# Essay Reflection: Addressing Cyber Attacks

*Abstract*—**The purpose of this essay is to present the case that the presentation, "Data Breaches", by Avi Gesser shed important light on the significance of professional ethics and privacy in technology by emphasizing the necessity of moral decision making, tackling the difficulties presented by AI and imposing strong privacy safeguards.** The connection between these insights and the course units on professional ethics and privacy will be examined in this reflection, with a focus on how ethical decision making shapes technology practices, professionals' obligations to safeguard user privacy, and the new moral challenges brought about by AI developments. This essay will illustrate the importance of these concepts in directing responsible and reliable technology development.

***Keywords—Data Breaches, Decisions, Cyberattacks, Privacy.***

## I. Introduction

We have had the honor of hearing from a range of guest lecturers during this course, each of whom brought a distinct viewpoint to share on essential computer science subjects. Avi Gesser, a cybersecurity, privacy, and artificial intelligence expert who counsels large corporations, delivered one of the most influential talks. The discussion made a great impression on me because I found that privacy safeguards and the moral consequences of AI in particular struck me as being extremely relevant to my career goals. I found resonance in the talk's emphasis on increasing consumer knowledge of cyberattacks and providing them with protective measures. Also, the strong need for technology professionals to respect moral principles while protecting consumers' privacy and security in a world that is becoming more interconnected. **The purpose of this essay is to present the case that the presentation, "Data Breaches", by Avi Gesser shed important light on the significance of professional ethics and privacy in technology by emphasizing the necessity of moral decision making, tackling the difficulties presented by AI and imposing strong privacy safeguards.**

## II. Supporting Arguments

### *A. Practical Judgement*

The importance of making moral decisions when dealing with cyberthreats was one of the main lessons learned from Avi Gesser's talk. Businesses strive to keep their systems safe from intruders, they must also take care to respect users' rights and privacy. For instance, while intrusive monitoring technologies and data collection methods may be useful in preventing cyberattacks, they may also compromise user privacy. This truly got me thinking about how simple it is to ignore the moral consequences of cybersecurity in favor of concentrating only on its technical components. In line with our course unit on privacy, Gesser's discussion emphasized the need for professionals to strike a balance between safeguarding systems and upholding users' rights. We discovered how important it is to protect user privacy and to be open and honest with people about the usage of their data. The ACM Code of Ethics and Professional Conduct, which emphasizes that computing professionals must make judgments that benefit the public and prevent harm, also links into the larger idea of professional ethics [1]. It's increasingly evident that making moral decisions is crucial in the technology industry. I learned from Gesser's talk that as aspiring IT professionals, we must be mindful of how our choices would affect people's security, privacy, and trust. The development of artificial intelligence brings with it a new set of problems that further complicate the ethical boundaries and need for more careful moral analysis.

### *B. AI Risks*

As we examine the relationship between artificial intelligence and cybersecurity in greater detail, it becomes evident that AI presents a unique set of difficulties, particularly when it comes to cyberattacks. The emergence of deepfakes where AI-generated audio or video recordings that can realistically mimic actual people is one of the most alarming risks. These can be exploited to influence financial systems, mislead people, or even distribute false information. Gesser's explanation of how attackers are now using AI to develop increasingly complex and difficult to detect threats highly caught my attention. It is challenging for conventional security measures to keep up with the increasing prevalence of AI-driven attacks, such as automated phishing in addition to deep-fakes. As a computer science student, I was somewhat taken aback by how intricate the field of digital security is growing. However, Gesser also discussed solutions to these problems, like biometric verification and multi-factor authentication which help confirm user identification and stop unwanted access. Given how easily AI can be exploited to deceive, these technologies are becoming crucial to maintaining security. I believe that using AI responsibly is essential for user protection, such as when it comes to AI systems that are made to identify deep-fakes or fraudulent behavior. This relates directly to the professional ethics section of our course, where we discovered that developing innovative technology alone is insufficient. Thus, we also need to take responsibility for their application. After hearing Gesser's talk, I came to the conclusion that although AI can solve a lot of cybersecurity issues, it also raises new ethical issues that require careful thought. As aspiring technology professionals, it is our responsibility to ensure that the technology we create serves to safeguard consumers' privacy rather than being used as weapons.

### *C. Vigorous Privacy Measures*

The significance of enforcing privacy safeguards, particularly in light of emerging cyberattacks, was one of the main lessons learned from Avi Gesser's talk. Gesser clarified that in order to preserve user privacy, businesses must put strong mechanisms in place to make sure that private information is not misused or made public during cyberattacks. This subject brought to mind the difficulties we covered in our privacy course section, where we talked about how businesses frequently have to balance gathering valuable data with protecting customer privacy. For instance, the capacity of technologies like Clearview AI, which have been widely used by police enforcement, to identify people in photographs with shocking accuracy raises questions about the possibility of privacy infringement [2]. This highlights the necessity of strict rules for the usage of such technologies. Businesses must use measures that collect only the most important information, encryption and anonymity to safeguard sensitive data in order to reduce risks. In our course, we also looked at professional ethics, and it's evident that protecting privacy is not only required by law but also by ethics. I became aware of the significance of incorporating robust protections into each phase of product development after listening to Gesser's presentation. As aspiring tech workers, it is our duty to make sure that privacy is a fundamental component of our solutions rather than only a last-minute addition.

## III. Conclusion

*In all, by focusing on moral decision-making, addressing AI-driven issues, and implementing robust privacy precautions, Avi Gesser's lecture "Data Breaches" emphasized the significance of professional ethics and privacy in technology.* As I think back on these concepts, I see how important these ideas are to achieving my long-term objectives in AI. Innovation is important, but so is making sure technology is applied morally. *Since technology is advancing and posing new risks like AI-driven attacks and privacy violations, these lessons are especially crucial today. I'm motivated to put ethics and privacy first in my work as a result of Gesser's talk, helping to create a more secure and reliable digital future.*

## Acknowledgment

Firstly, I want to sincerely thank Avi Gesser for the enlightening talk about artificial intelligence, privacy, and cybersecurity. I also want to express my gratitude to my group mates: Kalen, Alex, Joshua, and Vlad for helping me gain a deeper comprehension of the course materials. The concepts discussed in this essay were greatly influenced by the contributions from Avi, Alex and Kalen in the privacy policy section as well as in the clarification of ethical issues in AI. I value their cooperation and the variety of viewpoints they contributed.

## References

[1] "The Code affirms an obligation of computing professionals to use their skills for the benefit of society.," Acm.org, 2024. https://www.acm.org/code-of-ethics (last accessed: Nov. 29, 2024).

[2] [1] J. Clayton, "Clearview AI used nearly 1m times by US police, it tells the BBC," Bbc.com, Mar. 27, 2023. https://www.bbc.com/news/technology-65057011 (accessed Dec. 01, 2024).