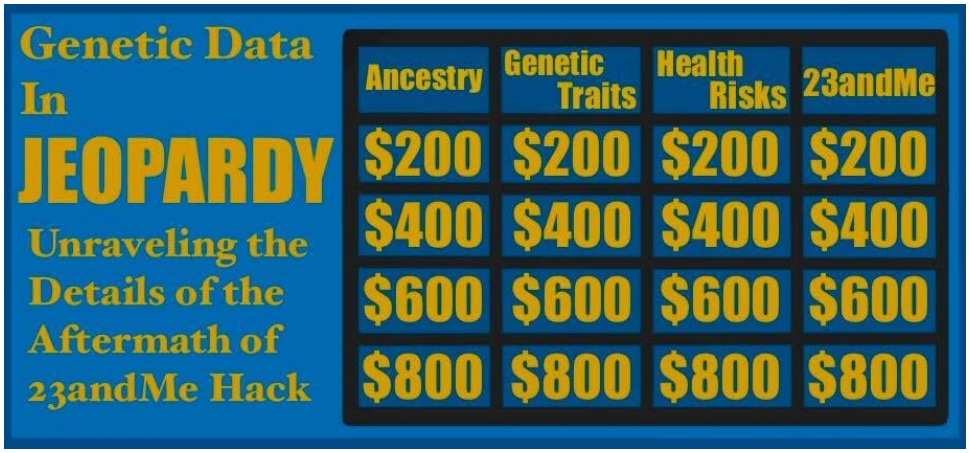
BRB Business Review at Berkeley
UC Berkeley's Leading Undergraduate Business Journal

Genetic Data in Jeopardy: Unraveling the Details of the Aftermath of 23andMe Hack

ON: FEBRUARY 7, 2024 / IN: LATEST, TECHNOLOGY



Author: Tamara Yaghi, Graphics: Walton Bullard

The BRB Bottomline: This article explores the 23andMe hack, the ethical implications, the risks associated with data breaches, and possible future implications.

All About the 23andMe Hack

23andMe is a genetic testing company that analyzes individuals' DNA to provide detailed reports on their ancestry, genetic traits, and potential health risks. They also conduct genetic research using customer data for scientific advancements. In July 2023, news broke that the renowned genetic testing and analysis company, 23andMe, had suffered a significant data breach. Hackers had infiltrated the company's databases, gaining unauthorized access to the genetic information of millions of individuals worldwide. The breach compromised highly sensitive and personal data, including customers' genetic profiles, health information, and other personally identifiable information. This disastrous and sudden data breach raised even more concerns about privacy and data security in today's digital age and about the safety of genetic testing.

Ethics, Risks, and Everything That Went Wrong

The 23andMe hack raises profound ethical questions regarding the use and protection of personal genetic data. Customers willingly share their genetic information with 23andMe in exchange for insights into their ancestry, health risks, and other genetic traits. However, this incident highlights the potential risks involved in trusting a third-party organization with such intimate details.

One ethical concern is the issue of informed consent. Customers often consent to the use of their genetic data for research and scientific studies. However, it is unclear whether

customers fully comprehend the potential risks when sharing their information. Companies tend to use consent agreements which often seek broad permission, making it difficult for individuals to fully comprehend all potential uses of their data. Additionally, some companies may not be transparent about how they store, share, or use genetic data. Some individuals may underestimate the risks or feel optimistic about the potential benefits of research, leading to them readily sharing their data.

Moreover, the breach reveals that, even with consent, there is a need for stricter safeguards to ensure the security and privacy of genetic data. As a world-renowned organization, 23andMe, along with other similar organizations, should prioritize the safety of their customers because genetic data can reveal sensitive information about an individual's health, ancestry, and predispositions to certain conditions. Inadequate safeguarding of customer data could have a direct negative impact on a company's brand, customer loyalty, and revenue. Therefore, the use of cryptography and blockchain-based solutions to manage data could prove to be of great value. Additionally, there are ongoing debates about HIPAA compliance for 23andMe and similar companies. Regulatory bodies in the US and elsewhere are actively considering this issue and weighing the potential benefits and drawbacks of applying HIPAA-like regulations to the broader realm of genetic data.

Another ethical consideration to take into account is the issue of potential discrimination and stigmatization based on genetic information. As genetic testing becomes more accessible, there is a risk that individuals may face discrimination from employers, insurers, or other entities based on their genetic predispositions to certain health conditions. For example, genetic data can reveal predispositions to certain diseases or health conditions, which could be exploited by insurance companies to deny coverage or charge higher premiums. Employers might discriminate against individuals based on their genetic predispositions, like Alzheimer's or cancer, causing insurance companies to use this information to deny coverage or increase premiums, even if the individual is currently healthy. Certain genes might be associated with higher risks for specific workplace injuries or illnesses, and employers could potentially use this information to deny jobs or limit career opportunities based on perceived health risks. As for this breach, the hackers were targeting individuals with Ashkenazi Jewish heritage and Chinese ancestry. They were able to illegally sell classified genetic information about these two communities on the black market. Till this day, the reasons behind targeting both these communities remain unknown and under investigation. Exploiting this sensitive information for financial gain is ethically problematic but nonetheless lucrative.

Furthermore, the 23andMe hack raises the question of ownership and control of genetic data. It asks: "should individuals have the right to control and access their genetic information, or does it become the property of the testing company and other entities?" The hack highlights the importance of regulatory bodies forcing companies to clarify ownership rights and establish clear guidelines for data handling and sharing in the genetic testing industry. In addition, if customers are given full ownership over their data, does that mean their information is protected and hack-proof? Once again, a blockchain-based system, as will be explained later, would put users in full control of their data as to who could have access, for how long, and when.

Lastly, the potential for misuse or unauthorized access to genetic data raises concerns about surveillance and privacy. Genetic information is highly personal and sensitive, and unauthorized access or breaches can have significant consequences, including identity theft or exploitation of the data for nefarious purposes. The stolen genetic data could be combined with other personal information to perpetrate identity-related crimes, such as opening fraudulent accounts or even blackmail. As witnessed through the 23andMe hack,

identity theft is extremely easy because these databases hold personal and highly confidential genetic and familial information for millions of people globally.

The Unfortunate Domino Effect

Obviously, following such an enormous data break, consumers lost complete trust in 23andMe and other genetic testing companies. Genetic testing companies also face short-term and long-term implications and direct and indirect costs, such as brand equity, loss of partnerships, loss of investors or reduced funding, legal fees, regulatory penalties, required security measures, and customer refunds. However, the biggest losses were incurred by 23andMe. According to Yahoo Tech, 23andMe's stock fell by 95%, causing the company's value to fall from $6 billion to $345 million. To add on, the NASDAQ stock exchange is considering delisting 23andMe from its stock exchange as a result of the mounting lawsuits that the company faces. As a result, governments and genetic testing companies are continuously reminded of the importance of implementing stronger safeguards to prevent unauthorized access and breaches of sensitive genetic information.

How to Build Hack Proof Databases

The future of genetic testing, taking into account the 23andMe hack, will likely involve heightened emphasis on data security and privacy protection. In response to the hack, genetic testing companies must invest in enhanced security measures including blockchain technology, advanced encryption protocols, and ongoing monitoring of databases to detect and prevent data breaches and minimize the risk of possible breaches. Blockchain technology is an unchangeable ledger (secure network) that stores an infinite amount of data securely. Therefore, with blockchain's secure and transparent nature, it holds promise in this regard, enabling individuals to share their data securely while maintaining ownership and control.

Some great examples of blockchain technology being used as a security tool can be found in the following companies: Philips Healthcare, Health Linkages, and Hashed Health. These companies employ blockchain technology to enhance data security, privacy, transparency, and compliance in the genetic testing, healthcare, and medical fields. For example, Philips Healthcare utilizes blockchain technology to build a secure ecosystem for storing patient medical data, in order to allow global medical facilities to collect and analyze various types of healthcare data. On the other hand, Health Linkages established secure digital blockchain networks for sharing patient information with medical centers. Therefore, it is evident integrating blockchain technology in such sensitive apps is feasible, highly secure, and a necessity to ensure no data breaches occur and safeguard all customer information.

Additionally, stricter regulatory frameworks and industry standards must be implemented by regulatory bodies or governments to ensure the protection of personal genetic data. Governments and regulatory bodies must establish clear guidelines regarding the collection, storage, and usage of genetic information. This includes ensuring informed consent, implementing strict security measures, and holding companies accountable for data breaches.

Furthermore, the incident must fuel discussions regarding customer ownership and control over their highly confidential genetic data. There must be an increased transparency and accountability regarding the use of a customer's genetic data. Genetic testing companies must be required to provide clearer information to customers regarding how their data will be used, who will have access to it, and how it will be protected. Additionally, individuals globally must become more forceful in asserting their rights over their genetic information, leading to new models of data ownership and consent; it must be demanded.

Overall, the 23andMe hack serves as a catalyst for the genetic testing industry to prioritize

and strengthen data security and privacy measures, ultimately shaping the future of genetic testing towards increased protection and responsible handling of personal genetic information.

To Sum it All Up

The 23andMe breach wasn't just a data leak; it was a detonation, blasting open a fault line in our digital world and exposing the precarious state of our genetic privacy in the digital age. The consequences for those affected remain shrouded in some uncertainty, but the potential harms – identity theft, discrimination, and the misuse of our most intimate information – are no longer abstract threats. They are a reality now.

Yet, amidst this stark landscape, a flicker of hope persists. Through collective action and unwavering resolve, we can craft a future where our genetic data isn't a liability, but a powerful tool wielded with informed consent and ethical responsibility. Let this breach be the catalyst for a new era of data privacy, where our genetic blueprints aren't stolen goods, but cherished treasures safeguarded not by mere technology, but by our collective demand for a world where privacy reigns supreme.

Moving forward, we must address the ethical challenges head-on. Robust regulations, empowered oversight, and clear industry standards are not luxuries; they are necessities. We cannot allow individuals to suffer the consequences of poorly built systems or face discrimination based on their genetic legacy. It is our collective responsibility to ensure that the benefits of genetic testing are harnessed responsibly and securely while upholding individual privacy and autonomy. Only then can we truly emerge from the shadow of the 23andMe breach and build a future where our genetic data serves as a source of empowerment, not vulnerability.

Take Home Points

- The 23andMe hack compromised the genetic information of millions of individuals, highlighting the need for better privacy and data security in the genetic testing industry.
- Ethical concerns and implications include but are not limited to: genetic data being used for discrimination and stigmatization of individuals by their community or employers or insurance companies, consent and customer data ownership guidelines regarding genetic testing, surveillance issues, privacy issues, and potential identity theft.
- Genetic testing companies should invest in enhanced security measures, such as blockchain technology and advanced encryption, to prevent data breaches.
- Stricter regulatory frameworks and industry standards are necessary to protect personal genetic data and hold companies accountable for breaches.
- There should be increased transparency and accountability regarding the use of customers' genetic data.
- Individuals should assert their rights over their genetic information, leading to new models of data ownership and consent.
- The incident calls for a future where the benefits of genetic testing are balanced with strong data security measures, privacy protection, and respect for individuals' autonomy.

Previous Post: **The Stripper Index: Decoding the Economic Signals of Sex Work**
Next Post: **Big Question Mark in the Stock Market**

LEAVE A REPLY