Lavontay Johnson

Prof. Kirkpatrick & Prof. Osgood

CYSE 495

28 March 2025

Untitled

BLUF:

Consumer genetic testing services including 23andMe and AncestryDNA enable scientific breakthroughs but simultaneously create substantial cybersecurity vulnerabilities because they digitize DNA information. The services provide important health and ancestry information yet they reveal highly personal and permanent data to cyber threats. According to Juliette Rizkallah the increasing number of hackers target genetic data for financial gain and social manipulation as well as ideological purposes. The 2018 MyHeritage data breach demonstrates why immediate legal and security measures must be established to stop unauthorized use and protect individual and family privacy rights and prevent discrimination.

Introduction:

Digital innovation advances at a rapid speed which causes technological boundaries to merge with biological systems. I believe the growing industry of direct to consumer genetic testing demonstrates a notable example of how human DNA becomes digitized through this process. People can learn about their ancestral history along with inherited traits and health risks through submitting saliva samples to services such as 23andMe and AncestryDNA. The services give customers valuable information, but they create new security threats which cybercriminals could potentially leverage. Our most intimate data now exists online which means our privacy and security stand at risk of exponential deterioration like Juliette Rizkallah said.

DNA as Digital PII

I think that the conversion of DNA into digital format creates a transformative power which holds both beneficial aspects and potential risks. I feel that the conversion of DNA into digital format has facilitated new biomedical research efforts which help scientists understand diseases better and create personalized treatments and deliver them more effectively. Digital DNA translation creates a new type of Personally Identifiable Information, also known as PII, which stands as the most private type. In my opinion, DNA stands as an unalterable piece of information because it cannot be modified like credit card numbers or Social Security numbers. When unauthorized parties acquire DNA data the effects become extensive while remaining everlasting. Genetic data faces risks from cybercriminals who aim to exploit it for financial benefit and power along with ideological motivations that I feel exceed current security standards and legal protections.

Cybercriminal Interest in Genetic Data

I believe the main issue Rizkallah highlights is cybercriminals showing rising interest in genetic databases. I think the digital format of DNA shares the same risks as financial data and medical records since thieves can steal it and sell it to darknet markets or utilize it to execute complex social engineering attacks. According to Rizkallah DNA possesses significant worth on darknet markets because awareness among cybercriminals about its value keeps increasing. The threat is real because hackers have launched attacks against genetic testing corporations in the past. The MyHeritage data breach from 2018 revealed the email addresses together with hashed passwords of more than 92 million users. The breach triggered a security wake up call for the whole industry despite the absence of stolen genetic information.

Privacy and Discrimination Risks

The consequences for privacy emerge as deeply concerning issues because of these security breaches. When genetic information gets compromised it reveals both personal identity and medical information along with information about biological relatives and disease vulnerabilities. I feel a hypothetical scenario shows how employers might discriminate against job applicants through data misuse by screening out candidates who demonstrate potential health issues or unwanted genetic traits. Insurance providers may increase premiums and revoke coverage when they discover genetic illness tendencies in their customers. I feel the two situations would impose penalties based on genetic factors which people cannot control.

DNA Misuse for Control and Surveillance

The digital representation of DNA poses a disturbing potential to become an instrument for political or social intimidation. Authoritarian governments and extremist organizations could use genetic information to locate specific population groups which they would then aim to harm. I feel modern history already demonstrates how technological instruments get transformed into dangerous instruments that defy their initial purpose. The combination of consumer genetic data with public law enforcement repositories through DNA evidence has proven effective for solving cold cases. The implementation of this technology for justice purposes in criminal investigations exposes individuals to potential privacy violations unless strong legal protections exist. Uploading personal genetic data can lead to police investigation of family members without the uploader's awareness.

Weaponization of Genetic Traits

I truly believe that one of the more alarming possibilities is the weaponization of genetic traits. A bad actor could manipulate digitized DNA data to carry out targeted attacks, both in cyber and

biological domains. For instance, state sponsored entities might develop biologically engineered weapons aimed at individuals with specific genetic markers. This may seem like science fiction but the increased availability of personal DNA profiles online makes such scenarios possible. Even in the business world, a competitor could use leaked genetic data to sabotage high performing employees by exposing them to have a predisposition to certain diseases or mental health disorders thus forcing them out of leadership pipelines.

Ransomware Meets Genetic Extortion

DNA based extortion is truly a new and emerging threat in the cybercrime landscape. Digital DNA has tremendous value on the dark web.. Cybercriminals could threaten to leak or alter genetic information unless a ransom is paid. Imagine a scenario in which a threat actor gains access to your DNA profile and uses it to falsely implicate you or a family member in a crime. Or they fabricate a genetic predisposition to a stigmatized illness and threaten to release it publicly. This type of extortion is more damaging than financial fraud because it strikes at the core of human identity, which is personal.

Genetic Social Engineering Attacks

I feel genetic information can also be used by social engineers who are popular among cybercriminals. A person's genetic background gives a way to highly customized phishing attacks. A malicious actor could send a targeted email to someone referencing rare family illnesses, fake medical trial invitations or fake offers for advanced treatment based on their genetic code. The message seems deeply personal and relevant, so the likelihood of falling for the attack increases exponentially. Attackers can also use DNA data to create fake family trees or impersonate relatives and thus open new fraud pathways.

Legal Gray Zones and Lack of Oversight

I think one of the most pressing concerns is the absence of robust legal protections surrounding genetic data. Financial and health data are subject to strict federal guidelines like HIPAA and PCI-DSS, but consumer DNA exists largely in a gray area. Rizkallah emphasizes the need to demand better transparency from DNA testing companies about how data is stored, shared and secured. At present, there is no updated legislation or standards for cyber biosecurity, so companies have a wide latitude to share genetic data with third parties, often under vague terms of service that users rarely read.

The Responsibility of the Consumer

As Rizkallah asserts, consumers are not powerless in this digital frontier. Knowledge is the first step toward protection. Before submitting DNA to a testing service, people should ask critical questions: Where will this data be stored? Who has access to it? How will it be encrypted? While we may not be able to stop the march of innovation or the interest of hackers in exploiting it, we can slow their progress by being more discerning with the companies we trust and demanding stronger accountability measures. Awareness of a well-informed public can be a powerful deterrent against corporate negligence and cybercriminal exploitation.

Conclusion: Innovation Versus Identity Risk

The digital DNA revolution provides significant benefits to medicine, ancestry and public safety but opens a new frontier for cybercrime. As Rizkallah stresses in Hacking Humans, the stakes are higher than ever. Unlike credit card numbers, our DNA cannot be changed or canceled. It is the blueprint of who we are and its misuse can potentially alter lives, families and societies. Security professionals, lawmakers, businesses and individuals must work together to ensure that

the next wave of digital innovation does not come at the expense of our most fundamental asset, our identity.