

Sean Shreve

12MAR2026

CYSE 200T

Professor Duvall

Discussion Board: Ethical Considerations of CRISPR Gene Editing

Based on your readings related to the BioCybersecurity section of this course, identify possible ethical considerations and explain your position.

CRISPR gene-editing technology offers significant potential benefits in medicine and biotechnology, but it also raises serious ethical concerns related to privacy, cybersecurity, and societal impact. The genome data itself is center stage of the ethical consequences of this technology. Genetic information contains incredibly detailed information about an individual's health, traits, and ancestry. Compromising this data could lead to criminal use, such as extortion, identity theft, or discrimination based on genetic outcomes. As an example, the National Institute of Standards and Technology (NIST), genomic data breaches could reveal disease risks or personal traits and potentially be used for financial exploitation or discrimination in areas such as insurance or employment (Pulivarti et al., 2023).

Cyberbiosecurity is now growing in response to higher vulnerability of digitizing DNA data. This field of study involves biological systems that interact with digital infrastructures, such as databases used by researchers and bio-med companies. Researchers have now demonstrated that synthetic DNA can now have code encoded into it, which opens new avenues to potential exploitation. It is currently unlikely that attacks of this complexity exist, but it does

highlight how biological data and computing systems are becoming increasingly interconnected, creating new security risks that must be addressed (Coldewey, 2017).

The development of CRISPR technology demonstrates that scientific progress must be balanced with strong ethical frameworks, cybersecurity protections, and privacy safeguards. Unfortunately, these are lofty goals that will have its difficulties getting built to an appropriate standard. We may see serious consequences in the future to companies/organizations that may not follow security protocols correctly. However, I am hopeful of the gains we will make with medicine and biotechnology. Perhaps the tradeoff will be worth the ethical compromise many take in pursuit for advancements in medical care.

References

Coldewey, D. (2017, August 9). *Malicious code written into DNA infects the computer that reads it*. TechCrunch.

Pulivarti, R., Martin, N., Byers, F., Wagner, J., Zook, J., Maragh, S., McDaniel, J., Wilson, K., Wojtyniak, M., Kreider, B., France, A., Edwards, S., Morris, T., Sheldon, J., Ross, S., & Whitlow, P. (2023). *Cybersecurity of genomic data (NIST IR 8432)*. National Institute of Standards and Technology.