Rockwell's Nightmare: The Digital War Between Smart Technology and Personal Privacy

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Nathaniel Douglas Barrington

Spring, 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Bryn E. Seabrook, Department of Engineering and Society

Privacy is No Longer Private

Picture a situation in which two friends are talking about a pair of hiking boots they want. A couple hours later, one friend scrolls on their phone, only to find that the same pair of hiking boots found its way to their advertisements. It is almost as if there were an unwanted listener in their conversation from earlier. Such interactions may be creepy, invasive, and a cause of unwanted stress. While companies largely do not use voice recognition technology to collect information on users, companies will use smart technologies and personal data collection to tailor their user experience, regardless of if it makes their consumers uncomfortable (Cawley, 2022). TikTok is a prime example of this, as it not only uses interaction data to bolster its algorithm's results, but it also uses regional data and language preferences to further create an image of who each user is (Newberry, 2021). TikTok provides this service to both make money and to provide really deep insights into their user base (*"Is TikTok"*, 2020). Even phone numbers from the app can be used to personally track the locations of their users, creating a serious security risk for any adversary of TikTok and the associated Chinese Communist Party (Doffman, 2021). There must exist some line in which users can receive tailored results without having their entire digital life be sellable to any company willing to pay for it. Actor Network Theory (ANT) is being applied in order to capture and evaluate the infinite network of "actors" involved in both the technological and societal aspects of the personal privacy question. The perspective provided by ANT showcases the complexity of the issue through which personal privacy versus data collection can be examined. In order to evaluate the limit to which smart technologies can utilize personal data, the following question must be addressed: how do personal data technologies such as TikTok influence the sociotechnical relationship between enhancing the user experience versus infringing personal privacy?

How Privacy Has Evolved in the U.S. and Abroad

Before the 21st century, if personal privacy and technology were mentioned in the same sentence, it was most likely in reference to Orwell's *1984* (Packer, 2019). In the novel, Orwell describes characters' terrified obsessions with the telescreens, and how there was "no way of knowing whether [they] were being watched at any given moment." Nowadays, personal privacy involves finding out ways to turn off your location services (Bay & Cohen, 2021). While decades apart, the connection between the theoretical telescreens and inherent trackers built into smart devices illustrates an eerie continuity that Orwell seems to have foreseen. As an initial means to combat this fear of technical oversight, Congress passed into law the Privacy Act in 1974, less than 50 years from the time this paper was written (U.S. Department of Health and Human Services). Given the act's relative recency, most families have parents and grandparents that remember a time in which the U.S. did not feel the need to address this privacy concern, as it did not exist in the time in which they grew up. However, personal privacy can be a very controversial issue in modern-day society with issues such as the San Bernardino shooters case. In December 2015, a married couple opened fire on a holiday party which the husband had attended and left, angry. The motives were not clear as to why the couple had acted as such, especially given the preparation that seemed to have been needed to carry out such a mission, given that weapons, tactical equipment, and a getaway car were all used in the process (Nagourney et al., 2015). Given that the shooting was the largest since the December 2012 shooting at Sandy Hook Elementary in Newtown, CT, the trial encapsulated the nation. Another reason that the trial was so important was the drama that ensued between Apple and the FBI to attempt to uncover pertinent data to the case, as Apple did not want to release the data to the FBI as they hoped to keep intact their user privacy policy, whereas the FBI wanted to use the phone

to mine data regarding one of the shooters involved (Nakashima, 2016). Given that the context of the shooter case revolved around multiple murders, it may be easy to recognize why the FBI pushed so aggressively to acquire the information stored in that device, but once the privacy policy rules have been breached, that inevitably means that under the proper circumstances, they can potentially be breached again. Making an exception for a law inherently creates a gray area in the process, which is already a problem in terms of how much of a role each company should play in protecting the privacy of its consumers. While the San Bernardino case is a highly sensitive topic to discuss, the development of the case illustrates how tricky the line can be when establishing how much autonomy a person can (and should) have over their personal information in contrast with the greater good of the community.

While the United States' issues with acquiring data from private companies may exist in cases such as Apple, the Chinese Communist Party (CCP) does not have this issue. The CCP's connection with TikTok is likely the reason for the "alarm bells" for the app to be sounding so loudly, and potentially one of the driving factors for Congress to have passed a multi-billion-dollar research-and-development-based package aimed at fighting the war on technology with China last June (Tomwfranck, 2021). The CCP "exercises power through TikTok," allowing them to both monitor its users and control the flow of information that the platform outputs (Melin, 2021). TikTok makes lots of money from providing full insights of the users on their platform with everything from location data to language used, to comments on a video and everything in between (*"Is TikTok"*, 2020). TikTok is not the exception, however. Many companies will take advantage of the idea that consumers need the "best new smart products" that with each iteration, get a little bit smarter, and therefore are able to create a more comprehensive picture of each user that interacts with the hardware and software (Moscaritolo,

2021). Among these devices include smart locks, outdoor security cameras, connected thermostats, even robot vacuums. Consider the Internet of Things (IoT) and its ability to connect a user's collection of smart devices, such as the ones just mentioned (Zheng et al., 2018). All these smart technologies can observe an individual's tendencies one way or another, and therefore are able to complete a more comprehensive network of aspects that exist within the scope of the device's monitoring ability. Furthermore, the advances in the IoT market outpace current regulations, signaling that personal data of consumers might be being breached even more than previously conceived (Petrescu & Krishen, 2018).

Actor-Network Theory's Inherent Grip on Personal Privacy Concerns

Modern day society is immensely complex, and the rise of digitization combined with societal growth over the past few decades has furthered these entanglements. Technology has facilitated communication and the transfer of information at speeds incomprehensible to those who had to carry letters via horseback just a few centuries ago. While these technological advances have given society great advantages in these areas, personal privacy has never been more of a concern in the history of humanity. Given this web of complexity that exists, Actor Network Theory (ANT) provides a useful resource to help dive into the nuances of personal privacy when it comes to technologies such as TikTok. ANT states that everything can be considered an actor and a network, with one's perspective defining which is which in a given scenario (Cressman, 2009, p. 3). Scientists and engineers are usually the "network-builders" that help to create a structure for the network, and this is no different in terms of smart technologies (Cressman, 2009, p. 3). Some of the actors within the scope of smart technologies are developers, stakeholders, users, but also software like an app, hardware like a phone, and walls of a house, if the device needs to be hung somewhere. Understanding that this web of actors

exists to both contribute to a positive experience for the user but also drive profit margins as high as possible illustrates the intricacies of the problem that companies face who develop software that could be viewed as hostile to the interests of personal privacy.

Actor-Network Theory is a very applicable framework for many topics, including personal privacy. Not so much regarding TikTok, but ANT has been used to describe the emergence and development of personal privacy issues in society. Bonner and Chaisson's discussion of legislation that has largely impacted the development of the privacy question highlights the web of stakeholders involved, such as those who implement international privacy principles to the users themselves. Social, political, and technical aspects intertwine to illustrate how the "constitution of privacy" has been shaped throughout the initial age of digitization (Bonner & Chiasson, 2005). Another of the authors' later works describe how history has repeatedly favored methods that reduce personal privacy of consumers through ANT (Bonner et al., 2009). Partially stemming from the lack of cohesion between different levels of organizations, ANT illustrates how the faults in proper data management can cause real security issues for those who believe their information is secure.

The Wicked Problem of Digital Privacy and its Addressal Through Differing Policies

Wicked Problem Framing and Policy Analysis methodologies are used to answer how TikTok, among other technological phenomena, elevates the concern with personal privacy as it regards to providing a comprehensive user experience. Sources that describe the friction between TikTok and several federal governments, such as China and the United States, are critical to this analysis. The Policy Analysis methodology reveals the extent to which conflicting interests exist between the foundations of two massive user groups with TikTok, highlighting the Wicked Problem Framing methodology. Since the root cause of the privacy issue has conflicting interests

at its source, the solution to finding a balance between privacy versus interconnectivity may not be solvable, and given that society already uses smartphones, it may have already been solved - in favor of interconnectivity. While the benefits of interconnectivity are highlighted, the trade-offs that exist with having such easy access to comprehensive data about an individual raises the question whether personalized user experiences or personal privacy concerns should be prioritized in both modern-day society and the society of tomorrow.

How Both People and Programs View the Personal Privacy Problem

To contextualize the progression of society in the digital age regarding personalized user experiences, it is worth referencing the rise of consumerism in the 20th century. Consumers have exponentially increased in their importance in marketing throughout the past century. Henry Ford's Model T color scheme quote, "You can have any [color], as long as it's black," illustrates the importance that consumer preference has influenced capitalistic tendencies in years past (Self, 2012). While the dawn of the assembly line allowed mass production of items, these items soon began to dissatisfy customers, leading to variations in similar products, which is where we are today. Customers want to buy different color phone cases, styles of cars, sunglasses, and everything in between for a multitude of reasons. These examples are all options that are tailored to specific users. Not dissimilar from the idea of product diversification is the notion of tailored advertising. Although executed differently, customers want to involve themselves with products that align with their goals, values, or their bottom lines. To gather this information, however, sites must utilize data collection to understand their user base so that they can provide these services, similar to TikTok's means in which they can extract deep insights (*"Is TikTok"*, 2020). Certain means in which these types of data are collected are further discussed below and

bolstered through the lenses of Actor Network Theory, Wicked Problem Framing, Surveys, and Policy Analysis.

The United States' means to protect the digital privacy of its citizens is not the most foolproof system. Currently, the Federal Trade Commission (FTC) oversees regulating data within the United States while also enhancing competition across broad sectors of the economy. The FTC and state laws have tried to protect consumer privacy, but many of these regulations are ineffective ("*Who regulates*", 2021). Through the past 50 years, legislation such as the Privacy Act of 1974, the establishment of the Do Not Call registry, the Children's Online Privacy Protection Act (COPPA) in 1998, and the Gramm-Leach-Bliley Act in 1999 are among the few examples of legislation passed before the 20th century that attempt to give privacy back to U.S. citizens ("*History of*", 2022). Specifically, in regards to the Gramm-Leach-Bliley Act (GLBA), it became the most robust means of requiring financial institutions to explain their sharing of information practices to their users and to also protect sensitive data (Staff, 2022). The GLBA's attempt to crack down on financial institutions illustrates that data handling reaches all sectors of society, given that money is involved in almost every transaction that occurs. It then becomes easy to see that using each person's financial data can be of great assets to those who have access and want to profit off this leg-up that they have, requiring the federal government to step in and regulate, such as is the case with all matters concerning policy analysis: when a problem arises, the federal government is usually called upon to fix it via legislation.

Unfortunately for groups like the FTC, Congress has struggled to pass legislation that will allow the FTC to tangibly enforce laws for companies to follow with respect to data collection. A report submitted to Congress in September of 2021 clearly stated the need for Congress to "enact privacy and data security legislation, enforceable by the FTC," signaling that

even the body whose job it is to protect U.S. consumers knows its limitations ("*FTC report*", 2021). The report also urged Congress to shore up section 13(b) of the FTC Act so that it may collect money when corporations engage in illegal or deceptive practices to then be distributed back to the consumers exploited ("*Revealing potential*", 2021). Government policy intertwined with the private sector will always create friction, as the government's purpose is to serve, while the private sector's is to sell. This branch in the network of personal privacy underscores the complications that arise between competing interests. Furthermore, when the government is ineffective at creating tangible roadblocks before a policy is enacted, such as limiting the power of private corporations and their use of personal data, it becomes exponentially harder to walk back stances that have been integrated into society. As an aside, consider the use of fossil fuels and its effects on climate change. Due to the U.S.'s inherent dependency on these fuels for our everyday lives, it becomes much harder to walk back policies that would benefit more in the long run, such as green energy. Policies that have already been implemented in society are hard to reverse, so it becomes inherent that Congress acts quickly to help steer the course of protecting personal privacy before it becomes too late.

Not to limit the analysis to simply the United States, it is important to look elsewhere to see what laws have been enacted and the extent to which they have succeeded. Most notably, the European Union enacted legislation titled the General Data Protection Regulation (GDPR) that went into effect in 2018. Its purpose is to protect its citizens from organizations that collect data on them. It imposes harsh restrictions on these corporations and punishes them severely for any violations. The legislation also empowers its citizens, as they can understand their rights to make informed decisions about how they choose to interact with the internet and agencies that may collect data about them (Wolford, 2019). Citizens are aware of the data processing done by

companies, and if data processing is done of any subject, it must be done such that the personal information is confidential and secure. Operating inside a system such as this instills trust in the systems that European citizens are using, creating a sense of security while browsing.

Businesses that operate under the scope of the GDPR must consider data protection at the forefront of its operations. When designing an app, a product, or a service, the developers must understand and be clear about what types of data will be collected and used, and how can that data be secured with the latest technology (Wolford, 2019). Data protection steps are essential to ensuring that EU citizens are safe and secure when operating online. Once data is guaranteed to be protected, processing the data properly is the next step. There are many rules and regulations that must be followed, of which some refer to consent, while others allow processing but only in the direst of circumstances. Examples of these are hard to find, as is the point, such that companies will not try to exploit any loopholes guaranteed by the wording of the GDPR. Through its ability to close loopholes, the GDPR, overall, has largely done a good job at not creating a wicked problem out of the data privacy situation. While we must acknowledge that there will be no perfect solution for the age of digitization and beyond, society must work to try and toe the line between privacy and progress. Maintaining an informed user base will most likely be the best way to do this.

While the GDPR is much further ahead in terms of data protection legislation than its counterparts around the world, the EU recognizes its own limitations with said legislation. The GDPR's Frequently Asked Questions section explicitly states that improvements with regards to new technologies will be very important to address in the coming months and years. Some of these technologies include Artificial Intelligence (AI), IoT, and blockchain, to name a few (Wigand, 2020). AI technologies relate very much to algorithms used in social media nowadays,

so recognition tactics that apps such as TikTok use will likely be at the forefront of this new wave of revamping the GDPR. Machine learning is a key means of TikTok such that it can create user groups and filter bubbles to place its users into, finding a niche or a community (Fischer, 2020). To do this, however, machine learning requires lots of training data to provide accurate results when used to predict on testing data (Joby, 2021). Since testing data is should be collected at the same cross-sectional or longitudinal periods as the training data to decrease validity concerns, data collection is a never-ending process for algorithms such as TikTok so that they can continually place users into their proper groups, depending on what their interests and interactions are with the software. The training and testing data used in these algorithms both tie into the ANT framework, given that their inherent stochasticity will undoubtedly change the end-product delivered by an algorithm that uses training and testing data to predict what consumers will enjoy. While developers and consumers are perceived as distant relatives in terms of research, development, and eventually production, If machine learning is to truly be adopted, which it has been, this never-ending flow of data consumption must come from somewhere and creating fake data to apply to the real world does not seem like the best course of action for a multi-billion-dollar company.

Outscoping from specific regions to more general actors that exist in modern day society include but are not limited to users, software, developers, companies, stakeholders, and stock markets. Specifically in terms of company executives, CEOs and corporations are obsessed with the bottom line (Brassfield, 2022). Users give these corporations money to increase their satisfaction or to connect with others. While executives and customers both want the "newest and best products available," these two groups that exist within the same network want these products for different reasons. Consider another actor in the system: software developers.

Speaking with many computer-science colleagues over the past few years, many times when working on projects, their goal is to complete the project as ordered by management or professors to meet a deadline. It is easy to imagine a situation in which developers would want to extend a deadline to account for data privacy, but other actors, likely managers, or executives, decide that these steps would be irrelevant since the app is already fully functional and is merely providing a service that creates little to no profit for them. Even if adding features that secure a user's personal privacy may be brought up as potential iterations in future meetings with managers and developers, such a feature may hurt's the app's bottom-line, as the data collected by the app may be of some monetary value to the company, illustrating that once a problem is introduced, it can be very hard to reverse. Maintenance work for buildings provide a clear image as to what can happen if issues such as privacy holes in apps continue: if small issues in a building's structural integrity are not repaired over time, this can lead to serious problems for those that use the building (Learning, 2021). Developers who do not address privacy concerns early and often can create this issue for themselves on a different scale, and sometimes it goes against the short-term monetary interests of the company and is pushed back on. Such a situation can quickly turn into a question of ethics, demonstrating how a problem can exist for hundreds of thousands of companies, creating the wicked problem we face today.

In many aspects, data privacy is already a wicked problem due to social media's advertising and data mining, specifically regarding TikTok. The platform has become such a concern recently that the idea of banning the application was even considered for a time in 2020 by the Trump administration (*"Is TikTok"*, 2020). Such is the issue with wicked problems like pollution and climate change, reversing tendencies that have already been established by society is extremely difficult. To consider a small scale, James Clear writes in his book, *Atomic Habits,*

of common struggles to alter one's behavior. Since people are comfortable in the status quo, it becomes difficult to alter one's behavior (2018). While crises such as global warming are slightly more convoluted than incorporating 30 minutes of reading per day into one's schedule, wicked problems are practices that have already been established and engrained in society. Since social media, and specifically TikTok, have developed an iron grip around the development and interaction of millions of people with digital content, the notion that TikTok will change its data collection practices to protect its users from data privacy are unrealistic.

TikTok's rise to prominence in the digital world is second-to-none, with its ability to produce content that anyone could possibly want. Its means at which it collects and distributes information of, for, and by users, is largely the focal point of this research. While analyzing TikTok and other smart technologies through an academic lens can be useful to an extent, this type of analysis can only go so far. Understanding if users are informed of these processes and their perceptions of it elevates the credibility of the research, as it is not only viewed through an academic light, but also that of the actual consumer. Given that real people use these systems, speaking with someone who is a user to these types of systems provides critical insight into how a typical person might interact with the application, rather than someone studying this topic in-depth. Sitting down with a fellow University of Virginia student, it was easy to learn some of these insights that were not able to be found in academia (2022). Beginning with general questions about smart devices the interviewee uses typically, it became evident that she was very familiar with smart technologies as a whole and their abilities to help consumers maximize their comfort with the systems they interact with. She mentioned uses of social media such as YouTube, Instagram, Twitter, and TikTok. All very similar, yet all very different in terms of how she uses each. She also made mention of online shopping and getting inspiration for purchasing

things through targeted advertisements. It was interesting to hear her perspective that the targeted ads she receives are welcomed such that she can see things that would actually interest her, rather than generic ads like one would receive when watching cable TV.

Transitioning into TikTok and other forms of social media, I spoke with her extensively about her initial period of downloading the app, her experiences with the "For You" page, her interactivity with the app, and her general frustrations with the app. To provide context, the "For You" page is a stream of content curated for each user. "For You" is advertised as a personalized "recommendation system" that creates a unique experience for everyone (TikTok, 2019). Given that all have unique recommendations based on their prior interactions with the app, she highlighted the instant gratification that TikTok provides to her. She noted that TikTok is very good at cycling through content that users like, while discarding content that they decided to not engage with. Mentions of likes and comments were brought up as well, as she described herself as an active user of both features. She also mentioned, somewhat surprisingly, that she enjoyed that the app was able to create and fit her into a specific user group. This insight was eye-opening, since it seems that many people tend to dislike when preconceived images of them are formed, and the only difference in this case is that a machine was doing the preconceiving, rather than another person. However, after hearing her relative nonchalance about a software creating an image of her in its database, it was not surprising to hear that privacy was not as much of a concern for her in terms of being advertised products tailored to her interests. From her talking points, she heavily implied that her user experience trumped her personal privacy concerns. This sentiment seemed to stem from a trust that the information that she fed and continually feeds TikTok is neither damaging nor revealing. Given that linked profiles and social media sites can create comprehensive user profiles regardless of any technologies that can listen to

conversations, I felt that her sentiments were slightly misguided and that she would be better served knowing her full rights and the means in which each site explains what they do with her data (Cawley, 2022). Even if her habits do not change, allowing those who use apps to understand the extent to which the back end of the platform uses their data in unknown ways could be very eye-opening for users. I found this conversation to be very enjoyable and enlightening, and to speak with someone outside of an engineering mindset was very helpful to engage with a different perspective. I did recognize that the conversation had its limitations. Framing pointed questions without introducing bias was extremely different. Furthermore, certain portions of our conversation were centered around specific instances in TikTok and other forms of social media that required prior background knowledge, and it was tough to address these questions without providing my own biases into the context of the question. I did feel her role as an undergraduate in college served the research well, as "Gen Z" is a key demographic in the explosion of social media and therefore data collection, but I understand the limitations with having such a small sample size of opinions referenced in a research paper. With further iterations of this research, several surveys would be included from people with different backgrounds and ideologies, instead of just one individual.

While personal privacy is at the forefront of many operations, specifically abroad, in the digital age, user experience still evidently is valued highly amongst actors who use products and systems that collect data. Although no clear line has been drawn in many circumstances, there evidently exists a trade-off that must be recognized between a positive, personalized interaction while simultaneously securing the information of those who use these products. Potential lines to be drawn could involve allowing individuals the power to understand how and in what ways their data is being collected and used via informed consent. In an informed consent system,

consumers can make informed decisions about how they choose to interact with smart devices and technologies. However, a system of informed consent only works if the users in which the program would be enacted for are properly informed. Otherwise, the wicked problem remains just as prevalent as before. While there are other avenues that exist that have not been explored above, the notion remains: if we, as a society, do not give ourselves the chance to define a boundary between user experience and personal privacy, then we play a dangerous game where the line between the two adversaries becomes even more blurry than it already is.

Limitations and Future Work (Next Steps in Privacy Analysis and Potential Limitations)

Opportunities for future work will be abundant, given that technology and user experiences have become central to societal development in the 21st century. Case studies involving smart technologies, marketing, and advertising, along with advances in machine learning and artificial intelligence will undoubtedly create many avenues of further research for similar studies. However, on a broader scale, assuming that further research would involve major corporations, these companies may not be willing to release their means in which they collect data if they are committing likely legal, yet suspicious practices. Therefore, if future experiments were to be run under the framework of a control group of participants that have their personal data exploited and a treatment group that values privacy and opts-out of the exploitation aspect, it may be difficult to discern correlation between the factors that still allow for a positive personal experience while recognizing personal privacy. Furthermore, suspicious practices are hard to monetarily quantify, given their nature. Therefore, the extent to which exploiting users for their personal information to profit from is limited.

Personal Privacy May Not be a Thing of the Past, but Will it be a Thing of the Future?

Personal privacy has become a major issue in the age of digitization. The widespread use of credit cards, online banking, and smart technologies have made society reliant on digital interactions. There comes a point, however, in which convenience and personalization of these user experiences becomes invasive. In many circumstances, these points are unclear and have already been breached by lackadaisical efforts from those in power to protect consumers. Some governmental efforts and companies have provided consumers with ample resources to make informed decisions about how they would like their data to be utilized. On the contrary, users may not worry as deeply about their personal privacy, recognizing the interconnectivity of the world, and thus, the interconnectivity of personal data, are simply means to which we all must accept to be an active member of society. While these lines may be different for different actors, circumstances, and the like, the wicked problem remains. Personal data is of the utmost importance to everyone's livelihood and understanding the trade-offs between enacting a positive use experience and infringing upon personal information must be studied and acted upon. With the development of technology and algorithms, it is essential that some semblance of data privacy standards is enacted. Those with competing interests to those of consumers could become very powerful with information about the entire world at their fingertips. What sounds like a situation in which the few could control the many is eerily similar to that of a real version of Big Brother, if he is not watching already.

References

Bay, S., & Cohen, J. (2021, July 26). *How to turn off location services and stop your iPhone apps from Tracking you*. PCMAG. Retrieved October 23, 2021, from https://www.pcmag.com/how-to/how-to-turn-off-location-services-on-ios-devices.

Bonner, W., & Chiasson, M. (2005). If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. *Information and Organization*, *15*(4), 267–293. https://doi.org/10.1016/j.infoandorg.2005.03.001

Bonner, B., Chiasson, M., & Gopal, A. (2009). Restoring balance: How history tilts the scales against privacy. An Actor-Network Theory investigation. *Information and Organization, 19*(2), 84–102. https://doi.org/10.1016/j.infoandorg.2008.12.001

Brassfield, M. (2022, April 1). *CEOS are obsessed with this one number. here's why you should be, too*. The Penny Hoarder. Retrieved April 13, 2022, from https://www.thepennyhoarder.com/bank-accounts/ceo-bottom-line/

Cawley, C. (2022, February 12). *Does your phone listen to you for ads? or is it just coincidence?* MUO. Retrieved April 14, 2022, from https://www.makeuseof.com/tag/your-smartphone-listening-or-coincidence/

CBS Interactive. (n.d.). *Is TikTok a harmless app or a threat to U.S. security?* CBS News. Retrieved October 23, 2021, from https://www.cbsnews.com/news/tiktok-cybersecurity-china-60-minutes-2020-11-15/.

Christian Wigand. (2020, June 24). *Press corner*. European Commission - European Commission. Retrieved March 18, 2022, from https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166

Clear, J. (2018). *Atomic Habits: An Easy & Proven Way to Build Good Habits & Break Bad Ones*. Penguin Random House.

Cressman, D. (2009). A Brief Overview of Actor-Network Theory: Punctualization, Heterogenous Engineering & Translation. https://summit.sfu.ca/item/13593

Doffman, Z. (2021, January 30). *Why you should change this tiktok 'phone tracking' setting*. Forbes. Retrieved December 7, 2021, from https://www.forbes.com/sites/zakdoffman/2021/01/26/why-you-should-stop-tiktok-tracking-your-apple-iphone-or-google-android-phone/?sh=1f9d972a69de.

Fischer, S. (2020, September 10). *Tiktok reveals details of how its algorithm works*. Axios. Retrieved March 18, 2022, from https://www.axios.com/inside-tiktoks-killer-algorithm-52454fb2-6bab-405d-a407-31954ac1cf16.html

Freedom of Information Act (FOIA) Division. (2021, July 12). *The Privacy Act*. HHS.gov. Retrieved October 23, 2021, from https://www.hhs.gov/foia/privacy/index.html.

FTC report to Congress on Privacy and Data Security. (2021, September 13). Retrieved March 17, 2022, from https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf

How the TikTok algorithm works in 2021 (and how to work with it). Social Media Marketing & Management Dashboard. (2021, August 23). Retrieved October 23, 2021, from https://blog.hootsuite.com/tiktok-algorithm/.

Joby, A. (2021, July 30). *What is training data? how it's used in machine learning*. Learn Hub. Retrieved March 18, 2022, from https://learn.g2.com/training-data

Learning, I. (2021, July 28). *Building maintenance: Everything you need to know*. Online Skilled Trades Training for Personal & Enterprise. Retrieved April 14, 2022, from

https://www.interplaylearning.com/blog/facilities-maintenance/building-maintenance-everything-you-need-to-know

Melin, E. (2021). China's sharp power through TikTok : A case study of how China can use sharp power through TikTok (Dissertation). Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-101079

Moscaritolo, A. (2021, August 3). *The Best Smart Home Devices for 2021*. PCMAG. Retrieved October 23, 2021, from https://www.pcmag.com/picks/the-best-smart-home-devices.

Nagourney, A., Lovett, I., & Pérez-peña, R. (2015, December 2). *San Bernardino shooting kills at least 14; two suspects are dead*. The New York Times. Retrieved April 7, 2022, from https://www.nytimes.com/2015/12/03/us/san-bernardino-shooting.html

Nakashima, E. (2016, February 17). *Apple vows to resist FBI demand to crack iphone linked to San Bernardino attacks*. The Washington Post. Retrieved October 23, 2021, from https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html.

Orwell, G. (2021). *Nineteen Eighty-Four*. Penguin Classics.

Packer, G. (2019, June 9). *Doublethink Is Stronger Than Orwell Imagined: What 1984 means today*. The Atlantic. Retrieved April 6, 2022, from https://www.theatlantic.com/magazine/archive/2019/07/1984-george-orwell/590638/

Petrescu, M., & Krishen, A. S. (2018). Analyzing the analytics: Data privacy concerns. *Journal of Marketing Analytics*, *6*(2), 41–43. https://doi.org/10.1057/s41270-018-0034-x

Revealing potential new strategy, FTC teams up with States after Supreme Court Rules Agency not authorized to seek monetary remedies under section 13(b) of the FTC act. Akin

Gump Strauss Hauer & Feld LLP. (2021, May 27). Retrieved March 18, 2022, from https://www.akingump.com/en/news-insights/revealing-potential-new-strategy-ftc-teams-up-with-states-after-supreme-court-rules-agency-not-authorized-to-seek-monetary-remedies-under-section-13b-of-the-ftc-act.html

Self, T. (2012, June 27). *You can have any colour, as long as it's black*. HyperWrite News RSS. Retrieved April 12, 2022, from http://www.hyperwrite.com/Articles/showarticle.aspx?id=90

Staff, the P. N. O., & This blog is a collaboration between CTO and DPIP staff and the AI Strategy team. (2022, February 11). *Gramm-Leach-Bliley Act*. Federal Trade Commission. Retrieved March 17, 2022, from https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

TikTok. (2019, August 16). *How Tiktok recommends videos #ForYou*. Newsroom. Retrieved April 14, 2022, from https://newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you

Tomwfranck. (2021, June 8). *The Senate is set to pass a massive bipartisan tech and manufacturing bill that takes on China*. CNBC. Retrieved October 23, 2021, from https://www.cnbc.com/2021/06/08/senate-takes-on-china-with-bipartisan-manufacturing-bill.html.

University of Michigan. (n.d.). *History of privacy timeline*. Information and Technology Services: Safe Computing. Retrieved March 17, 2022, from https://safecomputing.umich.edu/privacy/history-of-privacy-timeline

University of Virginia fourth-year student in discussion with the author, March 2022.

Who regulates data mining? Data Science Degree Programs Guide. (2021, October 15). Retrieved March 15, 2022, from https://www.datasciencedegreeprograms.net/faq/who-regulates-data-mining/

Wolford, B. (2019, February 13). *What is GDPR, the EU's new Data Protection Law?* GDPR.eu. Retrieved March 18, 2022, from https://gdpr.eu/what-is-gdpr/

X. Zheng, Z. Cai, & Y. Li. (2018). Data Linkage in Smart Internet of Things Systems: A Consideration from a Privacy Perspective. *IEEE Communications Magazine*, *56*(9), 55–61. https://doi.org/10.1109/MCOM.2018.1701245