Question 1:

For years, in the shadows of the internet, big technology companies such as Facebook and Google have been collecting and selling data on users to advertising companies, creating the advertising method known as “targeted ads.” In everyday life, targeted ads may seem harmless, benign, not worth the attention of an entire nation. I recently searched for dumbbells on Google to seek out what options are out there for an at-home gym, and less than hours later I began seeing dumbbell ads on every website I ventured to. Having received a rather harsh advertisement rejection education from my parents, I find I can fairly easily ignore such targeted ads. Dumbbells, deals on school textbooks, clothes, Chapstick, HDMI cables, and plenty of other random products have all found their way across the internet as Google’s ads follow me wherever I go. The issue is, what if the topic of the advertisement is of greater importance than my chapped lips or not-functioning HDMI cable?

In 2018, it was released that a company named Cambridge Analytica used Facebook and other social media platforms and browsers as vehicles for extracting data on voters, and then targeting the most persuadable voters with ads specifically designed for them for the 2016 presidential election. Even if a person was not a Facebook user, if their friend was or they accessed a website that Facebook was linked to, data about their browsing activity could have been used to determine whether they were a swing voter, and what message would persuade them to vote for the preferred presidential candidate. According to Isaak and Hanna in “User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection,” (2018) political targeted ads contributed to successfully tipping the scale in a few key swing states with less than 100,000 voters. As Berghel mentions in his article “Malice Domestic: The Cambridge Analytica Dystopia,” (2018) persuasion and manipulation are not new to the world of politics, but those looking to persuade or manipulate now have an ease-of-access to voters never seen before. Berghel also notes that while Cambridge Analytica’s actions are certainly unethical, some of the blame for such manipulation falls upon users. One of the methods for extracting data about voters was via an app called “thisisyourdigitallife” that requested personal information that was later used for targeting swing voters. Berghel argues that in the information age, the user must be aware of deceit and manipulation techniques and adjust their internet usage accordingly (ie – not giving out personal data to random apps such as “thisisyourdigitallife”). In any case, in the Cambridge Analytica scandal, there is a clear-cut violation of the ACM Code of Ethics as it relates to user privacy, harm, and honesty.

As a future computer science professional and citizen of the United States, such behavior truly frightens me. In the past, mass persuasion was limited to people standing on street corners boasting their opinions or talk shows that generally only attract a certain population, but the ability to target specific swing voters on such mass scale is a whole new concept. Democracy is founded upon individual thought and free thinking, so barraging voters with specific ads based on their browsing activity crosses an ethical line. Broadly-based advertising and marketing techniques are reasonable because while they play at human desires and values, they are tailored to a wide audience with no individual persons in mind, and usually affect only the buyer and those in their closest sphere of influence. However, political targeted ads to sway voters based on their individual desires crosses lines into invasion of privacy, big tech trustworthiness, and has an impact on all 300+ million people in the United States, a much larger impact than if a father bought a grill because a scantily-clad woman persuaded him from a TV commercial.

Three key ethical principles of the ACM Code of Ethics (last updated June 22nd, 2018) are 1) avoiding harm, 2) being honest and trustworthy, and 3) respecting privacy. Harm is defined by the ACM Code of Ethics as “negative consequences, especially when those consequences are significant and unjust.” (Association for Computing Machinery, 2018). Although any presidential candidate winning an election is not unjust in of itself, manipulating the population to ascertain a specific outcome is significant and unjust, harming a population that if left to their own devices, would have brought about a different outcome. In addition, Cambridge Analytica, Facebook, and the other social media platforms and browsers failed to be honest and trustworthy by slyly saving and distributing information about users for unjust purposes – swaying the election. In the process, all mentioned companies failed to respect their user’s privacy. According to the ACM Code of Ethics, “Computing professionals should only use personal information for legitimate ends and without violating the rights of individuals and groups.” Cambridge Analytica absolutely abused this ethical principle by swiping user data without their knowledge, and then utilizing that data to manipulate voters. Although Facebook and other social media platforms and browsers have disputed their knowledge about whether they knowingly allowed Cambridge Analytica to have access to their user data, they also failed to respect user privacy by not ensuring their user data did not end up in the wrong hands. Since we have condemned the actions of these companies, how can we as a population move forward towards solutions to prevent similar scenarios?

There are three main areas that require modification – public policy, public education, and technological solutions. Public policy changes could include requiring online platforms to hand over more control to the user. This would take the form of consent forms to use, share, or sell the user’s data, as well as notifications of when their data is used, shared, or sold to third parties or if the company’s data is breached. (Isaak & Hanna, 2018) As for public education, new educational goals revolving around user privacy while online must take priority in elementary and middle schools to provide people with the information they need to keep their information private while using the internet. Berghel especially believes in the purpose of public education because our current culture promotes complete trust in the internet and its usefulness without considering the privacy-compromising implications. He notes that the public’s current “willing suspension of disbelief” as it relates to the internet is childish and completely irresponsible. (Berghel, 2018) So while changes in public policy could prove useful, public education about internet user privacy is also an absolute necessity. Technological solutions go hand-in-hand with some public policy solutions, in that if social media platforms were required by the government to notify their users of data usage, the social media platforms would devise ways to notify their users of data usage. Another technological solution includes respecting user “do not track” requests, completely blocking data disclosure to third parties, which would extend “to all ‘partner’ third-party sites, cloud services, and collection devices.” (Isaak & Hanna, 2018) My final (and favorite) technological solution is providing users with easy methods to “identify, terminate, delete, and uninstall any content or applications placed on their devices or cloud service,” thereby eliminating unknown-to-the-user data collection. There are plenty more possibilities for reducing or altogether eliminating internet privacy issues, but people need to advocate against big tech invasions of privacy to begin forcing implementation of effective solutions.

With that, I would like to conclude with a quote from George Orwell’s *1984* – “The masses never revolt of their own accord, and they never revolt merely because they are oppressed. Indeed, so long as they are not permitted to have standards of comparison, they never even become aware that they are oppressed.” (Orwell, 1961) The public has allowed invasion of their privacy on the internet without question, but now we must bring our communal ignorance of privacy invasion and manipulation to an end.

Question 2:

Back in the pre-2000s era of computers, malware was mostly harmless and more of a prank than an effective tool for harming others’ machines, excluding a few special programs, including the 1986 PC-Write Trojan, 1988 Morris Worm, 1991 Michelangelo Virus, and 1999 Melissa Virus. Trojan-type malware typically requires the user to install the malware onto their computer, usually under the assumption it will actually help them. Worms programmed to automatically spread themselves via the internet, email, or other means, but where viruses, generally user-initiated programs, are designed to damage or delete information, worms simply mass produce for the purpose of slowing down processes. Only in 1988 with the Morris Worm was a person (Robert Morris) actually convicted for malware-related crimes, and the Michelangelo Virus acted more as a wake-up call to the public than as a devastating virus. (Love, 2018) However, the Melissa Virus – the first effective mass-emailed virus - opened up a whole new can of “worms” for the 2000s to struggle against.

Right after the turn of the millennium (2000), the ILOVEYOU Worm infected millions of computers, causing more than $5.5 billion in damages to major corporations and governments, including the Pentagon and British Parliament. (Love, 2018) The rest of the early 2000s was plagued with other viruses and worms that spread via emails and the internet, including the 2001 Anna Kournikova Virus and the 2003 SQL Slammer Worm (known for being one of the fastest-spreading worms of all time). But more to the point of how early 2000s malware led to malware of today, in 2005 the Koobface Virus took advantage of social media platforms, including Facebook, MySpace, and Twitter, to spread itself across the internet. (Love, 2018) With the increase of malware attacks in the early 2000s, malware toolkits rose in popularity, which eventually led to the creation of the devastatingly effective rootkit, a form of malware that operates in lower layers of the operating system, making it hard to detect and nearly impossible to remove. Rootkit infections usually require the infected machine to have its hard drive completely wiped to clean out the malware. (Love, 2018)

From 2010 to the present, the amount of (spear) phishing – cybercrime where victims are tricked into providing personal information - via social media and mobile networks to steal information from average citizens has grown exponentially. Bots and Botnets have become especially prominent on social media platforms for their ability to lure users to malicious profiles and websites where the true malware will be hidden. Meanwhile, organized and more sophisticated forms of malware have taken root with political and magnificent financial goals in mind. The Zeus Trojan of 2011 implemented a new malware strategy known as keylogging – this form of malware is a type of spyware that records keystrokes, allowing the hacker to steal usernames, passwords, financial information, and other sensitive information from unsuspecting users. (Love, 2018) Cryptolocker in 2013 helped fuel the ransomware community, where the motivation for hacking is monetary, and Backoff in 2014 introduced malware to Point-of-Sale systems to steal credit card information from customers.

Today, we stand at the precipice of another new age in technology, one that involves advanced machine learning, the spread of misinformation, and globalized high reliance on connectivity, a combination for a possibly morbid future. The latest and greatest in malware includes an uptick in phishing and ransomware as machine learning allows for more effective phishing messages and popular cryptocurrencies allow for anonymous ransom payments. (Moore, 2020) While cryptojacking, which is basically using someone else’s machine for cryptocurrency mining, simply uses processing power for mining instead of productivity, cyber-physical attacks attach cyber threats to physical structures involved in every-day life, such as power grids, water treatment systems, and public transit systems. (Moore, 2020) For example, a hacker could threaten to cause immense damages to large-city electrical grids and require a ransom to prevent the city-wide disaster. Meanwhile, state-sponsored attacks involve governments spending resources in attempts to infiltrate other government systems to steal data and gain political or economical leverage over other nations. Smart medical devices, electronic medical records, and third parties such as vendors, contractors, and partners, can also pose security risks since extremely private and sensitive information is now being logged electronically. (Moore, 2020) And of course, social engineering remains at the forefront of scams, masterfully tricking victims into offering private information or providing funds. But exactly who are the masterminds behind of all these forms of cybersecurity threats?

Today, motivations range from corporate espionage to cyberwarfare to gamer issues. (Grimes, 2018) The non-exhaustive list from Grimer also includes monetary motivations, hacktivists, and resource theft. In the past, young kids and adults messing around with hacking programs comprised most of the malware author or hacker population, but today it has become a profession of high esteem (in the sense that their work is sophisticated, not in the sense that it is good). Professional groups set goals for what is to be stolen or damaged, and then devise malicious software (often ransomware) to infiltrate the necessary networks and datacenters to extract what they desire, whether it is for leverage or for use. (Grimes, 2018)

Social media platforms currently provide an extremely effective and extremely dangerous vehicle for hackers to spread and implement software. Via bots, phishing and spam are now commonplace on social media platforms, tricking users daily into clicking a link and propagating the malware and possibly infecting their device. Additionally, because “social media networks thrive on data sharing, contact connection, and content searching,” it makes them ideal for de-anonymizing unidentified information, resulting in possible identify theft or a social engineering attack. (S. M. W., 2020) And as edge-computing releases the processing stress off of mobile devices such as smart phones and tablets, potentially private information could be stolen in the exchange of information from the device to the edge nodes.

Looking to the future, as automation continues to unfold in everyday life, such as self-driving cars connected over a network for optimizing traffic patterns, people will (rightfully) continue to fear cybersecurity attacks, but the cybersecurity industry will rise to the challenge as the demand presents itself. According to Dr. Moore, there is “a severe shortage of cybersecurity professionals,” (Moore, 2020) but considering the drastic increase in computer science students at colleges and universities in America – 2020 saw an increase by 7.6% from 2019 (McDonald, 2020) – over time, I predict that the cybersecurity industry may finally catch up to the mayhem caused by malicious hackers. As this happens, I imagine cybersecurity applications and programs becoming more widely available to everyday users, effectively reducing phishing and other scam forms of malware. However, my fear is that those with malicious intent will always have the advantage, as their role as the “bad guys” merely requires them to circumvent modern cybersecurity methods. In stark contrast, the “good guys” have to invent new software that can account for possible new hacking methods. The era of machine learning will bring about not just better defense mechanisms, but also more effective attack mechanisms.

Ethically speaking, humanity can hope that one day, malware authors will lay their keyboards to rest after realizing how their actions harm others, but unfortunately that outcome is unlikely. But more importantly, it is crucial that cybersecurity software remains ethical in that it does not require invasion of privacy or taking complete hold of machines to establish proper security against malware. If the cybersecurity professionals begin using unethical methods to provide security, are they any better than the hackers?

References

Association for Computing Machinery. (2018, June 22). The code affirms an obligation of computing professionals to use their skills for the benefit of society. Retrieved March 12, 2021, from https://www.acm.org/code-of-ethics

Berghel, H. (2018, May). Malice Domestic: The Cambridge Analytica Dystopia. Computer, 84-89.

Grimes, R. A. (2018, April 05). What hackers do: Their motivations and their malware. Retrieved March 12, 2021, from https://www.csoonline.com/article/3267988/what-hackers-do-their-motivations-and-their-malware.html

Isaak, J., & Hanna, M. J. (2018, August). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. Computer, 56-59.

Love, J. (2018, April 5). A brief history of malware-its evolution and impact. Retrieved March 12, 2021, from <https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/>

Love, J. (2018, March 28). Malware types and classifications. Retrieved March 13, 2021, from https://www.lastline.com/blog/malware-types-and-classifications/

McDonald, C. (2020, December 16). Number of students taking computer science degrees Up 7.6% in 2020. Retrieved March 13, 2021, from https://www.computerweekly.com/news/252493740/Number-of-students-taking-computer-science-degrees-rises-76-in-2020

Moore, M. (2020, December 02). Top cybersecurity threats in 2020. Retrieved March 12, 2021, from https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

Orwell, George, and Erich Fromm. 1984. New York, N.Y.: New American Library, 1961.

W, S. M. (2020, July 17). Social media as a tool for malware propagation, cybercrime, and data loss. Retrieved March 12, 2021, from https://techgenix.com/social-media-malware/#:~:text=Attackers%20may%20use%20malware%20to,friends%2C%20family%2C%20and%20peers.