There have been many security lapses over the past year due to it quickly becoming the go-to platform of the year with the massive influx of users (Evans, 2020).

In December, there was an antitrust lawsuit against Google by ten states due to the alleged deal with Facebook to "rig [the] online ad market" (McKinnon & Tracy, 2020). The ten states involved, accused the massive platform of running an "illegal digital-advertising monopoly" through the support and aid of "enlisting rival Facebook" in an agreement to have special treatment in Google run ad auctions. This deal had a secret 'code name' after Star Wars references: "Jedi Blue." This overall, undermines the heart of the competitive process, stated by the Texas Attorney General, Ken Paxton who led the suit. Lawsuits as such can ultimately take years to resolve and appear more often than not. Federal suits like this highlight Google's relationship with tech giants Facebook & Apple Inc. (McKinnon & Tracy, 2020).

While I have mentioned many things that can deem trying to protect yourself as "hopeless" – that is not the case. Individuals should still care about their privacy, even for those who feel that they have nothing to hide. Ways to take precautions with privacy: use some services based in countries with more strict privacy laws, for example Europe, with GDPR. Examples include: Tor browser for web browsing or Duck Duck Go, Start Page, Serax, etc. It is encouraged to use an encrypted email provider based in Switzerland (ProtonMail, Runbox, etc.) You can buy protectors/camera covers for your devices as many people have started doing recently. You can turn off your phones microphone and instead of texting through your phone you can use Dust or Signal to send encrypted texts. Lastly, for applications you can log on and remove their permissions (Pettijohn, 2019). As consumers become more careful about sharing data and regulators are stepping up their privacy requirements – companies are learning that data protection and privacy can help them with a business advantage. The data collected such as location tracking and personally identifiable information is "immensely valuable to companies" to understand unmet needs and their consumers ultimate pain points (Anant, Donchak, Kaplan, & Soller, 2021). Consumers nowadays are increasingly more and more intentional about the data

we choose to share. Due to "data breaches" – it is fair to assume that there is a looming lack of trust. For example, in one company there were "2 breaches that publicized 3.5 billion records." This sent consumers flying to find ways to increase the control they have over their data by "downloading an ad-blocking software" to prevent companies from tracking their online activity or simply going into panic mode. Because the awareness of these privacy issues is rapidly growing, it is crucial that companies handle their consumer data and privacy in a respectable manner which can lead them to be a "source of competitive advantage" (Anant, Donchak, Kaplan, & Soller, 2021).

To exemplify a scenario in which companies are receiving negative repercussions in the realm of the phenomenon of our phones listening to us, I researched an instance with the tech giant, Apple Inc. They faced backlash after it was revealed their contracted workers were listening to customers speaking into their personal 'Siri-enabled' Apple products. When individuals have such conversations, they often include private information. The company since admitted they haven't been "fully living up to their high ideals." Apple is not the only company that this is relevant to. Others such as Amazon, Google, Facebook and Microsoft are just as susceptible. In 2019, Apple released an official apology for listening to Siri conversations. Their statement included the definition of what they called the "Siri grading program" which ultimately allowed contractors to "review" a small percentage of things that people spoke to their Siri 'voice assistant.' The original purpose of this program was to 'measure how well Siri was responding and to improve its overall reliability.' It would ensure it was correctly understanding commands that were actually meant to "wake" Siri to increase the efficiency of the smart assistant to deliver the best experience for users as possible. They made a remark that they were going to immediately implement a few changes that would give users some control back of how their Siri requests are handled (Haselton, 2019). This would lead to a promised opt-out option within the new iOS software (Hern, 2019). Apple posted to their site saying, by default, they will "no longer retain audio recordings of Siri interactions – but will still use computer-generated transcripts to help Siri improve." It is daunting to know that workers for such companies are not only recording our every action, but they are also producing such transcriptions. Apple was recently criticized for "harvesting data while you sleep and sending it to third parties."

According to a report from the Guardian, Apple efficiently laid off more than 300 contractors who were working on Siri grading in Europe (Hern, 2019). The "ethics" behind this type of job – that was tapping into extremely personal information such as confidential medical information and even couples having intimate interactions – are hard to defend towards the end of this program being suspended. It was slightly comforting for many employees who were concerned regarding the ethics of this matter because they "never knew how to bring up the moral implications of this job" (Hern, 2019). After this scandal, Apple's reputation was in question and they had no regard for the protection of the employees that they 'forced' to listen in on conversations. There was a slight uproar on the financial side by the employees due to the lack of protection against something they had to of seen coming. To provide some sense of "comfort" to the matter, Apple explained that the grading process reviewed less than 0.2% of Siri requests/people" but it's also disquieting to know that out of the 1.65 billion Apple devices that are in use, you could be one of the 3.3 million people that they are tapping into (Hern, 2019).

Similarly, with social media platforms if you feel that Instagram, TikTok or Facebook are tapping too closely into your private, personal information and you deem the solution of just leaving/deleting your account – it won't erase the data that your or your network has shared. There really is no escape. Some articles I came across while researching indicate that "privacy"

is an advantage of technology. This false statement indicated that "with smartphones, you can do whatever you want without anyone knowing it." It also went on to say that "you can send messages to your loved ones without the fear of anyone knowing it" (Munoz, 2018). These statements are falsely alluding that your privacy is being intact while using devices, when in reality it holds many security risks and threats. Caution needs to be exercised when using your technology and individuals should not to believe everything they read online.

## PRIVACY & TRANSPARENCY AS A WHOLE IN TERMS OF CONSUMER EXPECTATIONS

Whether or not is seems daunting: "our phones routinely collect our voice data, store it in a distant server, and use it for marketing purposes" (Komando, 2019). Compared to previous eras, nearly everything today is recorded and sorted for posterity (Pettijohn, 2019). In actuality, the likelihood is low of an actual person analyzing each and every one of your audio files that was picked up by conversations; however, artificial intelligence is at an all-time high to use their algorithms to do the "listening" for companies to produce insights that will tailor specific ads just "for you." The more data they can collect and obtain from an individual, the more precise the campaigns will be (Pettijohn, 2019). These ads can quickly become more influential than the ads that were merely created from the general public to view. There are two sides of the spectrum. A: the benefit of having information right at your finger-tips without having to research on your own. One would view this method as 'short-cuts' that save time and are personalized. Yet, then where is the tipping point to where it becomes less of a benefit and more B: creepy and a complete invasion of privacy. While yes, most applications need user's consent to use the microphone and camera on our devices–it can still be 'listening' when app isn't actively running. Not only are audio and video being used – but our "geophysical" information is influencing the algorithms. Jeff Orlowski claims that "these personalized recommendations use data not just to predict but to *influence our actions*." Users are quickly becoming the easiest prey for all advertisers out there.

After watching the chilling film "Social Dilemma" it only furthered the reasoning for my research project to evaluate the implications within privacy and transparency across different generations. While the majority of this research can come off with a negative connotation, there are many who believe that with the right changes – we can salvage the "good social media without the bad" (Girish, 2020). In order to evaluate the implications of how different generations have ranging levels of threshold with this phenomenon, it is relevant to start by defining our generations.

According to the Pew Research Center, an individual's age is "one of the most common predictors of differences in attitudes and behaviors" due to the fact it denotes their place in the life cycle and their membership in a cohort of individuals who were born at a similar time (Pew Research Center, 2020). It is important to define the bounds of generations to fully analyze their differing opinions within my research. The Center for Generational Kinetics defined the generations as Silent, Baby Boomers, Generation X, Millennials, Generation Z, and Alpha. If an individual is born in 1945 or before, they are considered a member of the 'Silent Generation' – which in 2021, categorizes most grandparents in this being individuals 76+. The next generation holds a lot of older parents and is known as the Baby Boomers. This range is between the individuals born between 1946-1964, making the youngest member of this generation 57. My parents fall in this category but most of my peers' parents fall in the realm of being in Generation X. This generation holds birthyears between 1965-1976, making the youngest Gen X member

45. Millennials (also referred to as Generation Y) are to follow and are between the years 1977-1995. This generations youngest individual would be 26 years old today. This data is recently new in terms of the cutoff year as many of my peers relate to Millennials, as we grew up with similar realms. I was born in 1998, so technically I fall in the category of Generation Z, Gen Z for short, which were individuals born from 1996- 2010. This makes the youngest member of Gen Z only 11 years old. The current generation that starts at 2010-today are known as Generation Alpha (The Center for Generational Kinetics, 2020).

Upon my personal research within this context, my parents - both 'baby boomers' – are usually really worried about this phenomenon and understand that there truly is no way to effectively *stop* it. While, members of my generation 'Z' feel as if they "don't have anything to hide" and don't mind the reality that our technology is tapping into *everything* we do. My parents' age tends to be more worried about the government listening rather than companies, while my peers don't seem to mind too much overall. I plan to see the affects and consensus of this in my survey that I will conduct.

Within a similar realm, Gallup research also shows that the millennial generation can be described as "unattached, while simultaneously connected, unconstrained and idealistic" (Fleming & Adkins, 2020). It was also stated that 80% of millennials place either some or a lot of trust into companies to keep their data secure while thinking their data is simultaneously being "kept private." In stark reality, we actually have no right to privacy and we never really did. Some insightful information to note is that your data is already out there and eligible to be tapped into the second you have authorized the app. Once it has been downloaded and you clicked 'accept' or something similar – regardless if you delete the app or not, the creators still have access to whatever data they choose. Perhaps you downloaded 'FaceApp' in the heat of the #OldAgeChallenge but immediately deleted the app due to rising concerns about your data and photos – that doesn't change a thing. Just because an app isn't actively downloaded on your phone, does not mean that they lost the insights or data they can tap into (Pettijohn, 2019). It is quite unsettling to hear this because I fall victim to this same policy. I was a part of the mainstream challenge to download FaceApp but once I deleted the app it was – out of sight, out of mind. It is eerie to think that the creators still have the accessibility to look into my data of a challenge that I participated in almost 2 summers ago. The privacy landscape is changing rapidly and chaotically.

While consumers say candidly that they care about privacy, in stark reality only few have placed any real value on protecting their data. The individuals who have acted upon this are a part of a new group that the Harvest Business Review refers to as the "privacy actives." This came to be when 32% of the HBR survey respondents claimed they deeply care about privacy, are willing to act and in fact have done so by switching providers over data/sharing policies" (Harvard Business Review, 2020). This makes companies antennae's raise because these strong-feeling individuals care immensely about how their data is being shared and trust from these individuals is hard/almost impossible to regain. They claim to not buy from companies "if they don't trust how their data is used." While this group seems really daunting, there is also a complete polar opposite group as many individuals seemed comfortable with their information being shared if there were benefits involved (Harvard Business Review, 2020). Benefits including: personalized products or services, personalized ads, etc. There is a transparency gap, so understanding the context of that and clarifying the privacy policies to ensure people can interpret what they are reading in a timely manner is crucial.

The role and reach of social media platforms are largely growing within our modern world. Research conducted at Loyola University in Maryland states that media platforms allow for users to create accounts where they can provide behavioral, preference and demographic data about themselves to then be collected via things you post, like, accept or search on your device (Loyola University Engaging Media). Big data companies are collecting this data to ultimately "build personas" about you. Companies such as Facebook, Instagram, TikTok, Twitter, etc. are drafting these computer-based personalities. Through tracking our browsing history and our overall behavior through things we like, search and watch – they are able to produce ads that seem way too relevant to your specific person. For example, Instagram – through their integration with Facebook – both use our personal information to show ads that one would be incredibly inclined to click on due to pulling from information it has from how we interact and behave within both apps (Burke, 2019). Social media platforms as such use their profiles they create about us to *sell* such personalized ads. In more recent events, the booming of TikTok in 2020 – increasingly has been transmitting user's information to build specific content. Apparently, Apple has 'caught,' Chinese app, TikTok spying on millions of iPhone users in how they listen to individuals' conversations. This is because TikTok has been recording in the background without the app even being open. There has been no evidence to support the claim that TikTok is being used for "spying" however, but they do collect users' data in a similar way to Facebook and other popular social media apps.

Ever curious on what type of information that these corporations were potentially getting access to without our active permission? Personal medical details, confessions, intimate moments, arguments, even venturing into drug deals and that's just the start of it. Allow yourself to think of the amount of conversations you have with a device sitting near you. Around 81% of Americans own a smartphone, that is regularly on their person, so consider all the things a simple microphone can record: any noise, whisper, conversation – even in circumstances when you think you are in a private, secure space. That is just the audio spectrum. Reflect, now, on the multitudes of instances a camera can record, potentially save and share. To our dismay, our devices "transmit everything about [us] to a programmer in a city you [may] have never heard of and quietly share our sensitive information" (Komando, 2019). What's the payoff – might you ask? *Why* are companies so interested in our personal data? *Why* do our raw statistics matter to the likes of Google, Apple, Amazon, etc.? In their case they claim it is to "improve technology and make our lives easier/more enjoyable." But it seems too be good to be true that this is all for *our own* benefit – that's where the kicker of tailored advertisements steps into play. It is alarming to also revel in the fact that since our information is readily available for these companies and the government, it is easy for cyber-criminals to combat through our personal data to find "millions of filched email addresses, mortgage documents and even medical records." To combat this phenomenon, Alexa has added a setting where you can call out "Alexa, delete everything I said today" and it is assured to work as of June 2019 (Komando, 2019). Or in Google's case, you are able to access your own recordings and you can delete them if you desire. An important thing to note is that through the data they're collecting, the more it receives – the better it will understand and respond to us (Komando, 2019). This is the focal point of what I am trying to determine throughout this research project, of whether this fact in it of itself is disturbing or potentially favorable.

The first banner ad appeared online in 1994 on a Wired Magazine website called hotwired.com (GDPR, 2020). The ad ran a message that read "*Have you ever clicked your mouse right here? You will*" then sent the users to an AT&T campaign. Before diving deeper, it is

important to understand what a web banner ad is. This is a form of advertising that entails "embedding an advertisement into a webpage to attract traffic to new websites" (Creatopy, 2021). Every day I notice ads while scrolling through webpages on my computer. Due to the fact that I was paying particularly close attention to such advertisements during this research project, I actually stumbled upon hundreds of ads that were notably specific to my person. A majority had been things I had just spoken about out loud to a peer or something I had recently google searched on my own. For example, I briefly mentioned to my roommate that I need new Nike Air Force's and low & behold not even 20 minutes later I had this banner ad in the margins of the Forbes article I was reviewing. Or when I was looking up research articles, an ad for black masks that I bought on Amazon last week appeared at the very top of the page, the true banner ad. I additionally saw an on-page ad of the bridesmaid dress I bought for my best friends' wedding the day prior, that one felt too close to home. The consumer behavior of people is greatly impacted by the type of ads that pop up on our devices on a daily basis. Companies do this to get their products and/or services to the top of the consumers' mind. An exercise that I found myself doing one day was finding a word/topic/brand that I never, ever talk about and purposefully started talking about it *a lot* around my phone to see what would happen. In a mere 3 minutes, my Instagram had 2 ads for Jeeps – my key word – and my Facebook also had a banner advertising the car company. Try this at home, it is scary how fast and efficiently ads will appear. It is also noteworthy to mention that within any major journal or popular press article had a pop-up appear on the web page telling me my privacy rights before continuing on to the article.

It seemed very fitting to have all these privacy regulations appear as I was researching the exact matter. For example, when pulling up the Guardian article, a banner read "California residents have certain rights with regard to the sale of personal information to third parties. Guardian News and Media and our partners use information collected through cookies or in other forms to improve experience on our site and pages, analyze how it is used and show personalized advertising. At any point, you can opt out of the sale of all your personal information by pressing "do not sell my personal information." You can find out more in our privacy and cookie policy and manage your choices by going to 'California resident – do not sell' at the bottom of any page." These types of pop up messages are usually things that I just click accept to before reading, so it was incredibly fascinating to sit tight and read all the fine print words before clicking the pop-up button – because in this case it was really telling and insightful information about the server. The sleuthing has since become automated and how it once was tedious, it is now mechanized and happens within milliseconds. Consumers are "unwittingly giving away their information freely" (Pettijohn, 2019).

Finally, I am going to circle back to a previously mentioned topic – smart assistants. These were subject to legal issues, but it is necessary to understand what these are in depth and how companies use them to begin to work towards actions to be consciously aware of the devices merely sitting in our home, listening. A voice or smart home assistant is a "piece of software that communicates to the user audibly and responds to spoken commands." Examples include Amazon Alexa, Google Home and Apple's built-in Siri. As technology expands and becomes more intelligent, while sophisticated – more and more individuals are starting to integrate these into their homes. The speaker "Amazon Echo" launched the smart speaker trend. Google Home has been commercially and critically triumphant, due to "the vast amount of data Google already possessed. Apple followed these two, by releasing the Home-Pod recently – but has always been in the voice-assistant role due to Siri (CarbonTrack, 2018).

You can say commands "Hey Siri," "OK Google" or "Alexa…" and ask a range of commands such as turn it up, what's the weather, tell me a joke, play Bohemian Rhapsody, and a range of 200 third party skills. What's daunting is… they are always listening. Like mentioned earlier, they have to be actively listening to hear their trained wake phrase. Though useful, the continuous recording and analysis of speech can pose a serious threat to individuals' privacy. Here are ways you can turn these features off. If you want your Amazon Alexa to erase what it has heard you simply say, "Hey Alexa, delete everything I said today." If you would like to press further and delete old recordings you need to open the Alexa app and sign into the settings section. Select history and you'll see a list of all the entries. Select an entry and tap the delete button. If you want to delete all the recordings with a single click, you must visit the "manage your content and devices" page at amazon.com/mycd. If you are interested in your Alexa stopping listening all together, which defeats the purpose of having the product in the first place, nonetheless you go to settings on your Alexa account and choose Alexa Privacy, manage how your data improves Alexa, Help develop new features and turn off "use messages to improve transcriptions." Also grades how well Alexa performs, but lets users opt out of the program, by default (Haselton, 2019). For Google, to turn off the wake phrase, "OK Google," Go to Settings, Google, Search & Now, Voice, turn "OK Google" detection off. Google used to have a similar practice of "grading system" that Apple faced, and Google admitted that contractors leaked more than 1,000 voice recordings form Google assistance that was also suspended in light of the Apple scandal. Finally, for Siri to turn off its notorious wake phrase, one must go to iPhone settings, Siri & Search, and turn off "Listen for Hey Siri." Originally employees and outside contractors were allowed to listen to audio samples of the Siri interactions – but now will delete any recording which is determined to be an "inadvertent trigger" of Siri.

To conclude, candidly speaking, the screens described in the landmark novel '1984' are two-way televisions that George Orwell referred to as "telescreens." While the users think they are just for entertainment they actually pick up both audio and video of you while you're watching. Believe it or not, our smartphones and computers are doing the exact same thing. This sleuth-like behavior projects a shadow that there is a consistent private-eye over our everyday life. This phenomenon was merely once a concern outlined in this novel of how the *government* is listening – but our modern fear encompasses how *businesses* and *social media platforms* are also tapping into our "Big Data" routinely and it will only increase from here.

## RESEARCH METHODOLOGY

I gathered my research through a survey to gauge if there were any generational differences on technology's role in consumer manipulation. I wanted to assess the differing results of how young generation Z ranging to older individuals felt on the matter. I aimed to test how different generations have contrasting levels of threshold with this phenomenon. With ranging questions assessing consumers' comfortability with the idea of their devices constantly listening to them, to evaluating in what terms they find these actions acceptable – my goal was to seek out insight from people of all ages, ethnicities, backgrounds, etc. Within my context of retrieving research, I chose to collect data through a ten-minute survey. This 34-question survey serves as the heart of my research in which I will discuss promptly in the following section. It was to merely exemplify how consumers in our current world are impacted by our devices 'eavesdropping' on us. I intended to reach all ages to retrieve their opinion on the matter. I started out by sending out this survey to all my peers that I talk to on a regular basis to capture the audience of Generation Z, which are women and gentlemen roughly 21-23 years old. I

intended to reach the audience of 18-23 primarily through Greek life announcements through my sorority's "list serv" (email system) and through encouraging all my student involvement groups to take the survey as well. I sent it to many clubs and peers via email and group me to capitalize on the younger generation, since they needed to be 18+ to participate. To gain the millennial crowd, I sought out my sisters who are both in their early 30's to ask their friends to partake and I posted this survey on my social media where many of my followers completed it. Finally, I capitalized on the baby boomer generation, and older, by homing in on my parents age group and their network of friends on Facebook. After living in many cities across the United States growing up – there are friends and family members near and far that were willing to take 10 minutes to answer questions. My grandparents rounded out the survey and were a beneficial asset to capture all age groups. There was a drop-down segment of my survey that allowed respondents to choose: 18-23, 25-34, 35-44, 45-54, 55-64, 65-74, 75-84, and 85 or older. My Qualtrics survey that I conducted was submitted to and approved by the IRB, Institutional Review Board, and has been authorized to reach all areas of my target market. While my range needed to consist of 18-85+ individuals, my general demographics were all across the board but this was necessary to achieve my goal of analyzing potential generational differences.

**FINDINGS:**

With our social media platforms and devices as a whole non-stop collecting our personal data and then in turn using it to determine who we are and how approachable we are to "market" to – there is a looming question of – is this crossing the line? Is our overall privacy being breached and used at our expense? Or are we falling in line with what a lot of my peer's state of: not minding the "spying" due to the fact their digital footprint is ultimately "harmless" and in the end providing a more favorable user experience. There is a line and a balance between absurd/creepy and being favorable/beneficial.

The foundation of my thesis surrounded 4 main questions. The first being are people aware of their current levels of privacy? I went into depth on if they were aware that their devices are recording them constantly, even while offline – in the first place. Then I discussed certain scenarios and assessed their level of comfortability/threshold of how acceptable they deem these actions to be. I wanted to gauge how much of their data they personally *believe* is being tracked and if they were aware of how companies and/or the government use their data. The second category I addressed was: what issues related to privacy are people worried about? I asked questions that shed light on the threshold of whether the consumer finds it beneficial, or to put it plainly – creepy. I strategized these questions by asking whether the risks outweigh the benefits. To further analyze this category, I laid out scenarios/circumstances to determine when the participant feels gathering information is "okay." I evaluated if any participants were worried, and for those who were – I gathered insights on their uneasiness and what they do to 'prevent' the collection of their information. My next category encompassed what products people use that "invade their privacy." This is where I began to evaluate if people own voice-activated devices (due to this being the quickest way servers can pick up our information) and gathered insights on what devices people own. I gauged the participants opinions on which applications they *believe* listen to them the most. My final category embodied the idea of what steps people do to protect their privacy. Within this section it was feasible to ask how often they actually read the privacy terms and conditions. I wanted to measure their understanding of if they know why the government and companies gather their information and what they know about

other countries globally in how they protect their citizen's privacy in realm of technology – aka their consumer privacy protection regulations.

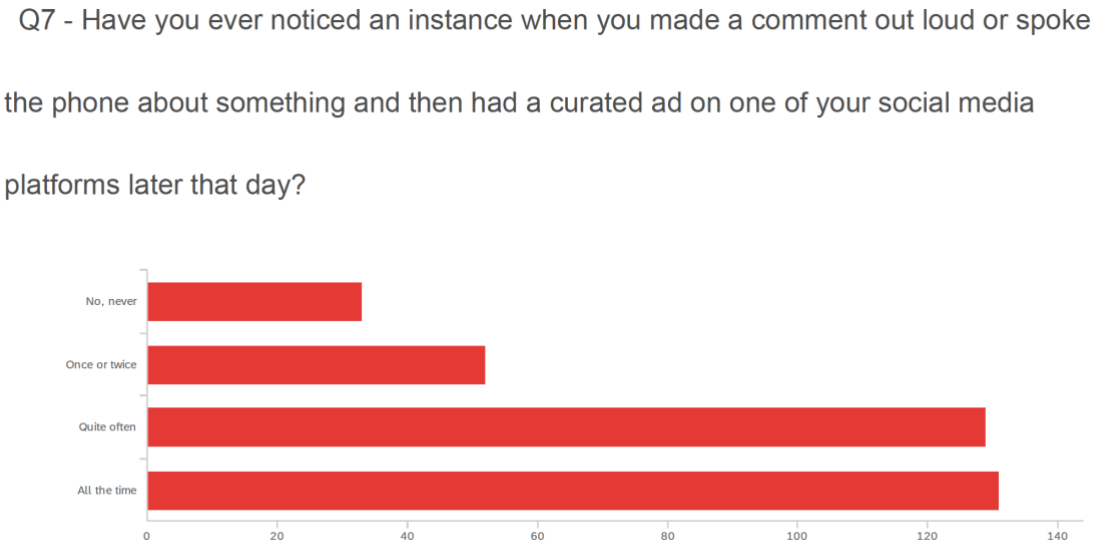
My survey polled a little over 400 participants and after filtering out completed surveys to gain the most accurate findings, the rough estimate per question was in the 340's

.

**Research Question 1:** ***Are people aware of their current levels of privacy?***

To explore this research question, I included 11 questions in my main survey. To begin, let's take a look at the nature of our phones tapping into our everyday conversations. I asked each participant if they have ever noticed an instance when they made a comment out loud or spoke on the phone about something and then had a curated ad on one of their social media platforms later that day. As shown in chart 1A, the answers strongly corelated to 'yes' as exactly 75% of the respondents either chose quite often or all the time. 260 of the 345 responses indicated this is something that is occurring in their everyday life.

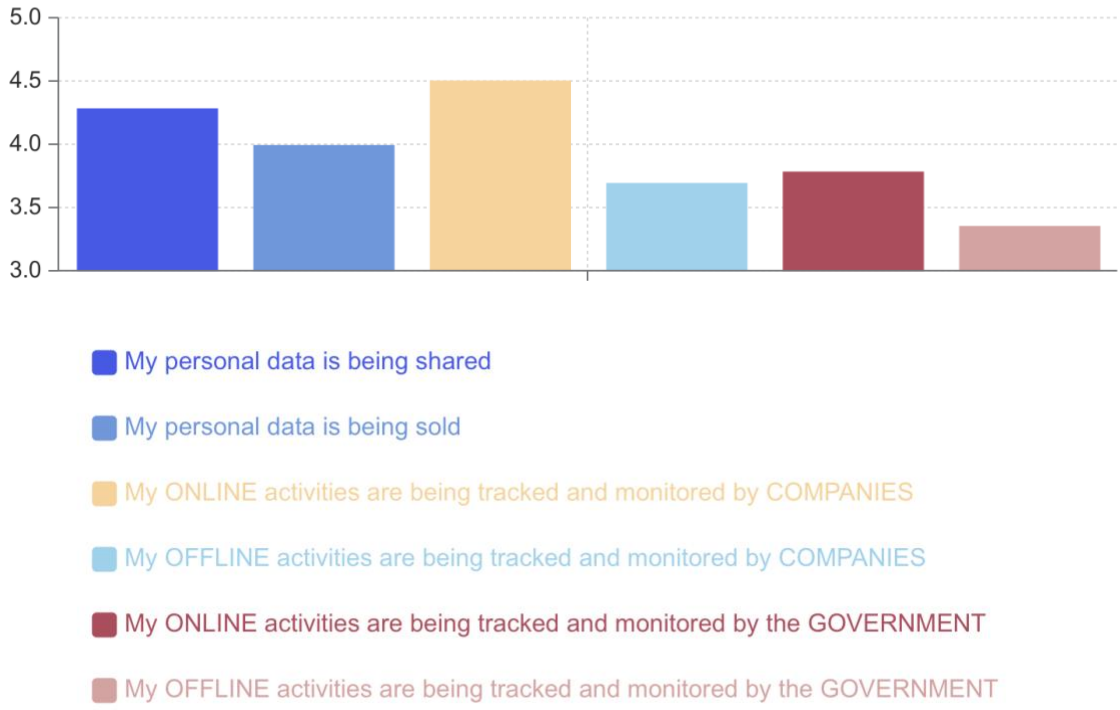
1A: Frequency of Curated Ads



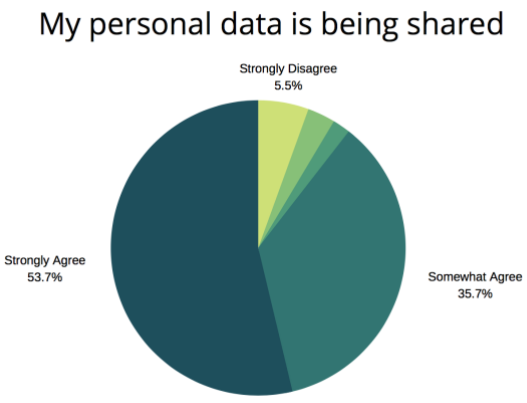

Next, I asked the respondents 6 general questions related to their personal data, both online and offline, being shared using a 5-item scale with responses from strongly disagree (1) to strongly agree (5.) The questions asked were: my personal data is being shared, my personal data is being sold, my online activities are being tracked and monitored regularly by companies, my offline activities are being tracked by companies, my offline activities are being tracked and monitored by the government, and finally my offline activities are being tracked and monitored regularly by the government. The chart(s) below summarize the average answer between these questions of 3.94 leaning slightly toward the agree side as you can see from chart 1B below. When comparing generations, the older generation of 40+ was more convinced than the 18-39 year old's that their personal data is being sold. This is proven through the average being 4.3 for the older generation and 3.76 for the younger folk. As a matter of fact, in all 5 categories the older generation was actually leaning more towards agree than younger. The category that had an overwhelming majority of the participants answering strongly agree was 'my ONLINE activities are being tracked and monitored regularly by COMPANIES' sitting at 232/362 – which is about

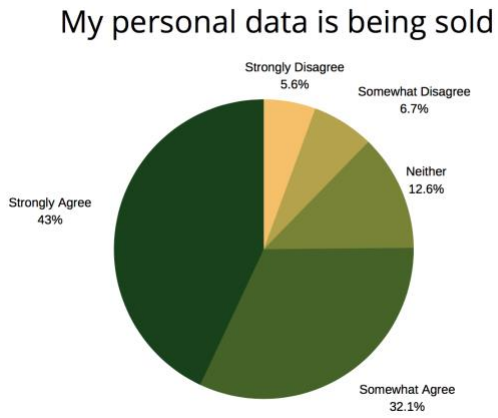
65%. Another thing I wanted to call out is that for all the categories, every single question had at least half the participants respond either “somewhat agree” or “strongly agree” about our data being shared/sold by both the government and firms. In order it was 89.47%, 75.14%, 93.922%, 66.48%, 70.08%, 50.70%. This demonstrates the belief the general public holds about outside parties using our information. Another thing to note, is that hardly any respondents said they strongly disagree with any of these claims, shown in chart 1C.

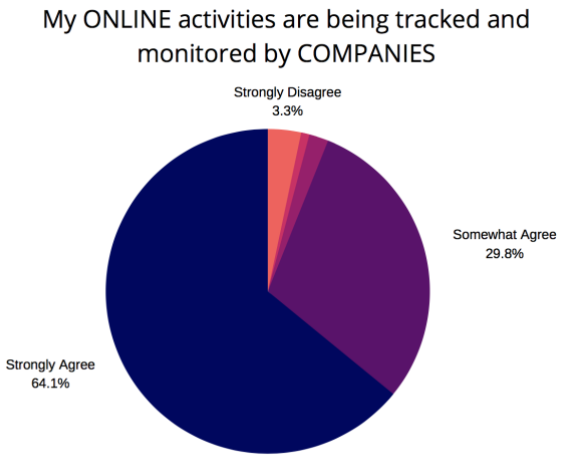
1B: Average Answer of Agreeability Matrix

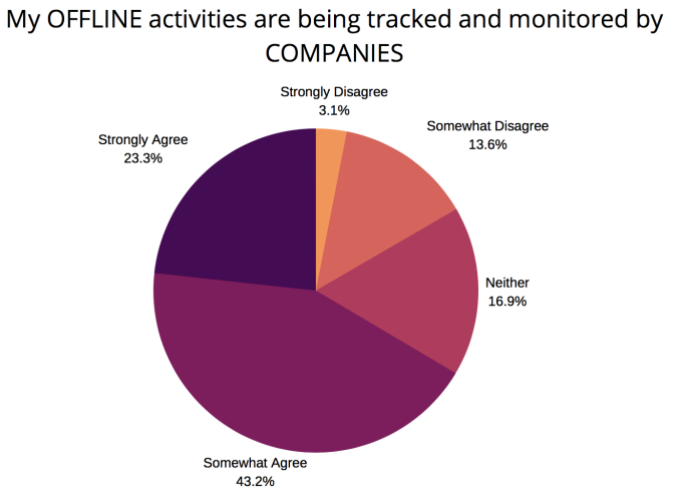


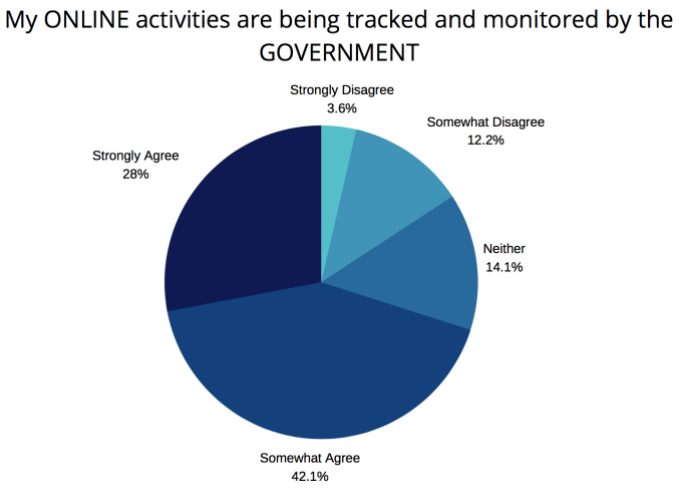

1C: Level of Tolerability with Both Online and Offline Activities Being Tracked

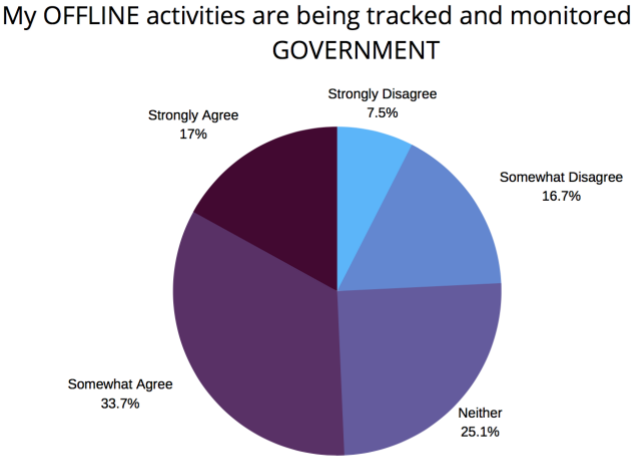




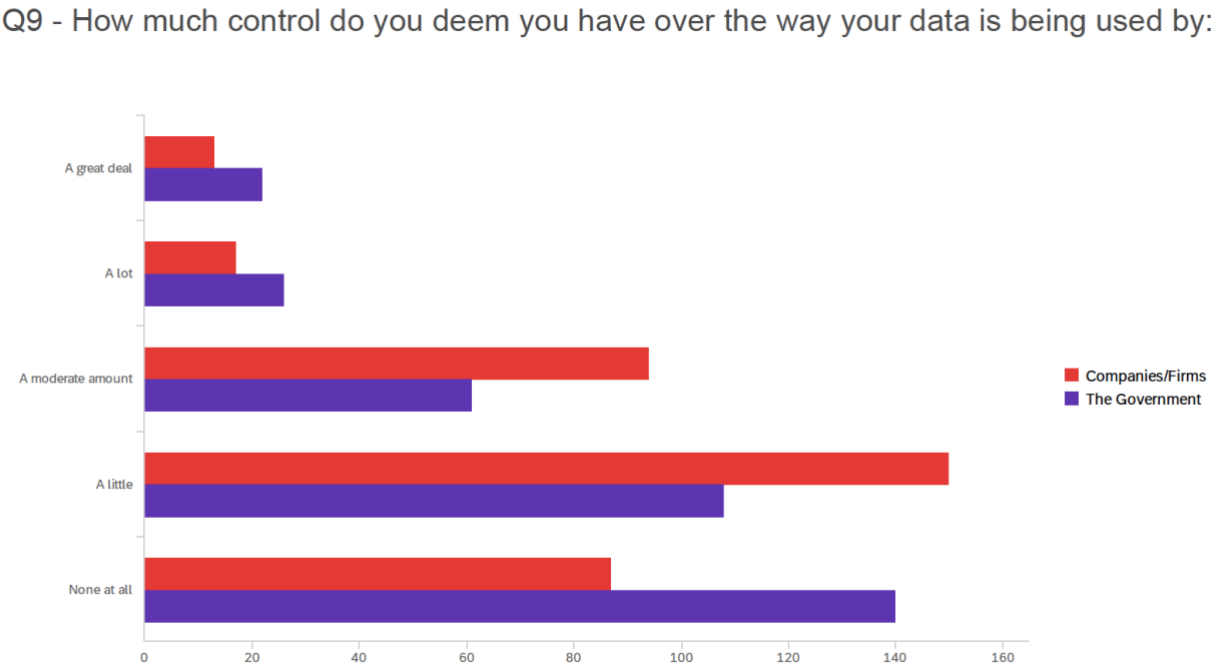




Next, I assessed the participants response to deem how much control they personally feel they have over the way their data is being used by both companies and the government as a whole. The responses clearly show that people feel they have hardly any control over the way their data is being used shown in chart 1D below. Just over 65% of participants said they have a little to no control at all when it comes to companies and just under 70% said the same for the government. This is such an outstanding percentage of the 360 participants I polled. This goes to show that we as people are aware that there is not much we can do when it comes to our data collection by outside parties.

1D: Reactions to Level of Control Individuals Perceive They Possess

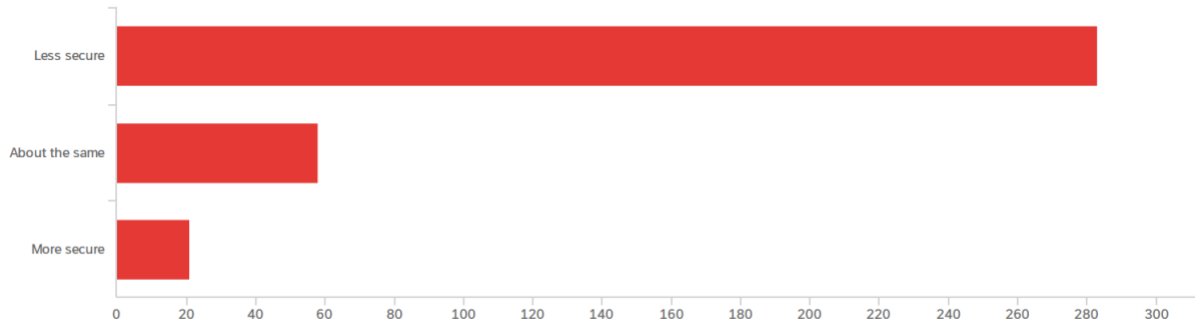



On a similar note, when I asked "on a scale from 1-10 how concerned are you with the ways that your data is being used by companies and the government" – the results show that individuals are slightly more hesitant/worried than not by the mean score being 6.29 for companies and firms and a slightly higher 6.51 when relating to the government. Out of the 300+ respondents, this just deemed they aren't entirely "okay" with this due to the slight hesitance of leaning slightly more worried.

When asking the overarching question about the past and how it relates to where we are today in terms of privacy, the respondents had an overwhelming response of 78.19% exclaiming that they think their personal data is less secure than it was 5 years ago. A little over 16% said it's about the same and only 5% of participants claimed that we are more secure. This is shown in chart 1E below.

1E: Security 5 Years Ago Vs. Now

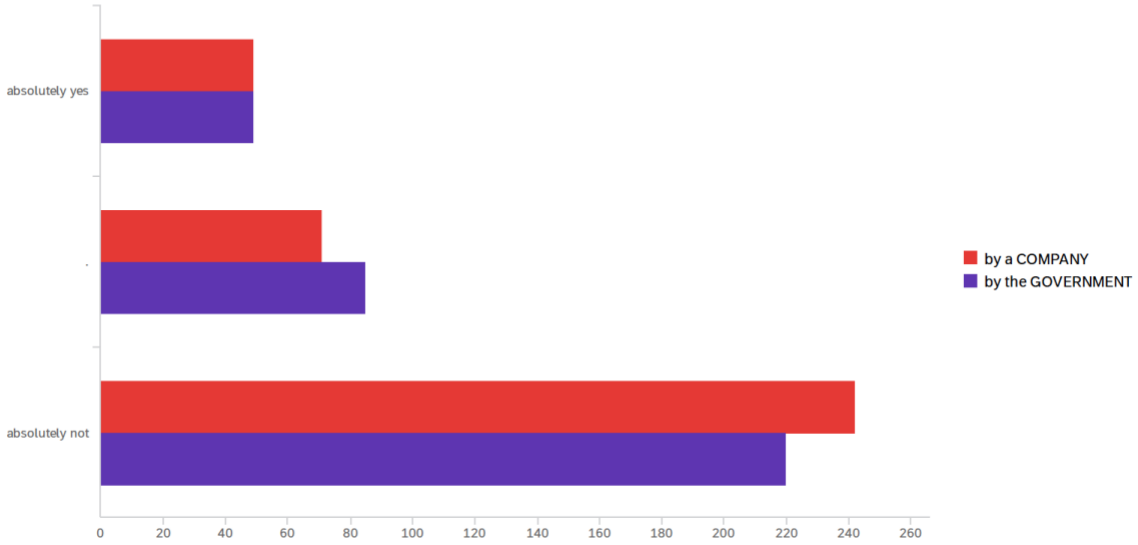
Q13 - Do you think your personal data is less secure, more secure or about the same as it was 5 years ago?




I followed up by asking "do you think it is possible to go through daily life without having your data being collected by either a company or the government" the respondents, once again, favored heavily towards the "absolutely not" column, shown in chart 1F below. A near 67% of respondents vouched a hard 'no' when it comes to companies collecting our information daily while a close 62% said the same for the government.

1F: Perception of Daily Life Without Our Data Being Collected

Q14 - Do you think it is possible to go through daily life without having your data collected by either a company or the government?

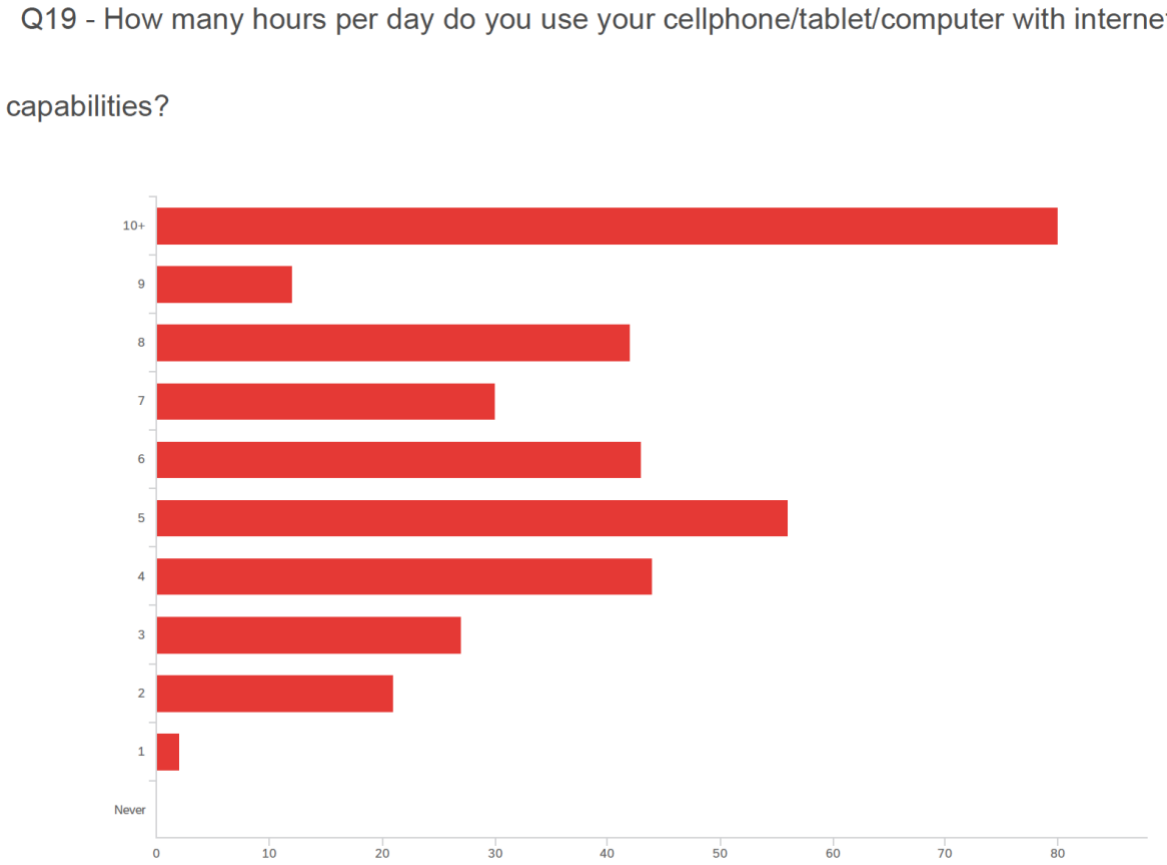



The next series of my thesis was discussion point where I asked my respondents how much of their data of what they do both online and offline – do they feel is being personally

tracked by companies and or the government. It was interesting to note that the mean for companies online, meaning they are actively using their device while the information is being retrieved, was 75% of data while for the government it was around 67%. For offline behavior, in regard to your device just sitting next to you and "listening" even when you are not actively using it, respondents shared only 50% by companies and a slightly higher 53% for the government. This can tie to the phenomenon previously mentioned of how younger generations claim that there is an "FBI agent living in my phone."

Next, to gauge how much time people spend on their devices per day, I asked how many hours from 1-10+ they deem that they are using devises with internet capabilities. A whopping 22% (80 people) claimed that they are on their devices for 10 or more hours while the rest of the answers varied from 1-9 hours shown in chart 1G below. An important callout is that not a single participant scored 0, showing that individuals today are on their devices at least once a day – modern life shown via the technology era.

1G: Frequency of Time Spent on the Internet




The next series I asked for the participants to respond with their range of agreeability ranging from strongly disagree to strongly agree over 3 main statements. They read: "I feel safe searching personal information on my technology/browsers, I believe the private browser is actually more secure and our devices <u>are</u> listening to us." My first call out, as you can see in 1H below is how around 30% of respondents don't feel safe searching personal information while

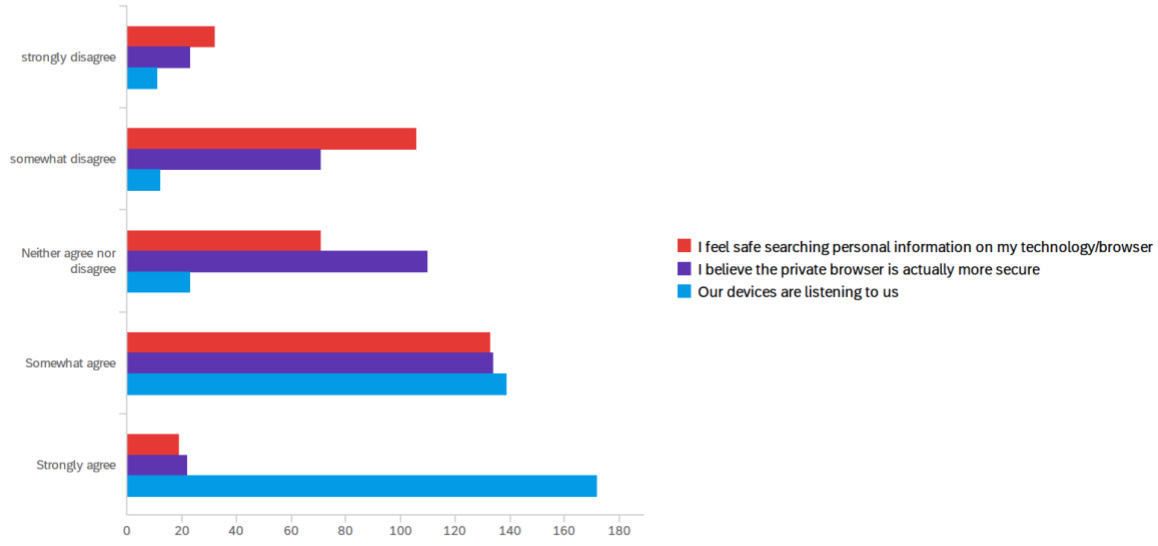
another 42.1% claimed they did feel safe. (Shown in blue circles below). There were some outliers of individuals who wholeheartedly did not feel safe (around 8%) and feeling extremely safe doing so (5%) For the next statement, just over 43% felt slightly more inclined that a private browser is more secure while 26% of participants were more hesitant to believe that. (Shown in yellow circles below). But 30% chose to neither agree nor disagree with this standpoint. Lastly, for our devises listening to us – a whopping 48% of participants stated that they strongly agree with this stance and nearly 39% "somewhat" agreed with this indicating that a shocking 6% was left alone on the belief that our devices are not listening to us. This is one of my strongest arguments within this research project indicating that 87% of the people I polled are in full agreeance of this phenomenon of our devices consistently listening to us. (Shown in the red markings below). When comparing generational differences, individuals 18-39 had a higher average of leaning towards strongly agree for this category than the older generation but both were still significantly strong. This proves that the younger generation is collectively more aware of what is happening with our technology. This data is shown below in charts 1H, and 1I.

1H: Breakdown of Feeling Safe Knowing Our Devices are Listening

| # | Field | strongly disagree | somewhat disagree | Neither agree nor disagree | Somewhat agree | Strongly agree | Total |
|---|---|---|---|---|---|---|---|
| 1 | I feel safe searching personal information on my technology/browser | 8.86% 32 | 29.36% 106 | 19.67% 71 | 36.84% 133 | 5.26% 19 | 361 |
| 2 | I believe the private browser is actually more secure | 6.39% 23 | 19.72% 71 | 30.56% 110 | 37.22% 134 | 6.11% 22 | 360 |
| 3 | Our devices are listening to us | 3.08% 11 | 3.36% 12 | 6.44% 23 | 38.94% 139 | 48.18% 172 | 357 |

II: Agreeability Matrix

Q49 - For each of the following scenarios, answer your range of agreeability:

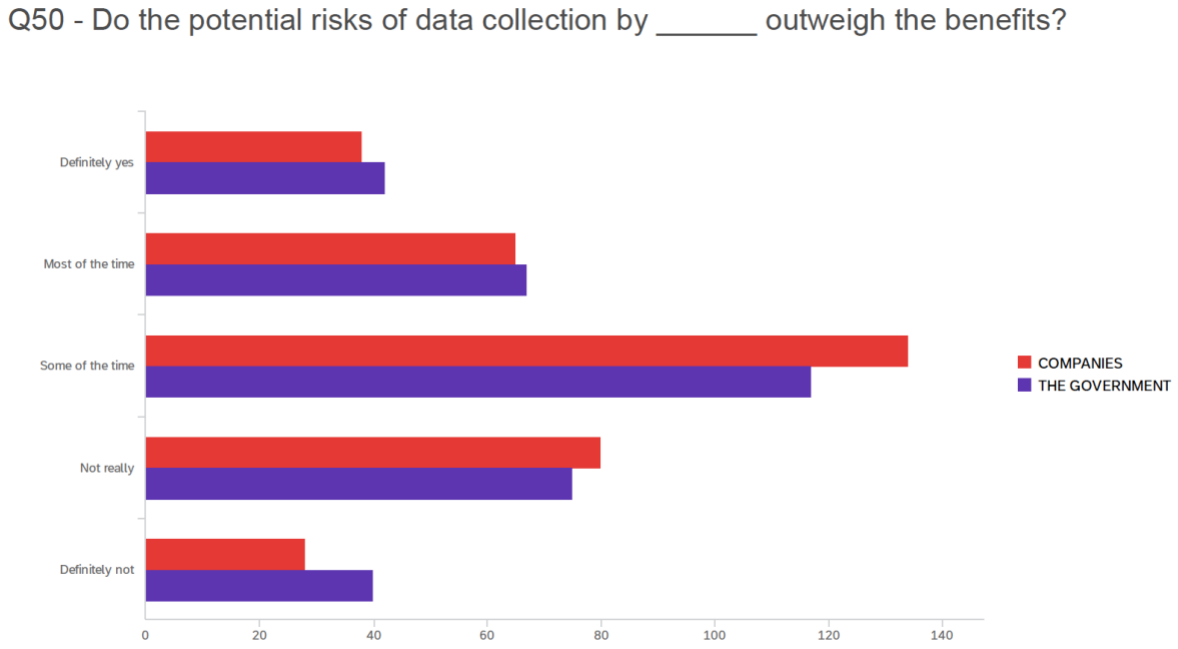


Via the discussion of feeling influenced by the ads that are appearing on our feeds due to our devices listening to us, drew me to ask the question of exactly how influenced they were by their ads that appear. Due to Instagram, and banner ads popping up while you're scrolling through websites being so personalized for myself I was very intrigued to see how others felt in this regard. I asked them to explain 0-10, with 0 being not influenced at all, 5 somewhat influenced and 10 being extremely influenced, there was a clear indication shown within the mean of exactly 4.99, indicated that overall people are "somewhat influenced:" by what is being shown. When comparing generations, the younger generation admitted being slightly more influenced than the older generation.

**Research Question 2*: What issues related to privacy are people worried about?***

To explore this research question in depth, I began by asking if the potential risks of data collection by either companies or the government *outweigh* the benefits. Essentially, I was aiming to hear the consensus on if people are more afraid of this vs. enjoy the benefits it implements into our lives. When analyzing the data that you see below in chart 2A and 2B, the largest group of respondents for both categories indicated that the risks outweigh the benefits some of the time. 38.84% said that for companies collecting their data, while 34.31% said it on behalf of the government. While this isn't a perfectly clear answer, it does indicate that individuals are more likely to be worrisome/fearful of risks within the realm of our devices listening versus feeling a weight lifted off their chest that things are more convenient/benefit them in some way. The responses summed up show a total of 68.7% concerning companies and 66.3% concerning the government leaning more towards the risks>benefits.

2A: Risks Outweighing Benefits




2B: Breakdown of Potential Risks Dominating the Benefits within Data Collection

| # | Field | Minimum | Maximum | Mean | Std Deviation | Variance | Count |
|---|---|---|---|---|---|---|---|
| 1 | COMPANIES | 1.00 | 5.00 | 2.99 | 1.09 | 1.19 | 345 |
| 2 | THE GOVERNMENT | 1.00 | 5.00 | 3.01 | 1.17 | 1.38 | 341 |

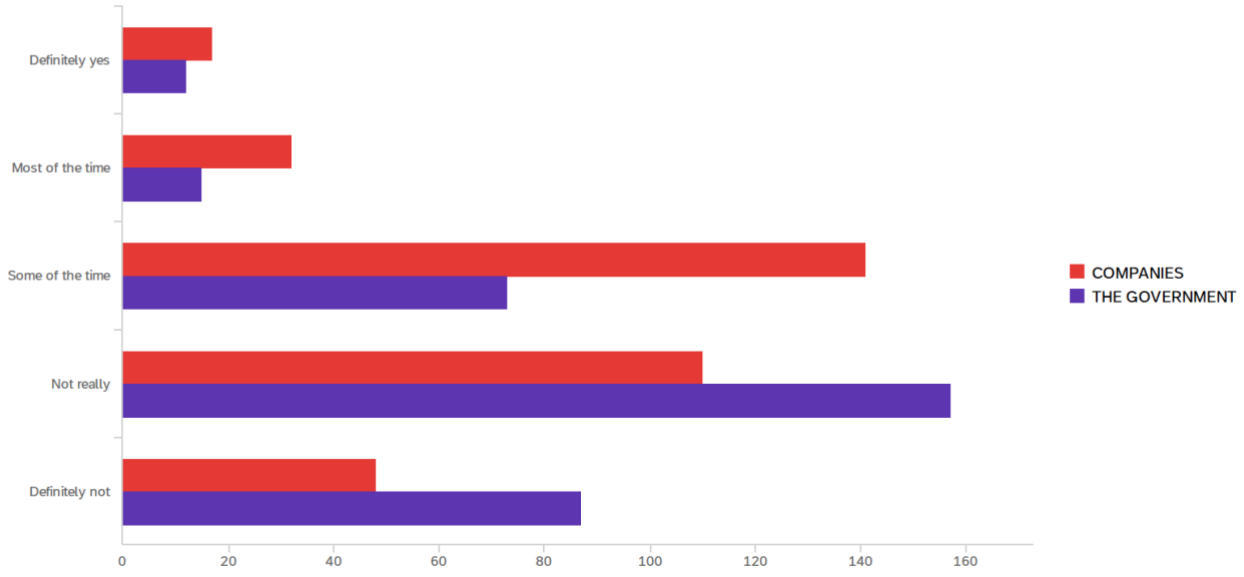
| # | Field | Definitely yes | Most of the time | Some of the time | Not really | Definitely not | Total |
|---|---|---|---|---|---|---|---|
| 1 | COMPANIES | 11.01% 38 | 18.84% 65 | 38.84% 134 | 23.19% 80 | 8.12% 28 | 345 |
| 2 | THE GOVERNMENT | 12.32% 42 | 19.65% 67 | 34.31% 117 | 21.99% 75 | 11.73% 40 | 341 |

To tag team this thought, I asked if the respondents personally benefit when companies/the government gathers information about them. I went on to clarify when companies gather information they will use it to personally cater advertisements, send intriguing emails, etc. The responses on this question heavily leaned towards "not really" or if anything at all "some of the time." This shows that it is not consistent & that the information the companies are trying to gather, use and produce personalization's to us simply are <u>not</u> sticking majority of the time. Just under 5% of respondents responded 'definitely yes' for companies and a whopping 3.49% said the same for government (shown in blue on 2D). Generationally, the older folks seemed to personally benefit more than the younger generation. While on the other hand over 45% and 71% for companies and the government respectively stated, "not really" and "definitely not" for feeling that personal payoff from these outside parties looking in. (shown in red on chart 2D)

2C: Frequency of Benefiting from Information Being Gathered

Q21 - Do you personally benefit when _____ gather information about you?

(Companies in terms of personally directed advertisements, intriguing e-mails, etc.)



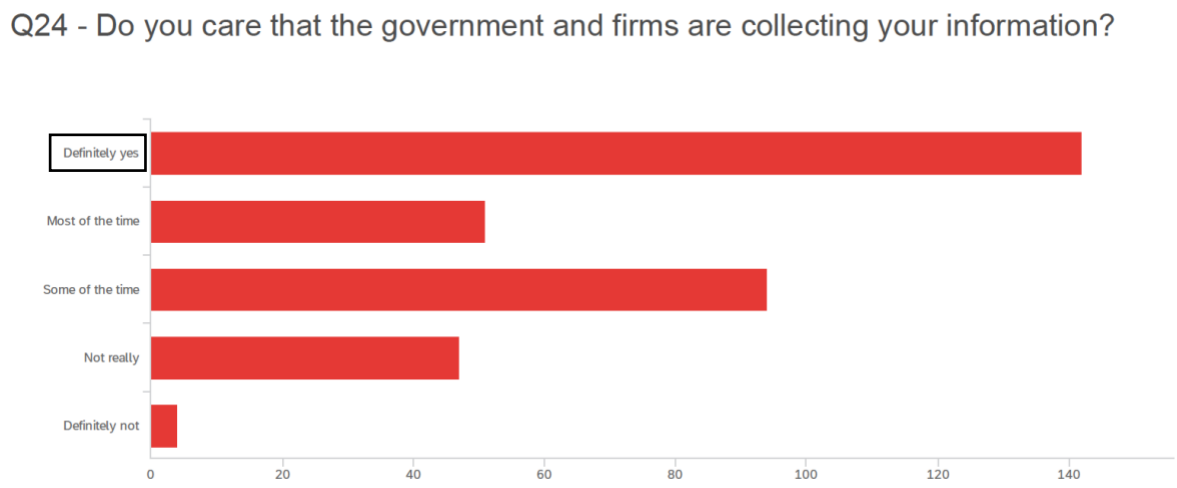
2D: Breakdown of Potential Personal Benefits

| # | Field | Minimum | Maximum | Mean | Std Deviation | Variance | Count |
|---|---|---|---|---|---|---|---|
| 1 | COMPANIES | 1.00 | 5.00 | 3.40 | 1.00 | 0.99 | 348 |
| 2 | THE GOVERNMENT | 1.00 | 5.00 | 3.85 | 0.96 | 0.93 | 344 |

| # | Field | Definitely yes | Most of the time | Some of the time | Not really | Definitely not | Total |
|---|---|---|---|---|---|---|---|
| 1 | COMPANIES | 4.89% 17 | 9.20% 32 | 40.52% 141 | 31.61% 110 | 13.79% 48 | 348 |
| 2 | THE GOVERNMENT | 3.49% 12 | 4.36% 15 | 21.22% 73 | 45.64% 157 | 25.29% 87 | 344 |

A very important question that I asked the respondents was “do you care that the government and firms are collecting your information?” 42% responded definitely yes and when combining this with the 'most of the time' row, that totals out to be around 57% of the “top 2 rows” indicating that majority of the people polled DO care about the act of outside parties listening in. Only 4 respondents, equaling just at 1% total responded they definitely do not care. Rounding out of around 15% of individuals seemed laxer with this act. One can see the responses are all across the board below in chart 2E, but the strongest callout reiterated is that people seem to generally care that our information is being collected.

2E: Opinion on Personal Information Being Gathered




In the next series of questions, I asked “In what circumstances do you think sharing information is okay?” I explained the scale of 1 being unacceptable to 5 being acceptable. The scenarios were as followed:

- Scenario 1: Poorly performing schools to share data about their students to a non-profit group seeking to help improve educational outcomes
- Scenario 2: Collecting data on all Americans to assess who might be a potential terrorist threat

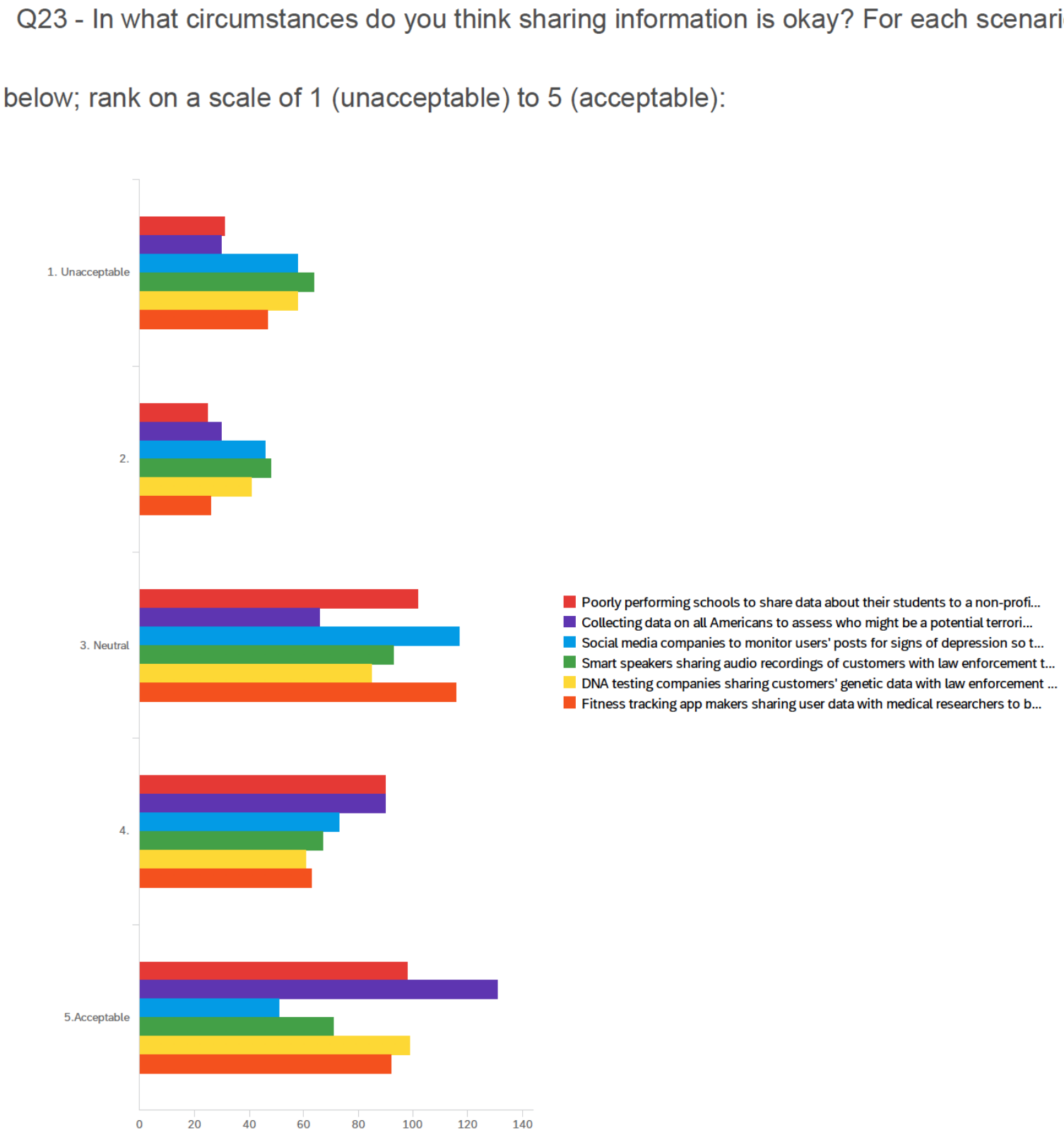
- Scenario 3: Social media companies to. Monitor users' posts for signs of depression so they can identify people who are at risk of self-harm to connect to council
- Scenario 4: Smart speakers are sharing audio recordings of customers with law enforcements to help with criminal investigations
- Scenario 5: DNA testing companies sharing customers/ genetic data with law enforcement to help solve crimes
- Scenario 6: Fitness tracking app makers sharing user data with medical researchers to better understand the link between exercise and heart disease

A few callouts I wanted to address for each scenario is that for the 1st one dealing with improving education outcomes, more than ¾ of the total respondents (83.82%) deemed that they were in the top 3 rows (neutral-acceptable) range for this circumstance. The next important finding is that within acceptable category, the strongest response was 37.75% in how it is 'acceptable' to collect data on all Americans to assess who might be a potential terrorist threat. To make the number stronger, when combining it with the second highest row of deeming above neutral, it was a whopping 63.68% of the total participants collectively agreeing that this is an acceptable scenario to gather ones' information. The 3rd and 6th scenario both had the highest response for the neutral category, indicating they don't favor it one way or another with nearly 34%, 117 and 116 individuals respectively, claiming 'neutral' for these circumstances with solving criminal investigations. Lastly, for scenarios 4 and 5 the answers were decently spread across the board as seen in charts 2F and 2G below.

2F: Breakdown of Level of Acceptability Between Each Scenario

| # | Field | 1. Unacceptable | | 2. | | 3. Neutral | | 4. | | 5.Acceptable | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Poorly performing schools to share data about their students to a non-profit group seeking to help improve educational outcomes | 8.96% | 31 | 7.23% | 25 | 29.48% | 102 | 26.01% | 90 | 28.32% | 98 | 346 |
| 2 | Collecting data on all Americans to assess who might be a potential terrorist threat | 8.65% | 30 | 8.65% | 30 | 19.02% | 66 | 25.94% | 90 | 37.75% | 131 | 347 |
| 3 | Social media companies to monitor users' posts for signs of depression so they can identify people who are at risk of self harm to connect to council | 16.81% | 58 | 13.33% | 46 | 33.91% | 117 | 21.16% | 73 | 14.78% | 51 | 345 |
| 4 | Smart speakers sharing audio recordings of customers with law enforcement to help with criminal investigations | 18.66% | 64 | 13.99% | 48 | 27.11% | 93 | 19.53% | 67 | 20.70% | 71 | 343 |
| 5 | DNA testing companies sharing customers' genetic data with law enforcement to help solve crimes | 16.86% | 58 | 11.92% | 41 | 24.71% | 85 | 17.73% | 61 | 28.78% | 99 | 344 |
| 6 | Fitness tracking app makers sharing user data with medical researchers to better understand the link between exercise and heart disease | 13.66% | 47 | 7.56% | 26 | 33.72% | 116 | 18.31% | 63 | 26.74% | 92 | 344 |

2G: Visual Representation of Ranging Levels of Acceptability for Each Scenario

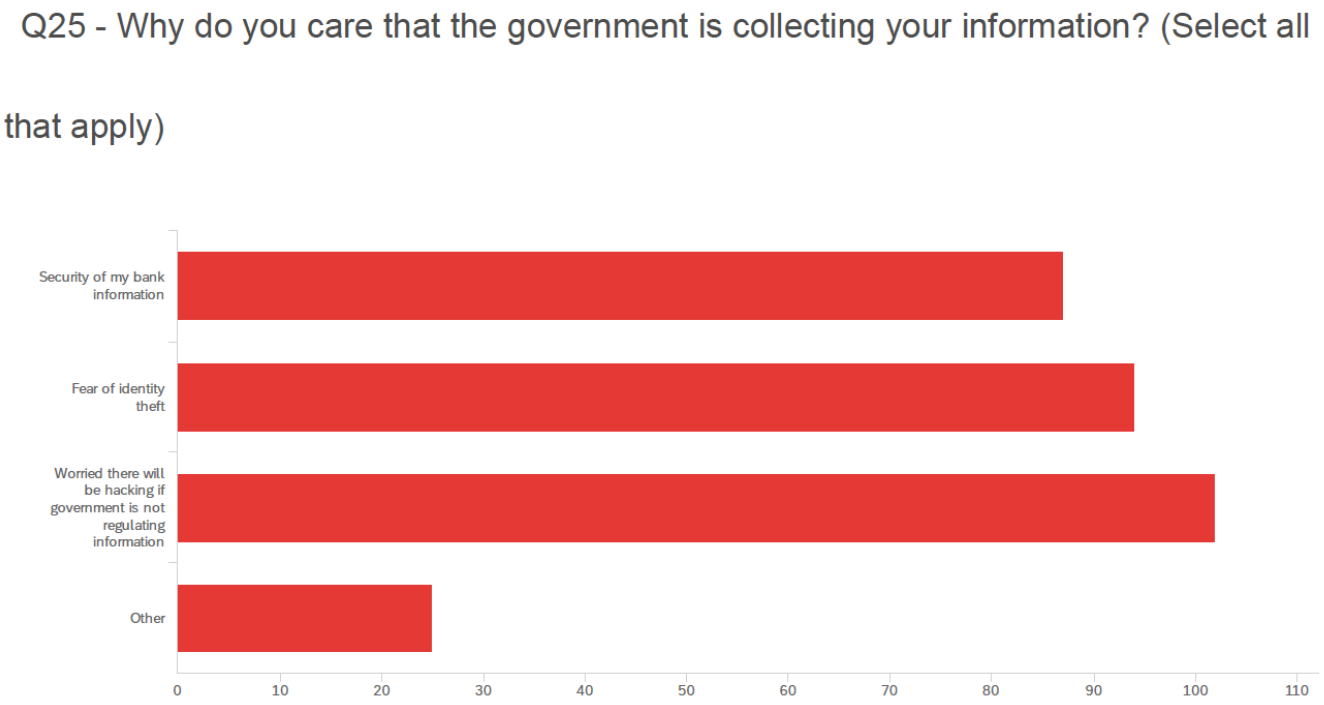


To further this research question, and to dig deeper, I asked "why do you care that the government is collecting your information" with the options listed as:

- Security of my bank information
- Fear of identity theft
- Worried there will be hacking if government is not regulating information
- Other

Overall, just about 28% people agreed with the bank option, 30% with identity theft fears, 33% with hacking and 8% said there as another reason why they cared so much that the government is collecting their personal information. This is shown in chart 2H.

2H: Reasons Individuals are Mindful of Their Information Being Collected




Within this "other" category, the responses were all across the board, here are some notable quotes that I will break into sections.

Some people simply just don't believe that it is in the cards for the government to have that much control, they expressed their worry in saying:

- "I don't believe it is the government's role to do so"
- "I do not trust the government"
- "Worried what the government will do with that information
- "We are living in a world with too much government control"
- "Control of America"

In a similar realm, many expressed this is a violation of our freedom and our rights that we were promised within our Constitution, here are some comments in that regard:

- "It is a violation of our rights for them to do so without granting out permission for their specific uses. Period. They are infringing on our rights for their own gain"
- "No privacy or freedom"

Some individuals found this to be crossing the line, beyond beneficial and into the creepy realm by stating:

- "It is uncomfortable"
- "I feel like they don't need to know what I am doing all the time, it reminds me of Black Mirror"
- "It's creepy and doesn't support the concept of freedom"
- "Overreach and abuse"
- "I don't stand to gain much by the government having my data. If companies do – I see the benefits for myself but when the government does it, it feels like it's only for their own gain"

Others are worried of what will happen if the government knows everything about us via our personal information, they expressed their concern with comments such as:

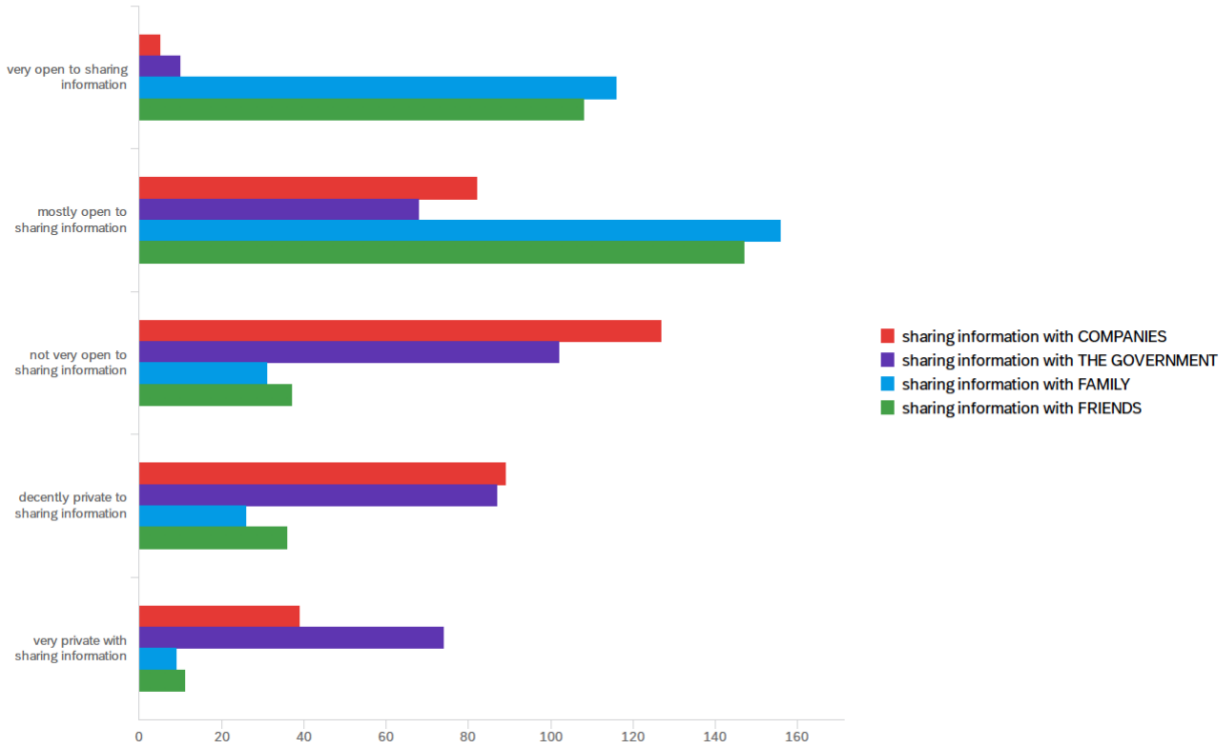
- "Not allowing us to have our own opinions"
- "Blackmail"
- "It is not the government's job to have all our information. Once they do, they can do anything and that is not what America is about"
- "For political use (i.e. collecting political affiliation information)"
- "I don't like the thought of the government knowing my personal thoughts, purchases and information"
- "I do not like big government, if things go bad and I oppose the government, they will know how to get to me"

To gauge how open individuals are sharing their information with anyone, not just companies and the government, I presented the statement of "we are sometimes more open with some people/groups than with others." I followed with asking "for each of the following, please indicate how 'open' you tend to be when it comes to sharing information with them" on a range from very open, mostly open, not very open, decently private, and very private. The categories were companies, government, family and friends. The results are shown in charts 2I and 2J below. An important call out that you can see is that the strongest category in the 'very' and 'mostly' open category was to their family members closely followed by their friends at 80.47% and 75.22% respectively (shown in blue in 2J). This result makes sense as these are relationships that you have that are built on foundation of trust so sharing information is not "uncommon." On the note of being incredibly open – a slight tangent is that 5 induvial proudly share their information with companies while 10 individuals do the same with the government (shown in orange below). The majority of the numbers sat right in the middle as they deem they're not very open to sharing information but weren't tipping over into the realm of purposefully being 'private' with what they do. This was an expected result as most aren't too comfortable with what's going on with our information to others at all times but aren't taking precautions to necessarily change the matter. 37% and 30% claimed this stance for companies and the government respectively. They just won't be handing their data or information on a silver platter. Another call out on the other end of the spectrum is that the strongest category that participants deemed to be "very private" with sharing was with the government with 74 responses indicating such (shown in green below). 37% were either decently or very private with sharing information with companies, 47% with government, only 14% with friends and a non-shocking low of 10% with family. This result was expected due to the fact you choose to open up to your family and chosen friends while it's more logical to feel the need to shelter that same information from the internet – in the fear it could fall into the wrong hands. These hands to some could be considered

companies/firms extracting everything about you for “their personal gain” and “big” government as a whole.

2I and 2J: Breakdown of Openness to Sharing Information with Different Groups

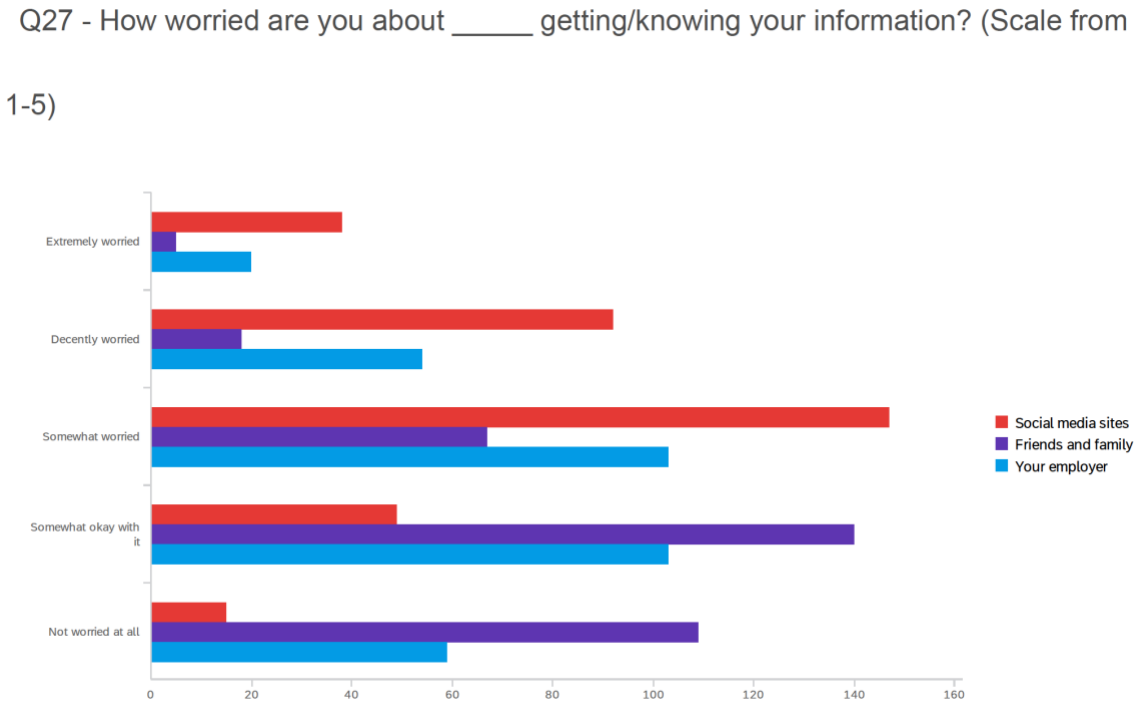
Q26 - We are sometimes more open with some people/groups than with others. For each of the following, please indicate how "open" you tend to be when it comes to sharing information.




| # | Field | very open to sharing information | mostly open to sharing information | not very open to sharing information | decently private to sharing information | very private with sharing information | Total |
|---|---|---|---|---|---|---|---|
| 1 | sharing information with COMPANIES | 1.46% 5 | 23.98% 82 | 37.13% 127 | 26.02% 89 | 11.40% 39 | 342 |
| 2 | sharing information with THE GOVERNMENT | 2.93% 10 | 19.94% 68 | 29.91% 102 | 25.51% 87 | 21.70% 74 | 341 |
| 3 | sharing information with FAMILY | 34.32% 116 | 46.15% 156 | 9.17% 31 | 7.69% 26 | 2.66% 9 | 338 |
| 4 | sharing information with FRIENDS | 31.86% 108 | 43.36% 147 | 10.91% 37 | 10.62% 36 | 3.24% 11 | 339 |

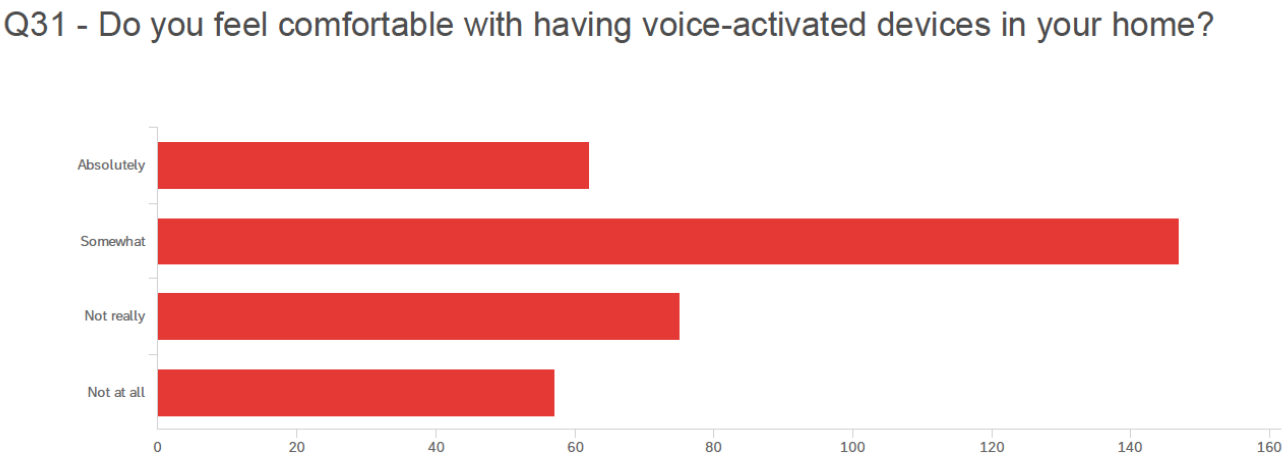
I followed up by asking "how worried are you about either social media sites, friends and family or your employer getting to know your information?" The least shocking, and most expected answer is that only 1% said they were extremely worried about their friends and family knowing their information, while people were the most worried about social media sites over their employer. 38% of the participants said they were either extremely or decently worried about these social media sites. Lastly, 48% said that they would be somewhat okay/not worried at all about their employer having their information.

2K: Threshold of Anxiety Surrounding Information Being Collected




The last question within this research question was "do you feel comfortable with having a voice-activated device in your home" and the responses were strongest at 43% for the response 'somewhat' and about tied at 16% for both sides of the extreme spectrum 'absolutely' and 'not at all.' This just shows that it really is personal preference and there are people who find this technology extremely beneficial while it seems some just deem this as invasive and creepy. The older generation seemed slightly more comfortable with having these in their home because they might be slightly less aware of how the media has portrayed the invasion of companies/government on our data, and the younger generation is on social media platforms to hear about this more.

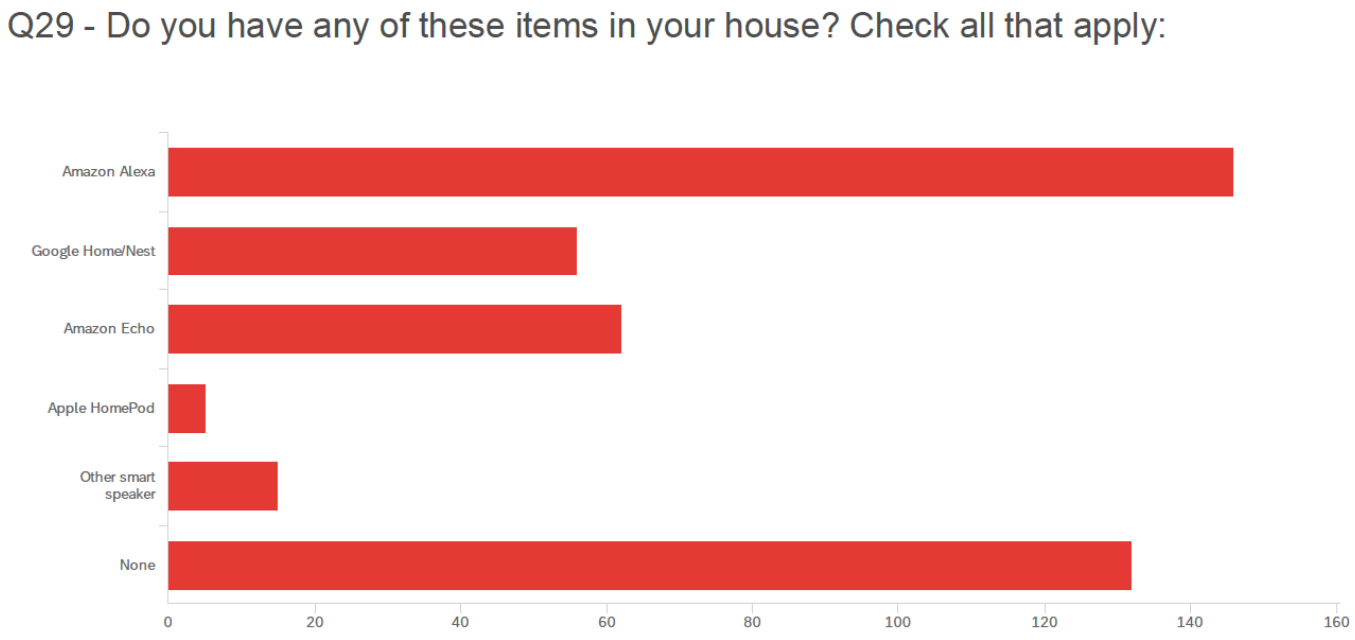
2L: Level of Comfortability Regarding Voice-Activated Devices




**Research Question 3:** ***What products do people use that are invading their privacy?***

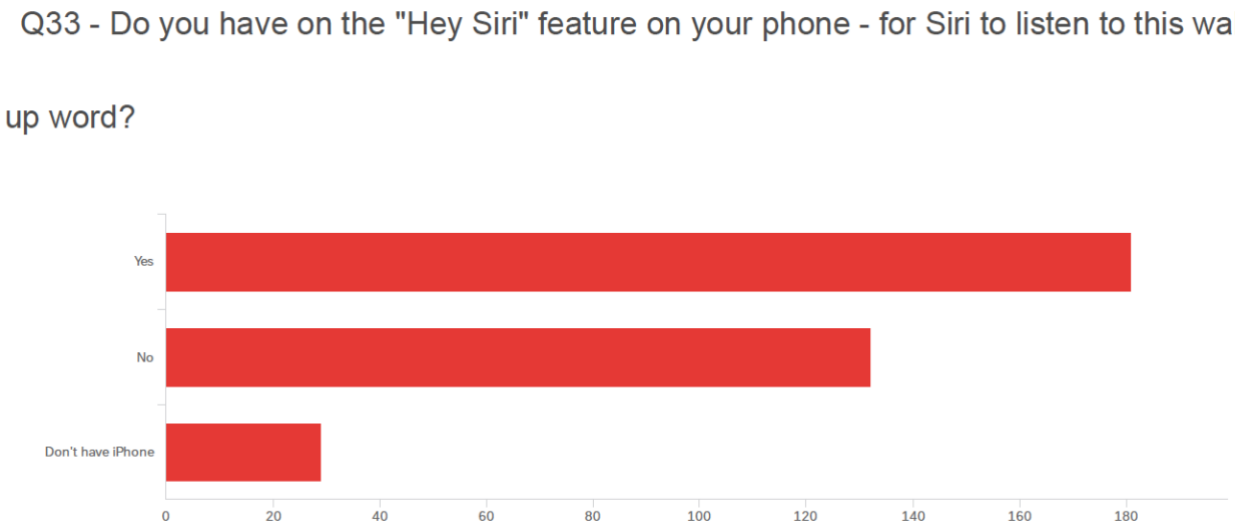
To fully evaluate the spectrum of the participants, I first needed to gain an understanding of the devices that they currently have in their home that would have a voice activated smart assistant that would be listening to the 'wake phrases' that I mentioned earlier. Upon polling them, 146 individuals had the tech giant Amazon Alexa in their home coming in at around 35%. The rest of the results showed that 14% had a Google Home, 15% with an Amazon Echo, 1% with an Apple HomePod, 4% with another type of device while 32% do not have a smart speaker in their home at all. These percentages are shown in chart 3A below.

3A: Voice-Activated Products Participants Own



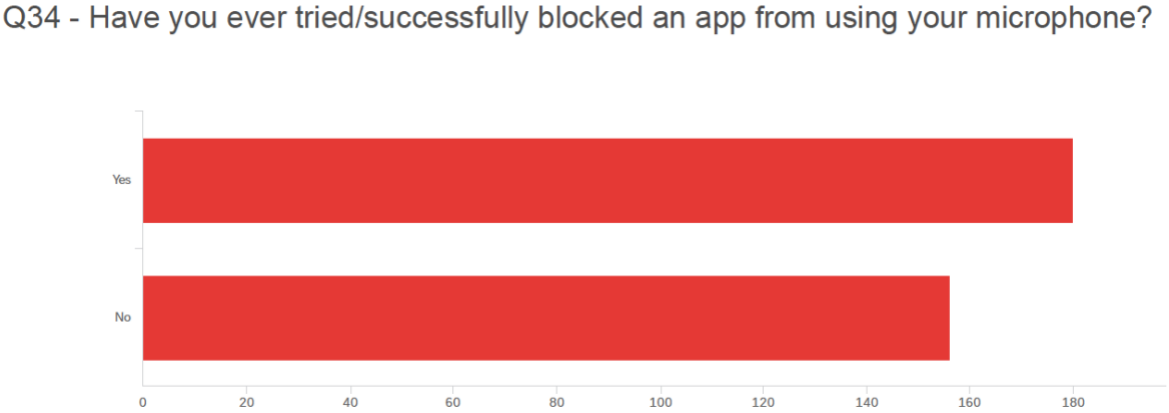
In a similar realm, I asked participants if they have an iPhone, in which only 8% of the individuals I pooled did not, if they have the "Hey Siri" feature turned on. It was intriguing to see that half of the remaining respondents answered yes. While the last 42% answered that they do *not* have it turned on. This was very thought-provoking to analyze in knowing for the 58% that answered yes, their phones are actively listening to them and what they do in order to constantly be listening to the wake-up phrase and how this can be Apple consistently pulling data from them. This is shown in the chart below.

3B: Amount of "Hey-Siri" Prompts Activated/Turned On



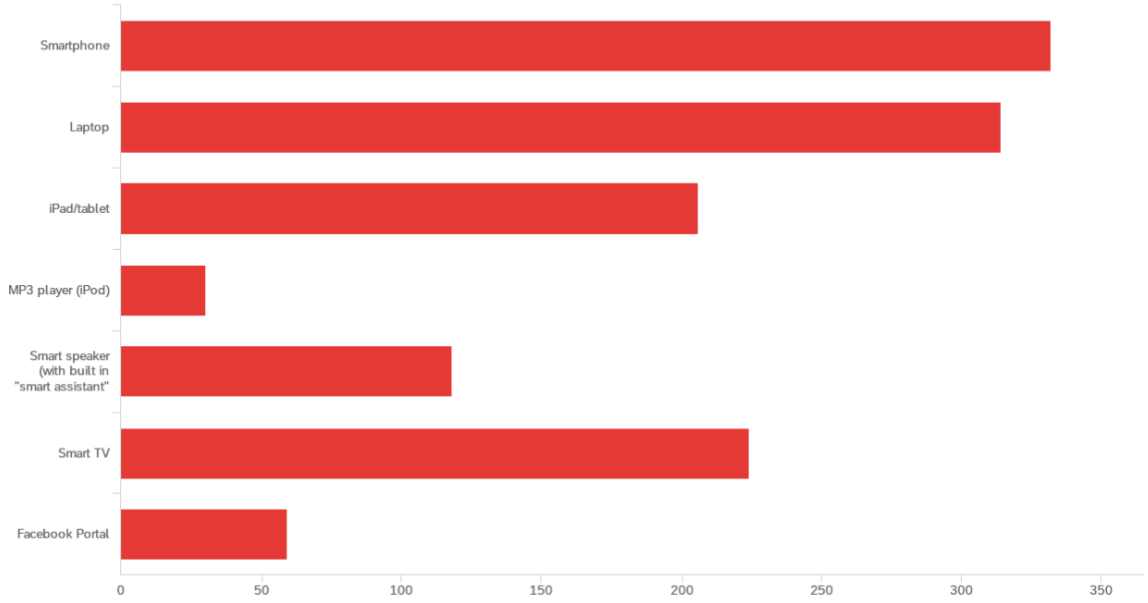

To support this claim, I went on to ask, "have you ever tried/successfully blocked an app from using your microphone?" and the results were pretty evenly split. With nearly 54% saying yes and a daunting 46% answering no – it seems that half of the respondents know how to go in and protect their data from getting extracted via microphone/conversation/etc. while the other half are either uneducated, have not tried or merely do not care. This is show in chart 3C below.

3C: Success in Blocking Microphone Access on Apps




In regard to people ranking their devices, people clearly have smartphones and some sort of laptop computer. iPads/tablets and smart TVs fell shortly after the two giants while smart speakers, Facebook Portal and mp3 players were chosen last. This is shown in the chart 3D below upon asking; "what pieces of technology do you own?"

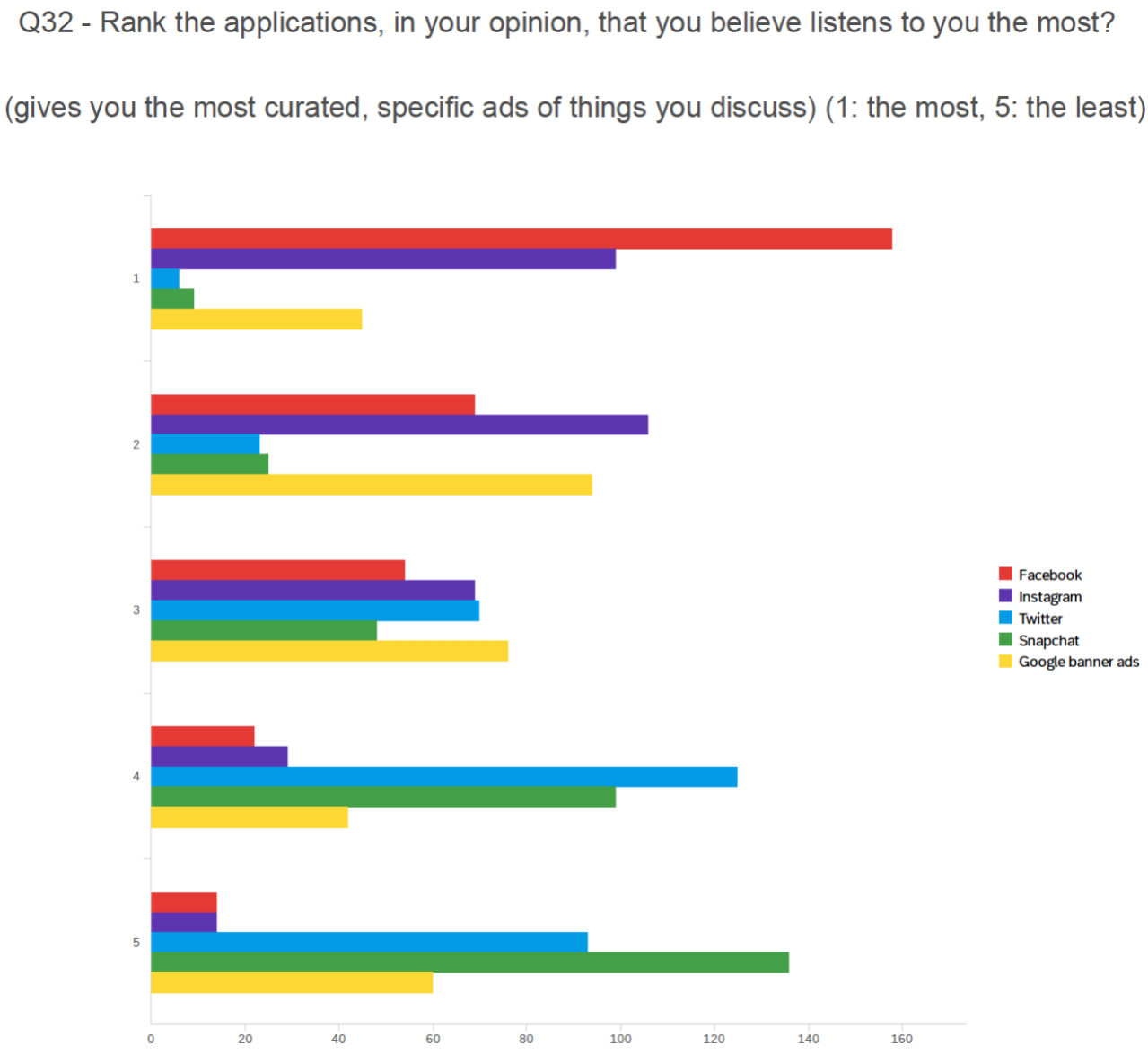
3D: Tally of Technology in Possession of Participants
Q30 - What pieces of technology do you own?




In regard to "ranking" applications that are eavesdropping on us, I asked the participants to evaluate their perception of 5 platforms: Facebook, Instagram, Twitter, Snapchat, and Google Banner Ads and determine their scale of which gives the most curated, specific advertisements based off things they discuss out loud. With 1 being the highest listener, and 5 being the least – the results are shown in chart 3E and 3F. Facebook was the clear winner on the with the average score being 1.94 resulting in many individuals ranking them as #1. Just under half of the total participants did this, coming in at 49.84% The next highest app that the general public believes is listening to us the most was Instagram. They received the highest number of votes for second place, but collectively with the individuals who ranked Instagram as #1, the combined percentage was 65%. The stark comparison between Facebook and Instagram when combining being ranked as 1 and 2 was 72% and 65% respectively. On the other end individuals strongly voted Snapchat for being in last place amongst the others listed as nearly 43% voted Snapchat to be in 5th place. Individuals also deemed Twitter wasn't a strong contender to be in the lead and this is shown through nearly 69% ranking it as either 4th or 5th. The last call out I wanted to make is that Google banner ads ranked all across the board not significantly showing out in any of the 5 spots. 3E: Breakdown of Apps' Rankings

| # | Field | 1 | | 2 | | 3 | | 4 | | 5 | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Facebook | 49.84% | 158 | 21.77% | 69 | 17.03% | 54 | 6.94% | 22 | 4.42% | 14 | 317 |
| 2 | Instagram | 31.23% | 99 | 33.44% | 106 | 21.77% | 69 | 9.15% | 29 | 4.42% | 14 | 317 |
| 3 | Twitter | 1.89% | 6 | 7.26% | 23 | 22.08% | 70 | 39.43% | 125 | 29.34% | 93 | 317 |
| 4 | Snapchat | 2.84% | 9 | 7.89% | 25 | 15.14% | 48 | 31.23% | 99 | 42.90% | 136 | 317 |
| 5 | Google banner ads | 14.20% | 45 | 29.65% | 94 | 23.97% | 76 | 13.25% | 42 | 18.93% | 60 | 317 |

3F: Rankings of Applications Based on Most Curated Advertisements

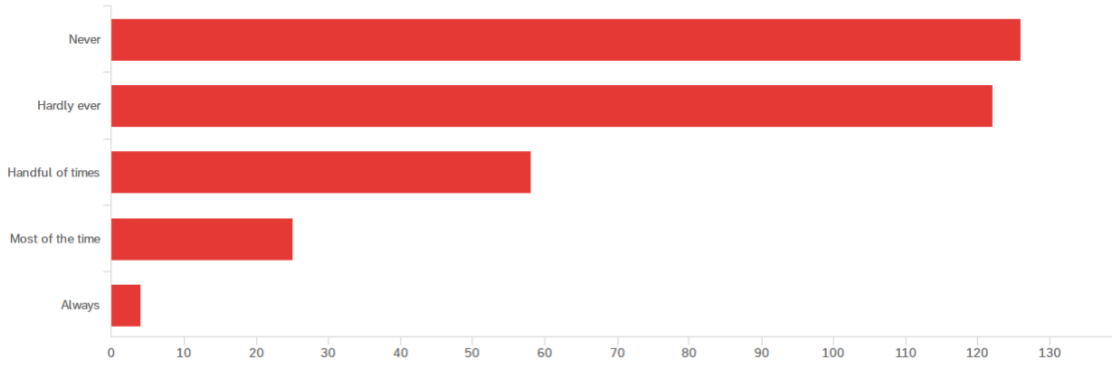



**Research Question #4:** ***What steps do people take to protect their privacy?***

To dive in deep to this final topic, I opened with asking "how often do you read the privacy policy/terms and conditions statements before clicking 'I agree' when downloading an app/using technology?" An outstanding 74% of the participants responded either never or hardly ever. A noteworthy total of 4 individuals of the total 335, said this is something that they always do. The other responses are shown in chart 4A below.

4A: Frequency of Reading Terms and Conditions Statements When Prompted

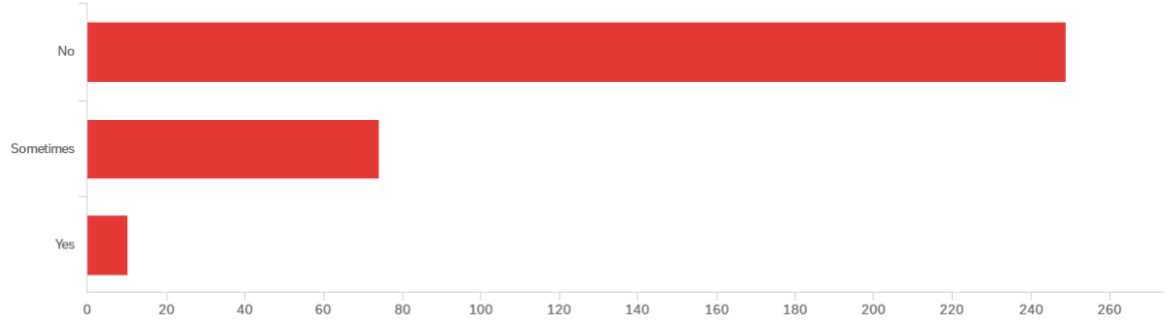
Q35 - How often do you read the privacy policy/terms and conditions statements before clicking 'I agree' when downloading an app/using technology?




Following that question, I asked, "when you do, do you read them ALL the way through" exactly 3/4$^{th}$s of the participants answered an astounding 'No' while 22% confessed "sometimes" and only 3% actually reads them all the way through. To put it into perspective, that equivalates to only 10 of the 333 respondents sitting down and reading every bit of what they are signing away to.

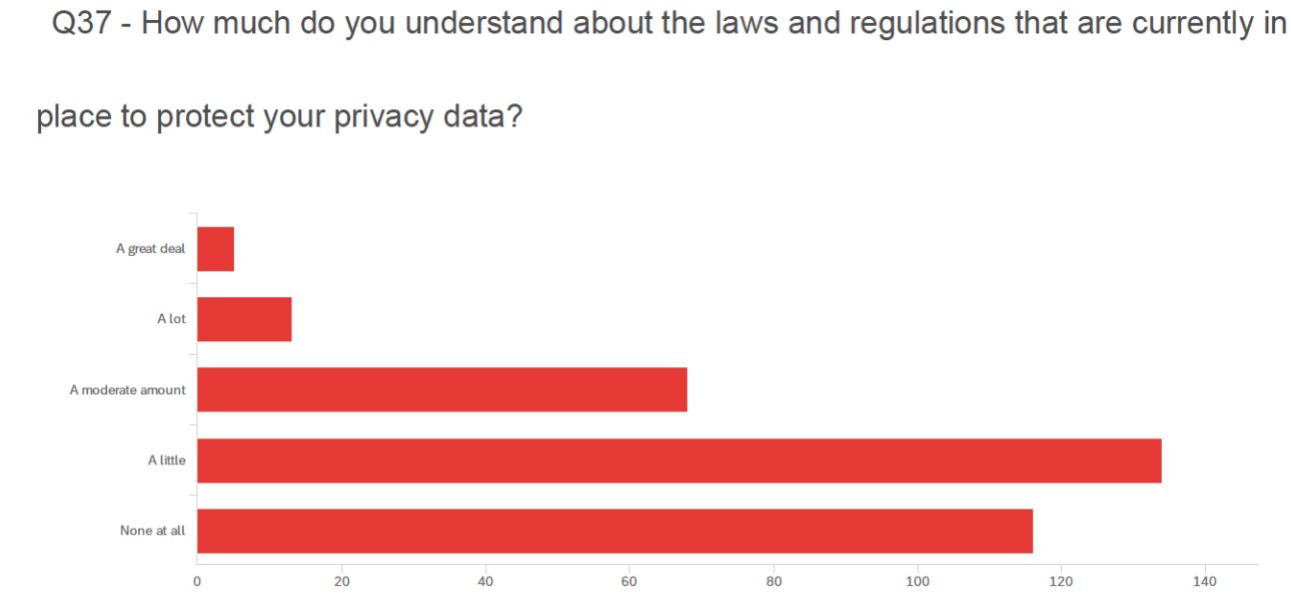
4B: Frequency of Comprehensively Reading Terms and Conditions

Q36 - When you do, do you read them ALL the way through?



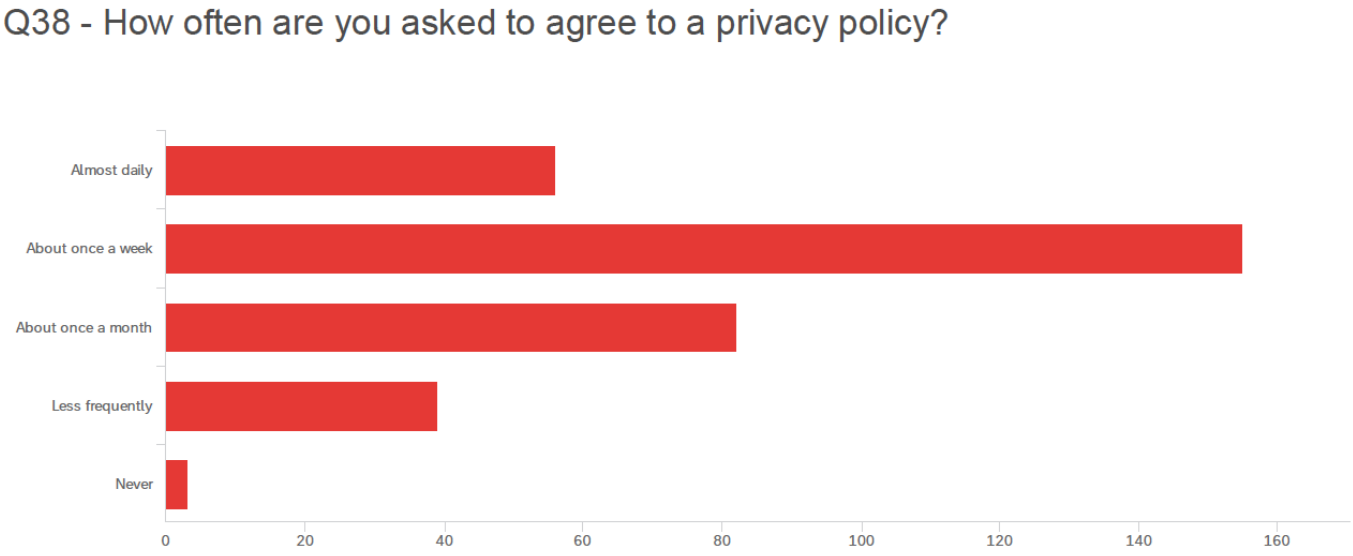

When asking about the laws and regulations that are currently in place to protect our data privacy, I asked how much the participants understood. Only 1.5% of the 336 polled, responded 'a great deal' and on the other end of the spectrum 35% responded 'none at all.' The largest section of respondents at just under 40% responded that they know "a little" – which is exactly what I was predicting within this realm. It seems that our citizens aren't aware of what laws are in place – a large part due to the fact that *there really **isn't** anything in place.* The stark reality that I hit on earlier is demonstrated here, while states like California and few others are trying to implement regulations similar to the EU – there really isn't much concrete for the US as of today.

4C: Level of Consciousness Regarding Current Regulations in the U.S.




Following that question, I wanted to gauge just how often these privacy policies are even appearing for individuals and the responses show that around 46% are seeing them arise around once a week while a shocking 16.72% are seeing these consistently, as they responded they appear *daily.* Another note I want to call out for this question is that only 3 individuals, ranking in at just under 1%, claimed they never see privacy policies showing that close to everyone surveyed has at least come across a few of these in their lifetime. After checking the age range of the 3 individuals who said "never," 2 were from Gen Z and 1 was a millennial – which was surprising.

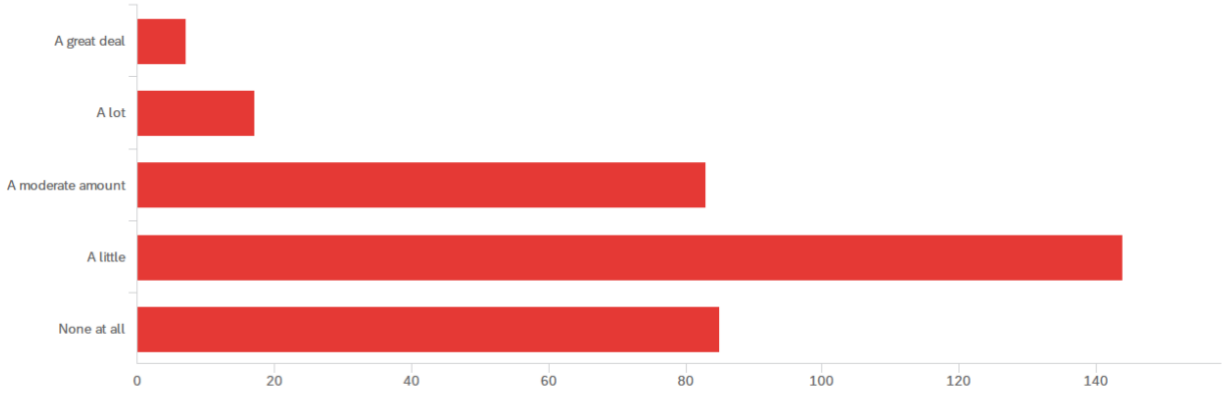
4D: Frequency of Privacy Policy Pop-ups



My next question asked how much is understood about what the government and companies are doing with the data that they are collecting. Individuals answers were across the board, but the strongest section deemed that individuals strongly felt they understood "a little" to a "moderate amount" as nearly 68% participants chose these options. On a similar note, around 25% of the individuals claimed they understood nothing at all – proving that sometimes we are blindly signing away information, or getting data taken from us without our full conscious consent – and have no idea what any of it is actually used for. Whose gain is it for, us or the third party? This is a question I discussed in my literature review and that stays ever present on my mind daily. Results are shown in the chart below.

4E: Awareness of How Our Data is Being Used

Q39 - How much do you understand what the government and companies do with the data that they collect?




In that regard our current system of data collection, aka privacy protection, is built on the idea that consumers are given notice about how firms collect and use data. Tying back to how our devices can use our microphones to tap in to our personal lives, I asked the participants "how often are you asked to approve a policy before your devices listen to you" with '0' being never and '10' being always. The average response for this was 5.43 which indicates for most, it's about 50% of the time when combining all the data together. This is shown briefly in the data chart below.

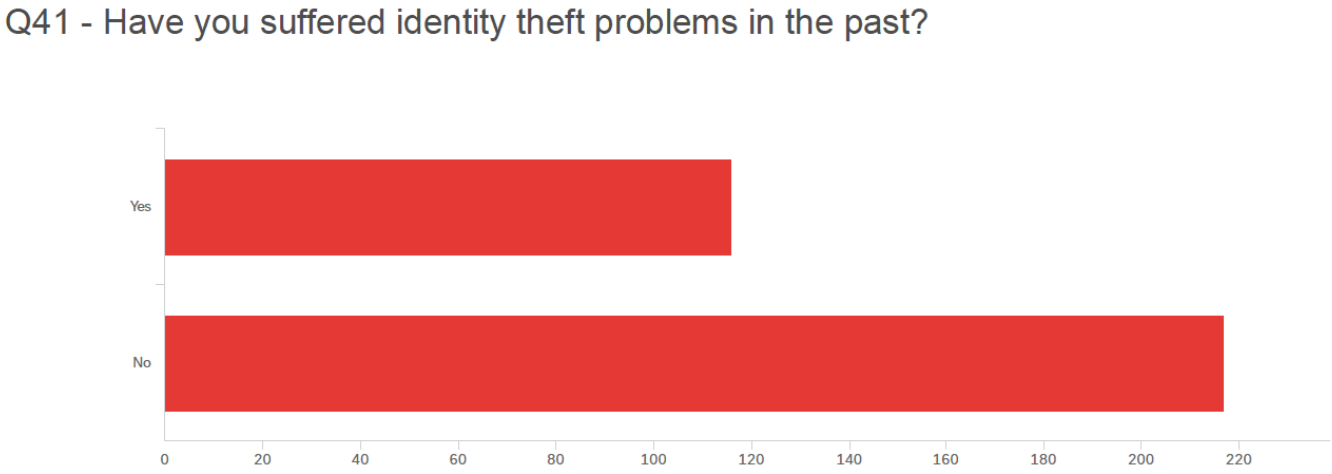
4F: Breakdown of Average Answer

Q40 - Our current system of data collection (privacy protection) is built on the idea that consumers are given notice about how firms collect and use data

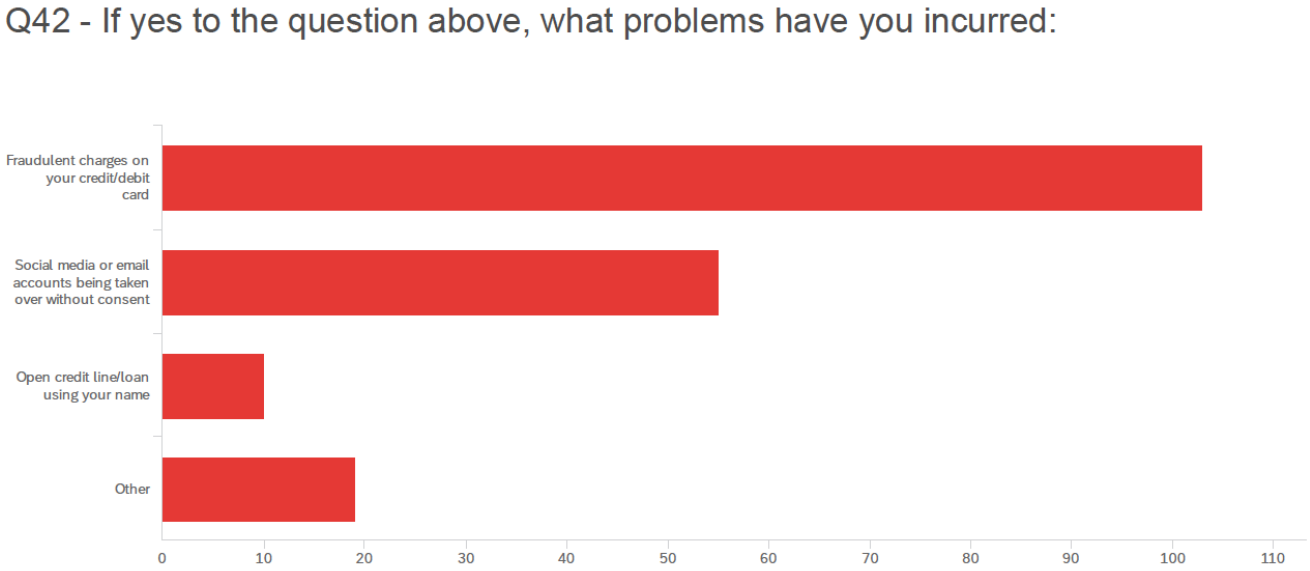
| # | Field | Minimum | Maximum | Mean | Std Deviation | Variance | Count |
|---|---|---|---|---|---|---|---|
| 1 | How often are you asked to approve a policy before your devices listen to you? (0:never - 10:always) | 0.00 | 10.00 | 5.43 | 2.98 | 8.87 | 308 |

To discuss the implications of identity theft problems potentially being the source of those who are so scared about being open with their personal information, I asked if the participants have suffered with identity theft in the past. The responses indicated that while 65% have not, over 100 individuals responded yes – equivalating around 35% total. This was gripping due to the fact that the follow-up question asked what problems they have incurred. I first asked if it was either due to fraudulent charges on your credit/debit card, in which 55% admitted to dealing with. Next, I asked if it was due to their social media or email accounts being taken over without consent and nearly 30% responded yes. And finally, I asked if it was dealing with an open credit line/loan using their name and only 5% corresponded with this. There were 10% that have dealt with another form of identity theft. These results are shown in chart 4G below.

4F: Recognition of Identity Theft Issues




4G: Breakdown of Identity Theft Problems

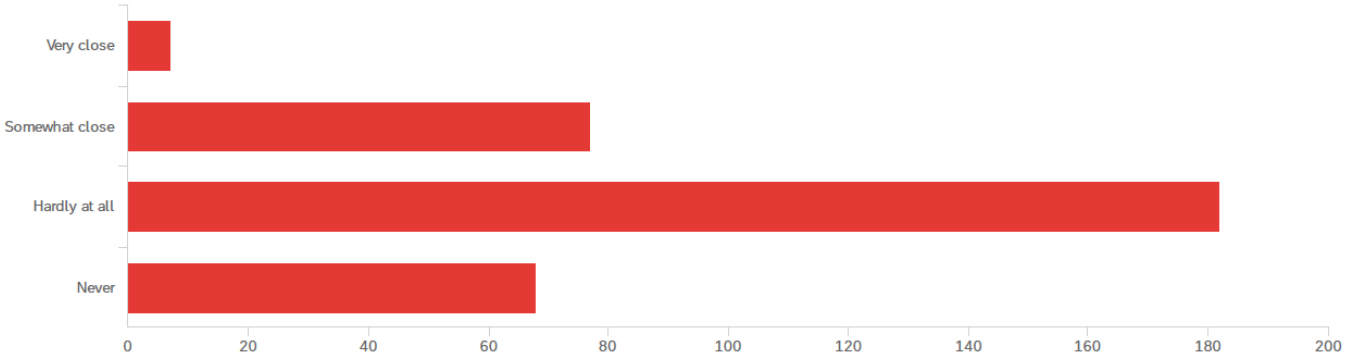



To follow up and just see how closely individuals are following privacy news, only 2% truthfully claimed they do while a whopping 75% answered either hardly at all or never! This

allowed the remaining 23% to admit that they follow it somewhat close but not as much as they could.

4H: Attentiveness to Privacy News

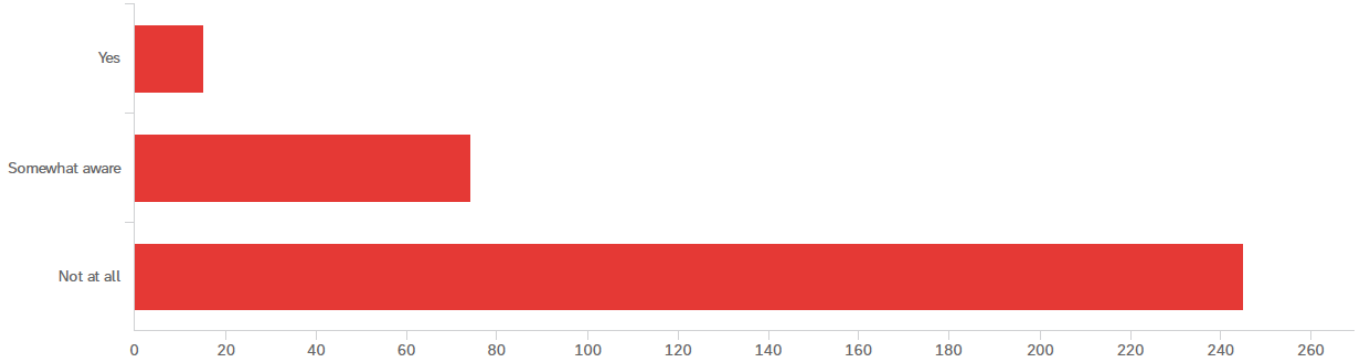
Q43 - How closely do you follow privacy news?




My last, and final question asked the participants if they are aware of other countries and how they protect their citizen's privacy in realm of their consumer protection laws. A whopping 4.5% answered "yes" while an astounding 73% responded "not at all." This goes to show that most of our citizens aren't even aware of the incredible regulations put in place by countries such as the EU. We, as a country, have so much to learn from them and it was fascinating to see that so many individuals are completely unaware.

4I: Knowledge of Other Countries' Privacy Laws

Q44 - Are you aware of other countries and how they protect their citizen's privacy in realm of their consumer protection laws?



**LIMITATIONS**:

It is fair to say that collecting data for this survey was rather straightforward in terms of composing a survey and sending it out. While conducting research during a pandemic was slightly beneficial since so many individuals are newly familiar with their technology and able to follow the link that was sent to them, I still ran into a few roadblocks – as anticipated. While over 400 participants completed my survey, not all of these individuals *completed* the survey, totaling my analysis range of about 340 results to sift through. Completion of the survey was one of my biggest challenges – a way this could've been resolved is through making some of the important questions mandatory therefore individuals had to answer it before turning in the survey. All this to say, I do think I should have increased my sample size in the sense that it is clearly efficient to have progressively more results when you are conducting research. While I had an incredible representation from Generation Z with 158 young individuals, only 60 Millennial's responded. On a similar note, I reached 37 members from Generation X and a shocking 75 Baby Boomers. Finally, I only reached 3 members of the Silent Generation. I would have liked to have the numbers average out slightly more across the board if I were to do things all over again but am still super pleased with my current range of responses based off how I distributed the survey to different networks/platforms to then allowed it to "self-spread" – if you will.

On another note, I should have created and distributed the survey out earlier than I did. This was live and active for the entirety of March 2021 but allotting a longer period could have helped me assess more people, overall. If Covid wasn't ever-present during my research period, I could have gone to more local businesses to advertise my survey to a broad range of people. I definitely didn't need more of my peers to take it as I received an adequate amount of input from this generation but would definitely like to see more from Generation X and older generations, so expanding past the University and my home could have deemed beneficial in the long run had circumstances been different. In terms of my study, I wish I researched slightly more documentaries/movies that are currently on the top of mind such as diving deeper into documentaries I've already seen, such as Social Dilemma, and Snowden, a movie I didn't hear about until after I wrapped up most of my research. This would've been in order to encompass up & coming films that are capturing a wide variety of audiences today informing others on the exact question I was researching. I could have then asked questions revolving around topics these documentaries/films discuss to then see if individuals take more or less precautions after watching.

Finally, if I could go back I would've also asked more questions around the up & coming application TikTok, as this is an app that actively *has* to listen to you and determine what you like to always create an exact "*for you* page." I tried to stick with questions that would appeal and resonate with all generations, but if I were to continue to research this topic or do it again, I would ask more questions about this app. I lastly would've polled the individuals on topics concerning Covid-19 and if this has increased their usage with technology and their experience with buying more things virtually and if the "beneficial" personalized, catered advertisements deemed more valuable than in years past.

**IMPLICATIONS AND FUTURE RESEARCH**:

To conclude, I believe that the research I conducted was an accurate representation of how different generations and individuals feel toward the act of our devices tapping into our personal information.

One of my underlying intentions through collecting responses on my survey was to study the implications of how different generations have ranging levels of threshold with the phenomenon of how our devices are ever-present and tapping into our everyday information. Upon analysis there wasn't too much of a clear divide in how older/younger generations answered questions or sections as a whole. There were certain individuals within each age group that were strongly opinionated one way or another, but there wasn't enough general consensus in the older generation, 40+, answering in a completely different light than those who are 18-39. My hypothesis would've been that individuals who were older would care more about their data being leaked and shared daily, because that's how a few adults in my close circle act – but I learned that this wasn't a shared "mega-concern" across the generation as a whole. When I evaluated, the older generation was slightly more concerned, yet it wasn't a significant enough number to proclaim that they were ultimately "more worried" on a large scale. Although my peers have drilled in my head that they aren't too concerned, since they generally don't have much to hide, it seems that all generations are aware this is occurring around them – which was assuring because that's the truth. Younger generations are expected to understand this phenomenon better solely due to the fact that they grew up in the technology era. I personally have had a desktop computer in my home since before I can remember, indicating I had access to the internet by the time I began school and I simply do not remember a world without the internet. It is an easier pill for younger generations to swallow that technology is so smart that it can gather information in a millisecond, so I was genuinely curious how uncomfortable this would make the older generations. These individuals grew up in a complete 180º flipped era where technology met them at later stages in life. The key difference is they knew a world without it and although it can make their life easier - it would have to be an adjustment nonetheless. My prediction was that older generations would find the act of technology listening to be way more invasive than my generation, per say, but it seemed as if they ranged about the same, only slightly leaning towards more worried – as mentioned before. An important call out is that all individuals were acutely aware of our devices being ever-present and listening, which is a relief. It was fascinating to see that generational differences aside, the individuals polled all seemed to be on the same page that while they are aware this is going on, they generally aren't actively trying to boycott or avoid this, it is more of an inevitable topic of concern.

It was convicting for my participants, and myself included, to reach the section in the survey about privacy terms and conditions. Throughout the survey as a whole, it is understood that most individuals stated they are aware of our ever-present technology acting as a surveillance camera on all our aspects of our life. After stating they are mindful of what's going on, I asked many questions evaluating their trust and consciously uncovered their acute worries on the matter. Then I wrapped up the survey bringing up the case that almost all companies and government-run websites give us a privacy terms and conditions document to read and "agree" to ultimately give our data away. I think this was the eye-opening part of the survey where people had to evaluate that while this is something that worries them, 74% of the participants never or hardly ever even read what they are presented on these pop-up screens. It may in fact state in bold font that their data is at risk of being taken and sold, but people are trained to click 'I accept" without even fully scanning the screen these days. Nearly 75% said that when they do end up reading them, they are never all the way through. This is mind-altering due to the nature of concern that they might have previously expressed a few questions prior. My main takeaway from this aspect of my research is that individuals who deem to find this act creepy and crossing the line are also in fact the same people who don't read the terms and conditions statements

when they are in our reach. It seems almost counterintuitive on how they aren't helping ease their own worries when an opportunity to is readily available.

Another key takeaway I had while conducting this research study is that not many people are aware of how little protection/regulation our country has over this breach of privacy. I learned so much throughout the beginning phases of this research project about other countries such as the EU and the amount of security they have for their citizens concerning these exact situations that we have in the US but was floored to hear how little our federal government has implemented 'change' over this phenomenon. While individual states are doing what they can to mimic the EU and set up protections for individuals, our nation as a whole has nothing in place to protect us. Companies and firms will just get a slap on the wrist, but there are no real actions set in place to punish or prevent data breaches from occurring – since this is not considered "illegal." A lot of this might be due to the fact that the government itself are the individuals behind the mantra of 'needing to know everything' about their own citizens. It was alarming to wrap my head around the fact that the reason regulations might not be in place by our federal government is because those are the exact individuals who want our information to be less protected in the first place. Another callout about this realm of my study is when I asked, only 18 participants in my survey said that they understood a great deal, or a lot of what laws/regulations are currently in place in this country to protect their data. Results show that only 2% polled understand just how miniscule our protection is while 34% admitted to knowing "nothing at all." This is an area that is not discussed in depth in the public light, but states like California with their 'California Consumer Privacy Rights and Enforcement Act' are on the right track and hopefully someday soon the nation as a whole will follow. In conclusion, the only other thing we can wish for is more individuals being coming to understand just how little our nation is choosing to protect our data.

To conclude, for the industry of Marketing as a whole – I believe that while I have personally benefited – it is ultimately an invasive way to try to reach consumers when delivering such precise, personalized ads. While I won't speak on behalf of why the government is funneling our information, it is clear that social media platforms do this for the sole purpose of giving us curated advertisements by third party companies/firms. It makes me eerily aware at times to be consciously careful of how much I say around my device due to the fact I want to feel that my conversations are kept private and not used to 'target me' as a consumer in a later "Instagram scroll." While this can deem beneficial in how it increases in online shopping via apps and clicking on ads instantaneously, I feel as companies and social media platforms should approach their action plan in a more candid, fair manor. I don't believe their intentions are malicious when trying to give us enhanced product placement, but after all my research within this study I do find it to be a bit calculated. When mentioning out loud that I need a new phone case, and then receiving a plethora of phone case brands on all my social media platforms the next hour – there is the repeated fine line of beneficial and creepy thoughts running through my mind. Yes, I needed this case, but it takes away my innate nature to want to go to the store/go online in my own fashion to begin researching different cases. It takes away the nostalgia of having a "want" or "need" for something. In comparison to 1984 or a Brave New World – the nightmarish vision of "future society" seems to be ever-present in our current technology era. The powerful influence technology deems to have on society as a whole is valuable to some but intrusive to others. While technology and science are used to enhance an individual's life – like depicted in both of these novels – one must not forget the fundamentals of what makes humans human. Sometimes *not* having everything in reach of our fingertips is the step we need to take to

re-center humanity. Marketing for companies has boomed after having easy access to their consumers information, but my sole recommendation is to avoid future hassle and just bring complete candor to the table and authentically state they are doing this. There have been many instances where platforms and firms have denied doing this – causing unnerve and tense situations to arise. Due to my survey, it showed that 81% of participants fell into the worried range about social media sites getting their personal information. So, while this form of marketing may come across as a quick way to target consumers, companies should be aware that this something that is unsettling their users. Marketing is only going to continue to soar within this era, as we have already seen – but remaining genuine, sincere and honest is the key to long term success with their worried consumers.

To finalize my thoughts, in conclusion, I thoroughly enjoyed researching this deep-rooted and persistent phenomenon. It is something that I am immensely passionate about, as this is something I first noticed by conducting mini experiments around my devices to see if they were listening to me. Becoming acutely aware of this paradox has sharpened my senses and knowledge on what's happening around me, daily. Through our devices tapping into our personal data and via the implications firms and the government have over our privacy as a whole – I have learned an extensive amount on this topic. It truly has put a lot of things into perspective for me as a consumer and has made me keenly attentive of how I should proceed from this point on and how I can educate others. The research conducted can be summarized in one statement: technology has an immense role in manipulating consumers and acceptable or not, it is only going to get more severe as time goes on.

## Bibliography


Antonelli, W. (2020, November 18). *What is Zoom? A comprehensive guide to the wildly popular video-chatting service for computers and smartphones*. Business Insider. https://www.businessinsider.com/what-is-zoom-guide#what-is-zoom.

Armental, M. (2021, March 1). *Zoom Foresees Robust Growth Even as Pandemic Pressures Ease*. The Wall Street Journal. https://www.wsj.com/articles/zoom-foresees-robust-growth-even-as-pandemic-pressures-ease-11614637492.

Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2021, January 22). *The consumer-data opportunity and the privacy imperative*. McKinsey & Company. https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative#.

Balis, J., Larson, E. K., & Saverice-Rohan, A. (2021, January 6). *Why consumer privacy can be a differentiator*. EY. https://www.ey.com/en_us/consulting/why-consumer-privacy-is-a-differentiator-not-just-a-compliance-risk?WT.mc_id=10463394&AA.tsrc=display.

Borchert, C., Pingeulo, F. M., & Thaw, D. (2014). Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act 13 Duke Law & Technology Review 2014-2015. Duke Law - HeinOnline. https://heinonline.org/HOL/LandingPage?handle=hein.journals/dltr13&div=3&id=&page

Burke, M. (2019, November 2). *Amazon's Alexa may have witnessed alleged Florida murder, authorities say*. NBCNews.com. https://www.nbcnews.com/news/us-news/amazon-s-alexa-may-have-witnessed-alleged-florida-murder-authorities-n1075621.

"CarbonTRACK." (2018, April 4). *How Voice Assisted Technology is Being Used*. carbonTRACK. https://carbontrack.com.au/blog/voice-assisted-techchnology/.

"Cash App". App. (n.d.). https://cash.app/.

"Centers for Disease Control and Prevention." (n.d.). *About COVID-19*. Centers for Disease l and Prevention. https://www.cdc.gov/coronavirus/2019-ncov/cdcresponse/about-COVID-19.html.

Custers, B., Van der Hof, S., & Schermer, B. (2014). Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies [Abstract].

Evans, D. (2020, April 4). *How Zoom became so popular during social distancing*. CNBC. https://www.cnbc.com/2020/04/03/how-zoom-rose-to-the-top-during-the-coronavirus-pandemic.html.

Dillion, N. (n.d.). *Wonder How 2021 May Differ From 2020? Federal Data Privacy May Be Enacted – Be Prepared*. JD Supra. https://www.jdsupra.com/legalnews/wonder-how-2021-may-differ-from-2020-7469745/.

Divatia, A. (2020, December 17). *Council Post: Looking Ahead to Data Privacy In 2021*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2020/12/18/looking-ahead-to-data-privacy-in-2021/.

"Do You Care About Privacy as Much as Your Customers Do?*" Harvard Business Review.* (2020, January 28). https://hbr.org/2020/01/do-you-care-about-privacy-as-much-as-your-customers-do%20heart%20of.

"First-Party & Third-Party Cookies: What's the Difference?" - *Clearcode Blog*. Clearcode. (2021, March 18). https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/#third-party-cookies.

Fischer-Baum, R. (20217-11-26). What "Tech World" Did You Grow Up In. Washington Post. https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2fgraphics%2f2017%2fentertainment%2ftech-generations%2f

Fleming, J.., & Adkins, A. H. (2020, October 20). *Data Security: Not a Big Concern for Millennials*. Gallup.com. https://news.gallup.com/businessjournal/192401/data-security-not-big-concern-millennials.aspx.

"Generational Breakdown: Info About All of the Generations." The Center for Generational Kinetics. (2020, November 12). https://genhq.com/faq-info-about-generations/.

Girish, D. (2020, September 9). 'The Social Dilemma' Review: Unplug and Run. Https://Www.Nytimes.Com/#publisher. https://www.nytimes.com/2020/09/09/movies/the-social-dilemma-review.html

Green, D. (2018, May). Big Brother is Listening to you: Digital Eavesdropping in the Advertising Industry. Duke Law. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1327&context=dltr

Gregersen, E. (n.d.). *History of Technology Timeline*. Encyclopædia Britannica. https://www.britannica.com/story/history-of-technology-timeline.

Haselton, T. (2019, August 28). *Apple apologizes for listening to Siri conversations*. CNBC. https://www.cnbc.com/2019/08/28/apple-apologizes-for-listening-to-siri-conversations.html.

Hern, A. (2019, August 28). *Apple ends contracts for hundreds of workers hired to listen to Siri*. The Guardian. https://www.theguardian.com/technology/2019/aug/28/apple-ends-contracts-hundreds-workers-hired-to-listen-siri.

"How Does Banner Advertising Work?" *Creatopy*. (2021, March 16). https://blog.creatopy.com/banner-advertising-basics/.

Komando, K. (2019, June 20). *When smart devices watch you, what do they do with the data?* USA Today. https://www.usatoday.com/story/tech/columnist/2019/06/20/what-do-smart-devices-do-data-they-collect-you/1483051001/.

Kree, J. (2020, May 6). *FBI warns of hackers stealing information through smartphone apps*. KDBC. https://cbs4local.com/news/local/fbi-warns-of-hackers-stealing-information-through-smartphone-apps#:~:text=FBI%20warns%20of%20hackers%20stealing%20information%20through%20smartphone%20apps,-by%20Justin%20Kree&text=Including%20that%20seemingly%20innocent%20gaming,%2C%20passwords%2C%20even%20banking%20information.

Larkin, B. (2019, June 25). *What It Was Like to Live Without Today's Technologies We Totally Take for Granted*. Best Life. https://bestlifeonline.com/life-before-technology/.

Masur, P. K. (2020). How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information [Abstract]. The Politics of Privacy: Communication and Media Perspectives in Privacy Research,8(2).

McKinnon, J. D., & Tracy, R. (2020, December 16). *Ten States Sue Google, Alleging Deal with Facebook to Rig Online Ad Market*. The Wall Street Journal.

https://www.wsj.com/articles/states-sue-google-over-digital-ad-practices-11608146817?mod=article_inline.

Merriam-Webster. (n.d.). *Smartphone.* Merriam-Webster. https://www.merriam-webster.com/dictionary/smartphone.

Merriam-Webster. (n.d.). *Technology*. Merriam-Webster. https://www.merriam-webster.com/dictionary/technology.

Munoz, R. (2018, August 22). *8 Advantages and Disadvantages of Smartphone Technology*. MobileCon. https://www.mobilecon2012.com/8-advantages-and-disadvantages-of-smartphone-technology/.

Naeini, P. E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Crannor, L., & Sadeh, N. (2017). Usenix Privacy Expectations and Preferences in an IoT World. Proceedings of the Thirteenth Symposium on Usable Privacy and Security. Retrieved from https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini

Nielson Company. (2020, March). Digital Landscape PDF. Neilson Data. https://www.nielsen.com/wp-content/uploads/sites/3/2020/06/Landscape-Report-Mar-2020.pdf

"Norton Online." *Is your phone easy pickings for identity thieves?* (n.d.). https://us.norton.com/internetsecurity-privacy-is-your-phone-easy-pickings-for-identity-thieves.html.

Olito, F. (2020, August 20). *The rise and fall of Blockbuster*. Business Insider. https://www.businessinsider.com/rise-and-fall-of-blockbuster.

Pettijohn, N. (2019, September 3). *Of Course Your Phone Is Listening To You*. Forbes. https://www.forbes.com/sites/nathanpettijohn/2019/09/03/of-course-your-phone-is-listening-to-you/?sh=6e3bf05d6a3f.

Pew Research Center. (2020, June 5). *Demographics of Mobile Device Ownership and Adoption in the United States*. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/fact-sheet/mobile/.

Pew Research Center. (2020, July 28). *The Whys and How's of Generations Research*. Pew Research Center - U.S. Politics & Policy. https://www.pewresearch.org/politics/2015/09/03/the-whys-and-hows-of-generations-research/.

Sauer, G. (n.d.). *A Murder Case Tests Alexa's Devotion to Your Privacy*. Wired. https://www.wired.com/2017/02/murder-case-tests-alexas-devotion-privacy/.

Schechner, S. (2021, January 25). *Google Pursues Plan to Remove Third-Party Cookies*. The Wall Street Journal. https://www.wsj.com/articles/google-progresses-plan-to-remove-third-party-cookies-11611581604.

Shearer, E. (2021, January 12). *86% of Americans get news online from smartphone, computer or tablet*. Pew Research Center. https://www.pewresearch.org/fact-tank/2021/01/12/more-than-eight-in-ten-americans-get-news-from-digital-devices/.

Silvestro, M. (2017, July 20). Alexa, Do You Have Rights?: Legal Issues Posed by Voice-Controlled Devices and the Data They Create. American Bar Association. https://www.americanbar.org/groups/business_law/publications/blt/2017/07/05_boughman/

Velez, F. (2021, January 16). *What's in Store for Data Privacy in 2021?* CPO Magazine. https://www.cpomagazine.com/data-privacy/whats-in-store-for-data-privacy-in-2021/.

"Venmo." *Venmo App*. (n.d.). https://venmo.com/.

"What is Covid-19" *Latest* Medical News, Clinical Trials, Guidelines - *Today on Medscape*. (2021, March 31). https://www.medscape.com/answers/2500114-197401/what-is-covid-19.

"What is GDPR, the EU's new data protection law?", *GDPR.eu*. (2019, February 13). https://gdpr.eu/what-is-gdpr/?cn-reloaded=1.

Wiggins, C. (2016, November 4). *5 Times George Orwell's "1984" Predicted the Future*. Bustle. https://www.bustle.com/articles/193033-5-times-george-orwells-1984-predicted-the-future

"3 Ways That Social Media Knows You Better Than Your Friends and Family Do - Emerging Media Online Master's Program" *Loyola University Engaging Media*. (n.d.). https://www.loyola.edu/academics/emerging-media/blog/2017/3-ways-that-social-media-knows-you-better-than-your-friends-and-family-do.

"5 Ways Your Smartphone Causes Identity Theft." *Protect Your Identity and Data* ARAG is there to help when you need an attorney or legal help. (2017, June 19). https://www.araglegal.com/individuals/learning-center/topics/protecting-your-identity/five-ways-your-smartphone-causes-identity-theft.