Ever since the inception of the World Wide Web, our society has been increasing connections to it and communications utilizing it around the globe. Every year, we have more users getting online with more devices. While many of the gadgets making these internet connections are personal computers, we have an increasing number of Internet of Things (IoT) devices, or devices that have functionality to transmit data, but not necessarily as their primary function. These devices have been designed to make human life easier, but come with negatives as well. With the expansion of production and distribution of these machines worldwide comes new concern over our privacy: What information are these devices tracking with and without our knowledge and approval? What of our data is being shared with which companies and groups? Are they able to house our data securely? Are we still being listened to when our devices are told to stop listening? Our information has taken on new risk with the conveniences of these new, powerful technologies.

IoT technologies have been transforming the way we work and live since the 1980's. The first instance of such technology has been credited to students at Carnegie Mellon University when they connected a vending machine to the Internet to remotely monitor purchasing habits of the users. (Marchant, 2021) Hooking up this device to share information online began an evolution of technology. In 1999, the term 'Internet of Things' was coined by the computer scientist Kevin Ashton when he proposed attaching RFID chips to products to track their progress through the supply chain. "In 2000, LG announced the first smart refrigerator, in 2007 the first iPhone was launched and by 2008, the number of connected devices exceeded the number of people on the planet" (Teicher, 2018). In addition to a smartphone in the hands of nearly 90% of the world's population, there are currently over 10 billion devices connected to the Internet, even despite a recent chip shortage slowing this number's growth (BankMyCell, 2022).

Amazon's Echo, Google's Nest, and Meta's Portal are the main hubs of smart technology in homes, accompanied by many smaller manufacturers creating smart lightbulbs, doorbells, thermostats, cameras, speakers, ovens, vacuums, and so much more. These devices connect to our home Wi-Fi connections, allowing commands to be sent in person and remotely, switching devices on and off at a spoken word in the next room over, or a press of a button anywhere around the world, and they will even "learn", adapting to what their users' specific needs are. But to be able to do this, the devices need to be on and listening all the time, and with this, they can be collecting data on what their users are talking about, when these discussions happen, how many people are in the residency, what their routines are, the shape of their homes, and much more.

Data collection through IoT devices has spurred a change in how corporations function, with many referencing the gold rush when discussing the importance of big data. One of the co-founders of Beam Technologies, a company selling smart toothbrushes, explains their shifted focus. "[P]eople often refer to us as a toothbrush company, but we're not. We're actually not interested in toothbrushes at all. We're interested in health data" (Bishop, 2019). Considering the social construction of technology theory, it can be observed how companies have changed from generating data themselves to collecting it from their consumers, whether it be to better products or as a more direct revenue stream. Personal data, engagement data, behavioral data, and attitudinal data are all of interest to companies for business. While some companies have been brought into existence with the main goal of collecting data and sharing it with other groups, other corporations have brought about teams to focus on the collection and interpretation of consumer data to improve customer experiences, refine marketing strategies, transforming it into cash flow, and to secure more data (Freedman, 2022). It was estimated that American companies

spent nearly $20 billion in data collection in 2018, and that number has been on the rise since (CBS News, 2018). Within our corporatized world, markets are constantly shifting with companies always trying to fight for the top spot, and the successful companies have figured out the need to control data to take first place on the ladder.

While some companies use this data in-house to better their platforms and devices, plenty of this data also gets shared with third parties to make money and build alliances. Nest, a subsidiary of Google, produce smart thermostats, smoke and carbon monoxide detectors, and security cameras that have now been installed in thousands of homes. Their thermostat is designed to "learn" when users are home based on motion tracking, what temperatures are set throughout the day to determine what temperatures is appropriate at a given time, and will connect with energy companies regulate usage during their peaks and drops in demand on energy from the network. These changes in usage are reported to have helped reduce energy wastage by up to 50%. Their security cameras record and store visual and audio data, which it analyses in real time to provide security in the home. Nest is able to notify owners when the cameras detect movement when no one is supposed to be in the home, reporting potential intruders. Nest has stated that they will not share this personal data to anyone, however after their acquisition by Google, that may no longer be their decision to make (Marr, 2016). Walmart, currently the largest retailer in the world, has an internal team to research and deploy new data-led initiatives throughout the business, including ways to better understand their customers' needs, and provide them with the products they wanted to buy. This "Data Café" references a database consisting of 200 billion rows of transactional data, collected in part by smart cash registers, from their past few weeks of purchases and returns, and cross-references that with data from 200 other sources, including meteorological data, economic information, telecoms data, data from social media, gas

prices, and a database of events that took place in the vicinity of Walmart stores (Marr, 2016). This information allows Walmart to better their stores and stock for their customers. “Insurance companies, which historically sold car insurance based on driving records, have more recently started using such data-driven profiling methods. A Florida insurance company has been found to charge people with low credit scores and good driving records more than people with high credit scores and a drunk driving conviction. It's become standard practice for insurance companies to charge people not what they represent as a risk, but what they can get away with” (O’Neil, 2016). This profiling with large datasets hurt those that were in need of a car to live and work, but were unable to afford extra costs for insurance.

Facebook made headlines worldwide in 2018 when the attorney general of Washington D.C. filed a lawsuit against the company over sharing data with analytics company Cambridge Analytica, who had been reportedly creating psychologically tailored advertisements based off 87 million users’ Facebook profiles, done to influence people's voting preferences in the 2016 US presidential election. Many attributed the election results at least partially to these targeted ads, and users had mixed feelings towards their privacy on Facebook, ranging from “I'm not bothered”, to “I'm extremely concerned” (Hinds, Joinson, & Williams, 2020). Looking through the lens of Lasswell’s hypodermic needle model, we can see how this data can be used to manipulate users’ experiences and push them towards making decisions based on specific information they have been pushed, without any knowledge of the manipulation going on. His theory states that the mass media can influence a group of people directly by “shooting“ or “injecting“ them with messages that are specifically designed to trigger a response. When factoring in datasets to target specific groups, a message can be conformed specifically for someone of a certain mindset, creating a higher chance of the desired response.

Amazon and other companies have been reported accepting data from Facebook's users obtained through private messages, as well as other data shared on the platform. Facebook's Portal device, often used to make calls and run apps in a residential home, is also reported to collect information which can be used to change a user's advertising experience on Facebook-owned properties (Wagner, 2018). With user data now existing in multiple companies' databases, the chance of personal data being reached by hackers or being sold off to nefarious groups increases greatly. Cambridge Analytica is not the only data broker company. The industry for companies specifically geared towards the buying and selling of information on customers has risen significantly in the past decade. Compiling different datasets on a single consumer to create a detailed profile is immensely valuable for advertising, as well as surveying and research (Freedman, 2022). By utilizing multiple smart devices, companies can gain even more specific stories of a user's life. A doorbell can note when someone leaves their home, their car's GPS finds the best route to take to the store, the cash register timestamps a customer's credit card information, all while their pedometer is tracking heart rate, number of steps taken, and the genres of music being listened to. This information is stored in databases by various companies who contribute to each other's wealth of knowledge, creating highly tailored profiles of users to best fit their needs and desires.

While big data can assist companies to provide better services to their users and better their manufacturing, users' concerns have increased greatly in regard to their privacy. Buying, selling, and sharing of user data has become so prevalent that individuals have begun taking this loss of secrecy in their lives as an inevitability and given up on the general concept of privacy altogether. Plenty of this information may appear innocuous enough to share in exchange for services, but as businesses continue to push what information they collect - such as who users are

spending their nights with and blueprints of their homes - consumers are becoming more wary. Back in 2016, a survey was conducted on Americans' confidence with various groups' collection of data. It revealed there was plenty of skepticism with social media sites, and mixed concern with companies and retailers. These concerns are justified; In 2017, nearly 2 billion consumer records were exposed, which includes personal data on almost half the population of the United States (Kennerly, 2018). The number of data breaches continue to rise every year; In the first half of 2019 alone, 4.1 billion data records were reported to have been compromised through 3800 data breaches globally (Hinds, Joinson, & Williams, 2020). These breaches can end up with people having their identity stolen, credit cards opened in their name, accounts being used fraudulently, and in some cases, blackmail, and similar strategic personal attacks. "According to a 2022 Ipsos poll, 70% of Americans think that, over time, limiting who can and can't access their data has become tougher. This poll also found that only 34% of Americans think that companies adequately safeguard consumer data" (Freedman, 2022). Outside of direct attacks to databases, there are many other ways hackers obtain identifiable information. "Communications can be intercepted or data compromised by unauthorized parties to collect [personally identifiable information], authentication can be brute-forced, credentials can be extracted from device firmware, credentials can be extracted from mobile apps, credentials can be intercepted at login, and new firmware can be uploaded with malware" (Bastos, Shackleton, & El-Moussa, 2018). With more and more IoT devices collecting data on their users and their surroundings, more personal information is at risk for being stored improperly and attained by hackers, extending to real harm both on and offline.

Today, about 83% of the global population owns a smartphone, up considerably from six years ago when less than 50% owned one. With modern devices becoming cheaper and

conveniences increasing for average users, production and consumption of these gadgets continue to grow. Data collection is happening with consumer, enterprise, and public space IoT devices, and privacy concerns can arise. The devices can track locations, patterns of searches, media shared, movement speeds, and more. While plenty of this information is collected with "agreement" from the devices' owners through the end user license agreement from the manufacturers, most users never read these agreements, and may not even be able to understand them. In one social experiment conducted, only 1 percent of technology users was found to actually read the provided terms and conditions, allowing companies to potentially get away with adding in ridiculous clauses (Sandle, 2020). Nearly a third of TikTok's userbase is composed of users aged below 20, (Doyle, 2022) while the platform's 14-page Terms of Service uses such jargon as "indemnify", "arbitration", and "intersperse". Hall discusses how media is encoded and decoded, and how if a user is unable to decode a message, as most TikTok users are most likely unable to, or chose not to in terms of their End User License Agreement (EULA), then there is no consumption of the information (PBS, 2016). Despite this lack of understanding, the users are meant to be held accountable for the terms they sign off on. This begs the question: Who is at fault for the miscommunication of term agreements – the consumer for not being able to understand, or the manufacturer for not putting concepts into language that is digestible? If a message is unable to be decoded, there is no meaning to the message. Just because a user signs off on a platform's rules does not mean they understand what they are allowing.

The risk of database breaches is not the only potential problem with consumers' privacy. IoT devices connected to the Internet face the possibility of being breached directly. Savvy hackers may be able to intercept traffic coming and going directly from a smart device between it and its manufacturer. The reason so many laptops have built in privacy screens is due to the

potential of being spied upon by hackers gaining access to the built-in webcam. The same applies for standalone security cameras if they are connected online. There even exists search engines and tools to assist gaining unauthorized access to smart devices to simplify the process for ne'er-do-wells (Bastos, Shackleton, & El-Moussa, 2018). Devices can also be manipulated to spread malware to other devices connected on the same network, creating another point of weakness for hackers into a system. Not often do consumer IoT devices come with the ability to better secure their connections, and even less frequently do manufacturers include instruction on this in in easy-to-understand text. Criminals can find any information that may be transferred between these connected devices, and potentially even information that is stored in the device without being sent to the cloud, such as account names and passwords, IP addresses, and similarly connected devices. Companies producing any device with the potential to transmit data to the Internet need to ensure security protocols are up to standard, so their users' information stays safe.

As the concept of privacy in terms of personal information being collected by companies has been gaining speed, legislature has not quite caught up yet in all nations. The general consensus is that the European Union (EU) has been much more attentive to updating policy surrounding individuals' privacy compared to the United States (US). In May of 2018, the EU instated the General Data Protection Regulation (GDPR) to allow citizens greater understanding and control of how their personal data is being used by companies, as well as a gateway to filing complaints against companies misusing their data (Frankenfield, 2020). In the US, the closest thing that exists to this is the California Consumer Privacy Act of 2018 (CCPA), created to outline standards for data collection, the consequences for companies improperly storing user data, and the rights of California consumers exercising over their own data (Hennel, 2021). The

country itself does not yet have a comprehensive, equivalent guideline put into place for data protection of individuals, but policies are upcoming as of next year; Virginia, Colorado, Connecticut, and Utah all have state specific privacy and consumer data protection acts that will go into effect sometime in 2023 (Blair et al., 2022). Freedman anticipates major change for businesses when it comes to data collection: "Businesses that are so far untouched by data privacy regulations can expect a greater legal obligation to protect consumers' data as more consumers demand privacy rights. Data collection by private companies, though, is unlikely to go away; it will merely change in form as businesses adapt to new laws and regulations" (Freedman, 2022).

In a society where the ideology neoliberalism reigns supreme, it makes sense that data is king; our capitalistic, free market has competitors always trying to one-up each other, which includes their ability to capture and make use of data. The fact that these datasets have so many uses to increase revenue becomes incredibly enticing, even necessary, for companies to focus on. New algorithms and new technologies are constantly being developed and deployed in part to allow users better experiences, but also to better understand and track statistics, increase marketing strategies, and sell more product. We can see how corporations use their private spaces to their advantage in this way, and how they leverage their platforms' affordances to their users to persuade them into allowing capture of their information. By offering them such conveniences in the form of free email usage or devices to make their home lives easier, the idea of giving up their personal data becomes a much easier pill to swallow. Are there still ways to prevent the loss of our data? Users can use VPN software to block certain groups access to their traffic. When signing up for services, individuals can use separate accounts that are not linked to other datasets. Consumers can do research before buying IoT devices, exploring what the

manufacturer captures from the devices and what they do with that data. Much of the responsibility also falls on the corporations, too. Companies need to become more upfront with what data they are collecting and sharing it, explaining it in simple to understand language so consumers are in the know from the get-go. If they do not, how the public sees the companies may change, losing them business overtime. The government also needs to put into place regulations for the data collection and sharing as IoT devices begin to invade our privacy outside the home with security cameras in public spaces, as to keep the population safe and allowed privacy. The collection of information from using IoT technologies is a very important topic to understand in this day and age as the usage of these devices continues to rise, and knowing what we are trading for our ability to use these technologies is not as straightforward as it may seem to some.

References

Bastos, D., Shackleton, M., & El-Moussa, F. (2018). *Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments*. IET. https://ieeexplore.ieee.org/document/8379717

Bishop, R. (2019). *The Walls Have Ears - and Eyes - and Noses: Home Smart Devices and the Fourth Amendment*. Arizona Law Review, Vol. 61, Issue 3, pp. 667-698.

Blair T., Childress W., Del Sesto R., Hadgis K., Hirsch W., Hu S., Krotoski M., Liao T., Ligorner K., Parks G., Schireson T., Spies A. (2022, September 14). *Data Privacy: Evolving Updates to the Global Landscape*. Morgan Lewis. https://www.morganlewis.com/pubs/2022/09/data-privacy-evolving-updates-to-the-global-landscape

CBS News. (2018, December). *Facebook faces lawsuit for Cambridge Analytica privacy breach.* https://youtu.be/JADsm2YmApQ

Doyle, B. (2022, October 9). *TikTok statistics - everything you need to know*. Wallaroo Media. https://wallaroomedia.com/blog/social-media/tiktok-statistics/

Frankenfield, J. (2020, November 11). *General Data Protection Regulation (GDPR) Definition and Meaning*. Investopedia. https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp

Freedman, M. (2022, November 21). *How Businesses Are Collecting Data (And What They're Doing With It)*. Business News Daily. https://www.businessnewsdaily.com/10625-businesses-collecting-data.html

Hennel, C. (2021, November 19). *CCPA: California Consumer Privacy Act Explained*. Termly. https://termly.io/resources/articles/ccpa/

Hinds, J., Joinson, A., & Williams, E. (2020). *"It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal*, International Journal of Human-Computer Studies, Volume 143. https://www.sciencedirect.com/science/article/pii/S1071581920301002

BankMyCell. (2022, October 1). *How many people have smartphones worldwide*. https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

Kennerly, E. (2018). *Privacy and the internet.* CQ Researcher. https://library.cqpress.com/cqresearcher/document.php?id=cqresrre2018020900

Marchant, N. (2021, March 31). *What is the internet of things?* World Economic Forum. https://www.weforum.org/agenda/2021/03/what-is-the-internet-of-things/

Marr, B. (2016, April). *Big Data in Practice*. John Wiley & Sons, Ltd. ISBN 9781119278825.

O'Neil, C. (2016, October 10). *Big-Data Algorithms Are Manipulating Us All*. Wired. https://www.wired.com/2016/10/big-data-algorithms-manipulating-us/

PBS Idea Channel. (2016, October 5). *But Wait: Do We Really CONSUME Media?* https://youtu.be/fRsQ0-94O9A

Sandle, T. (2020, January 29). *Report finds only 1 percent reads 'Terms & Conditions'*. Digital Journal. https://www.digitaljournal.com/business/report-finds-only-1-percent-reads-terms-conditions/article/566127

Teicher, J. (2019, June 13). *The little-known story of the first IOT device*. IBM. https://www.ibm.com/blogs/industries/little-known-story-first-iot-device/

Wagner, K. (2018, October 16). *It turns out that Facebook could in fact use data collected from its Portal in-home video device to target you with ads*. Vox. https://www.vox.com/2018/10/16/17966102/facebook-portal-ad-targeting-data-collection