BLUF:

As DNA is digitized, stored and commodified in ever greater volumes, law faces a crucial question how can those dealing in genetic property rights strike the right balance between encouraging solutions to disease by promoting investment, innovation and personalized medicine but without yielding up our genetic information on terms which make us less free, open to discrimination or exposed still further to irreversible privacy harms? Unlike a stolen credit card number, which can be easily replaced, DNA is not something that can be altered if it falls into the wrong hands; it has lifelong and generational consequences. To protect humanity from the misuse of genetic technology, governments, biotech companies and IT security professionals need to work together on legal frameworks, ethical guidelines and cybersecure measures to be implemented for benefits derived by human genomics without compromising individual rights or human dignity.

Ethical and Societal Implications -Aniyah

Many people argue that individuals should retain full autonomy over their own genetic data including the right to share or sell it especially if doing so can advance medical research, personalized treatment, or genealogy. The promise is compelling: donors might contribute to cancer research, pharmacogenomics, or population health studies. But this autonomy must be tempered with safeguards, because DNA is not just any data: it's deeply personal, immutable, and carries implications for one’s relatives as well. Laws should be straightforward and let you know the real risks of selling your data. *Knowing me, yes, I would take a DNA knowing it could be hacked in the right reassurances. I would be sure to go with the company with rigorous*

encryption standards. Having a company who deeply understands that DNA exposure is irreversible is crucial.

Privacy and Security - Kaemon

DNA is a far more dangerous form of personally identifiable information (PII) to lose than a Social Security number because it contains permanent, unchangeable details about a person's genetic identity, health risks, and biological relationships. While a Social Security number can be replaced and monitored for fraudulent use, DNA cannot be altered once exposed, making it a lifelong vulnerability. If DNA data is hacked, the long-term consequences can be severe. Hackers could use genetic information for identity theft, discrimination in health or life insurance, or even to make unauthorized medical inferences. Beyond individual harm, a DNA breach can also reveal information about family members and descendants, exposing entire genetic lineages to privacy risks that persist across generations. *In my opinion, DNA should be protected more than it already is if it is detrimental if hacked. If this is exposed, the consequences would be too severe to recover from.*

Technology and Responsibility-Aniyah

Yes, I believe that companies who deal with DNA should be regulated by cybersecurity. *It's important to know that like banks and federal buildings, DNA is also a high valued asset.* The consequences of breach or misuse are not simply monetary losses; they are existential, irreversible, and far-reaching.

Conclusion- Aniyah & Kaemon

The article shows that as our DNA becomes part of the digital world, protecting it is more important than ever. DNA data can help doctors and scientists make big discoveries, but it also creates serious privacy and security risks if it's stolen or misused. Unlike a password, we can't change our DNA. That's why companies, lawmakers, and cybersecurity experts must work together to create strong rules and protections. *We need to make sure the use of genetic data helps people without putting their personal information or future at risk.*