Brooke Dietmeier

Info 351: Information Ethics and Policy

May 23, 2024

Information Ethics Under the Microscope: Privacy, Crime & Security

I. Introduction

As beautifully stated by E.O. Wilson, "We are drowning in information, while starving for wisdom. The world henceforth will be run by synthesizers, people able to put together the right information at the right time." This paper embarks on a crucial exploration into the ethics of our digital age, focusing on three core areas: the evolution of hacking, the intersection of privacy and technology, and the complexities of government and political hacking. By tracing the journey of hacking from its roots as a creative curiosity to its current role in both crime and activism, and examining the profound impacts of technological advancements on privacy, this paper seeks to address the ethical landscape of cybersecurity. These reflections will serve as a foundation for my future work, guiding me towards helping to create a more secure and ethically responsible digital world.

II. Privacy In The Digital Era

A. Importance of privacy in the new era of digital technology

Bill Gates aptly noted in an interview about his opinions on the NSA, "Historically, privacy was almost implicit, because it was hard to find and gather information. But in the digital world, whether it's digital cameras or satellites or just what you click on, we need to have more explicit rules - not just for governments but for private companies." This quote highlights the

evolving nature of privacy in the digital era. Today, privacy is of utmost importance as it ensures freedom from intrusion, allowing individuals to live without unwarranted interference. It grants individuals the control over their personal information, enabling them to manage what is shared about them to other users, business, and government entities. Privacy protects individuals from being watched, tracked, or eavesdropped upon without their consent.

Historically, privacy threats were limited as personal information was rarely recorded or stored for a long period of time, as data often disappeared without a trace. However, with the advent of digital technology, there is now an extensive collection of every action ever performed online, a permanent record of every user's online activity. Privacy threats come in various forms, including government surveillance for law enforcement and tax collection, as revealed by Edward Snowden's disclosures about the PRISM program. In the private sector, personal data is often used for marketing and advertising without explicit consent. Unauthorized use by insiders involves employees misusing access to sensitive information. Additionally, theft of information through data breaches and cyber theft, as well as accidental data leaks due to human error, pose significant risks to privacy.

Edward Snowden, a former U.S. Computer Contractor, stated in his book *Permanent Record*, “Saying that you don’t need or want privacy because you have nothing to hide is to assume that no one should have, or could have to hide anything.” Snowden discovered that the government was accessing data on servers of major companies such as Microsoft, Yahoo, Google, Facebook, Youtube, and Apple. His disclosures revealed global surveillance programs in cooperation with telecommunication companies, which collected the telephone records of millions of U.S. customers without their knowledge or consent. These revelations stress the

pervasive and multifaceted nature of modern privacy threats, necessitating a strong and well-informed approach to protecting the personal data of users of digital technology.

B. Technology Advances and Privacy

Technological advances have a profound impact on our privacy and cybersecurity, especially with the rise of the internet and increasing use of digital devices. The biggest impact of technology on privacy is the vast amount of personal information that is collected, stored, and shared with third parties. A key example of this is the concern of the collections and misuse of search query data and the leakage of personal data through apps. Companies analyze this data to improve search services, target advertising, develop new services, train AI, and monitor user opinions. Who can see this mass amount of data collected on each user? This visibility raises serious concerns of privacy issues, especially when it comes to possible misuse of the private interests of users.

In Discussion two, [peer 1] argued how some people may argue that the use of big data and search queries enhances their internet experience by increasing the speed and accuracy of searches. During our debate we came to the conclusion that despite this argument, it is doubtful that these individuals feel comfortable with third parties having unconsented access to their search histories, especially when searching for private topics such as health and psychological problems, bankruptcy, gambling and other addictions, conspiracies, hot-topic political debates, and erotica [Baase S.].

C. Privacy in Business and social sectors - targeted advertising

The use of personal data for targeted marketing by third parties, corporations and governments raises serious ethical questions about privacy. As stated in Chapter two of the book [Baase S.], the Federal Trade Commission (FTC) works to ensure deceptive and unfair advertisements can be prosecuted, but this is becoming an increasingly harder job with the volume and sophistication of online advertising. Tools used by companies such as behavioral tracking, data mining, cookies and tracking pixels, big data analytics, geolocation services, and personalized algorithms make it more challenging for the FTC to monitor and regulate the myriad ways personal data is used for targeted advertising.

Data mining is often used by businesses and government agencies to search and analyze large amounts of data to find patterns and develop new information. In Chapter two, the book states how data mining includes a combination of profiling to determine characteristics of people likely to engage in certain behaviors, and matching to combine and compare information from different databases. A key example of the ethical dilemmas in data mining is Target's use of data mining to determine if a customer is pregnant by analyzing their purchase history. By analyzing certain products, Target could predict if a consumer was pregnant and send coupons timed to specific stages of their pregnancy. In one case, a high school girl was sent advertising for maternity products, which angered her father who accused Target of encouraging his daughter to get pregnant. However, he later discovered that his daughter was indeed pregnant and became highly concerned with how Target knew about his daughter's personal and private information before her own family did [*Forbes*].

While customer data is highly valuable to marketers, advertisers, and government agencies, it's also highly sensitive and personal. Tracking consumer behavior without complete transparency is unethical from both a deontological and utilitarian perspective. When companies

track consumer behavior without transparency they risk causing significant harm such as breaches of privacy, exploitation of vulnerable populations, and erosion of consumer trust. Manipulating customer data solely to meet business goals without mitigating risks to consumers is especially problematic, particularly with legislation like GDPR in place.

D. Reflection on change in thinking

Initially, I perceived data collection and targeted marketing as a beneficial tool used by companies to enhance the user experience by providing more relevant content and advertisements. I thought I understood how my data was being used, but I didn't fully grasp the ethical implications or the extent to which my privacy was being compromised. Through detailed discussions with my Peer Group one, my opinions and beliefs on privacy in relation to data collection in the digital era have changed.

Through the readings in this class and Edward Snowden's book, *Permanent Record,* I feel I have come to recognize the profound ethical concerns data collection and usage raises. I understand better that while technological advancements have brought many benefits, they pose significant risks to privacy rights. It is crucial we learn how to balance leveraging technology for innovation while still valuing the protection of individual privacy through careful consideration and regulation.

My awareness of the ethical considerations surrounding data collection and privacy has made me appreciate the need for transparency and informed consent in data practices. It is highly unethical for organizations to collect data through deceptive practices, they must inform individuals about what information is being collected. We may not be able to halt the mass

collection of data with the ever rising use of technology, but it's ethically crucial that organizations provide individuals with control over secondary uses of their data.

III. Crime and Security

A. Evolution of Hacking

The term hacking has undergone significant evolution over time, transitioning from a way to describe an inquisitive person to a person of malicious intent. As addressed in Chapter 5 of the book, the perception and nature of hacking has shifted throughout three different eras: era one from 1950-1970, era two from 1970-1990, era three during the early 2000s. According to Britannica, the first computer hackers were MIT students during 1955 when students were encouraged to find programming shortcuts to save time and money. These individuals were seen as inquisitive and creative, able to take a computer and make their systems do new and innovative tasks.

As time progressed into the 1970s, the term hacking began to take on a more negative connotation. There was a large shift during this era where hacking was no longer solely about pushing technical and intellectual limits, but also about pushing legal and ethical boundaries. As hacking evolved to include activities such as viruses, vandalism, harassment and theft, the U.S. government became concerned about the shift in hacking and passed the Comprehensive Crime Control Act in 1984 and the Computer Fraud and Abuse Act in 1986.

The early 2000s brought international and social conflict, marking a new motivation for hacking: social activism and governmental hacking. Facilitated by the spread of the World Wide Web, criminal and governmental hacker groups could operate across continents, leading to epidemic levels of computer viruses and large-scale cyber crimes. Today, hacking is more

prevalent than ever, occurring on both sides of the legal spectrum. This has led to the coinage of terms such as “white hat hackers,” “black hat hackers,” and “gray hat hackers” to differentiate between the various actions and ethical stances of hackers.

B. Government and Political Hacking

Since the terrorist attacks and international conflicts that came along with the 2000s, the use of hacking by governments and hacktivist groups introduces further ethical and legal complexities. As defined in Chapter 5 of the textbook, Hacktivism is the use of hacking to promote political causes. Just like any form of activism, the ethical justifications for hacktivism vary, with some viewing it as modern-day activism and others viewing it as criminal activity. The textbook detailed a fantastic example to highlight the complexity of analyzing the ethicality of hacktivism. Citing the comparison of a religious group hacking a gay dating website to protest homesexuality with an environmental group disabling a real estate developer’s website to protest a new housing development. These actions raise critical questions about whether hacktivists are merely exercising their freedom of speech and if these actions are covered under First Amendment rights. In our discussion, my peer group and I discussed the different examples where this argument may fall under First Amendment rights. However, it’s difficult to justify hacktivism as a form of free speech because it impedes the freedom of others to speak.

Government hacking involves economic and military espionage as well as disabling enemy infrastructures. A few examples include attacks originating from China on U.S. official and military projects, the Stuxnet virus used by the U.S. and Israel against Iran’s nuclear facilities, and the San Bernardino Case when the FBI hired a hacking company to unlock an Iphone. The ethical and legal implications of government hacking include issues of sovereignty, justification of cyber attacks as acts of war, and the potential for unintended harm to civilians.

Identifying the source of a government assisted attack has posed a significant challenge, as it often teeters on a thin line between accusing a state of international warfare and providing definitive proof. However, there have been a few notable hacking groups associated with governments including: Cozy Bear - Russia, Lazarus Group - North Korea, Double Dragon - China, Helix Kitten - Iran. The increase in the use of cyberwarfare and the widespread chaos government hacking can cause raises critical questions about balancing national security with respect of international law and human rights.

C. Hacker Tools and Techniques

In our group discussion for this module, we explored various hacking tools that we had personally experienced. For instance, I recounted a recent phishing attempt where someone impersonating my boss asked me to buy $600 worth of gift cards. Common hacking tools and viruses are faced by civilians on a daily basis, and some of these tools may cause financial distress while others escalate to more serious crimes. For example, one case study our group examined was about David, a working father whose 14 year old daughter was targeted by an online predator via her smartphone. David's inability to monitor her usage led to serious consequences and pointed out serious dangers of online grooming. Chapter 5 of the textbook goes on to highlight many more examples of various tools and techniques hackers use, including viruses, worms, and phishing schemes.

Furthermore, we discussed Season 1, Episode 2 of Mr. Robot, where Elliot (the main hacker) faces ethical dilemmas about joining the hacker group Fsociety. Our group debated the ethical implications of hacking and online criminal behavior. Agreeing that from a deontological viewpoint, the action of hacking is unethical due to privacy violations and loss of autonomy. While a utilitarian approach might justify hacking if it leads to a greater good, such as

dismantling a corrupt corporation, it still poses significant risks such as misuse of information. Our discussion was eye opening for me, as it emphasized the ethical complexities of hacking and online criminal behavior.

D. Reflection on change in thinking

As a cybersecurity-focused Informatics student, I am passionate about creating a safer and more transparent online world while ensuring the confidentiality and security of personal and private information for all users. This class has challenged me to view online criminal behavior from an ethical focus rather than strictly a technological viewpoint. I do believe that ethical hacking, also known as White Hat Hacking, is critical in our digital era to identify and address cybersecurity threats and exposers for individual users, companies, and governments. I also recognize that without Black Hat Hacking, there would be no need for ethical hacking. The balancing act between the two is crucial to maintaining robust cybersecurity defenses, making it critical to enforce clear cyber laws and ensure formal agreements of consent are put into place.

The evolution of hacking shows a shift from the early days when it was a creative pursuit by inquisitive minds to today's day and age where we often see the word "hacking" making news headlines for the wrong reasons. The early 2000s complicated this landscape with hacking used for social activism and government espionage, which raises critical questions about government involvement with cyber warfare. This class, specifically the readings, helped me better understand the ways in which hacking has evolved over the last few decades and encouraged me to keep an open mind when approaching cyber-related issues.

IV. Reflection on change in thinking

The combination of lecture, class discussions, and chapter readings have helped me shift my perspective to identify clear ethical standards as a cybersecurity student. Understanding ethics is a critical skill cybersecurity professionals need to have, as it is essential to establish a strong cybersecurity defense strategy. Hacking and online criminal activity involves complex ethical considerations that require balancing technological advancements with respect for privacy and individual rights. This class has helped elevate my ability to understand these critical complexities by emphasizing the importance of transparency, consent, and accountability in data practices. I have learned that ethical hacking involves more than just identifying vulnerabilities—it also requires a commitment to ethical principles that protect individuals' rights and promote trust in digital systems.

Understanding ethics is a critical skill for cybersecurity professionals because it is essential for establishing a robust cybersecurity defense strategy. Cybersecurity is not just about technical ability, it requires a moral compass to navigate the ethical dilemmas that arise in protecting data and systems. These issues are not black and white; they demand a sophisticated understanding of both the potential benefits and the potential harms of cybersecurity measures.

In future studies and workplaces, I will apply the ethical frameworks and analytical skills developed in this class to address cybersecurity challenges responsibly. I am better equipped to advocate for policies and practices that prioritize privacy and ethical considerations. This class has not only expanded my technical knowledge but also instilled a strong ethical foundation that will guide my actions as a cybersecurity professional dedicated to creating a safer and more honest online world.

Works Cited

Baase S. (2003). A gift of fire : social legal and ethical issues for computers and the internet (2nd ed.). Pearson Education.

Carpenter, K. (2013). Ethical issues of online advertising and privacy. *University of Tennessee Chattanooga*.

Cybercrime case studies. (2023, March 30). https://www.police.vic.gov.au/cybercrime-strategy-2022-2027/cybercrime-case-studies

Facts, F. (2023, January 25). The impact of technology on privacy and cybersecurity. *Medium*. https://fastfacts101.medium.com/the-impact-of-technology-on-privacy-and-cybersecurity-4d2037331311

Hayden, M. (2022, July 13). *The ethics of customer behavioral tracking*. Lytics Customer Data Platform (CDP). https://www.lytics.com/blog/ethics-of-customer-behavioral-tracking/

Hill, K. (2022, August 11). How Target figured out a teen girl was pregnant before her father did. *Forbes*. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=4c0a378f6668

National Cybersecurity Alliance. (2023, March 17). *How can ethical hacking be "Ethical"?* https://staysafeonline.org/cybersecurity-for-business/how-can-ethical-hacking-be-ethical/

Volle, A. (2023, May 12). *Hacker | Definition, Types, & Word Origin*. Encyclopedia Britannica. https://www.britannica.com/topic/hacker

[peer 1] (2024). Discussion 2: Privacy https://canvas.uw.edu/groups/1080384/discussion_topics/8772256

[peer 1,2,3] (2024). Discussion 5: Crime and Security https://canvas.uw.edu/groups/1080384/discussion_topics/8772287