Q: The author questions if satisfying our curiosity through direct-to-consumer DNA testing is worth the risk of a permanent data breach. Do you believe the personal and medical benefits of DNA digitization outweigh the lifelong security risks?

A: The article presents a difficult ethical question: whether satisfying our curiosity through direct-to-consumer DNA testing is worth the risk of exposing our most personal information. While the author acknowledges that consumer DNA testing can advance medical research and potentially help discover treatments for fatal illnesses, she also emphasizes that DNA is the ultimate form of personally identifiable information (PII). Unlike a Social Security number or credit card, DNA cannot be replaced if it is stolen. I believe the medical benefits of DNA digitization are valuable, but if, and only if organizations collecting this data invest heavily in cybersecurity and provide transparency about how genetic information is stored, used, and protected. Otherwise, it is a ticking time bomb waiting to go off.

Q: Rizkallah raises the concern of where to "draw the line" regarding privacy, such as whether it is acceptable for an employer to request your DNA to see if your genetic makeup makes you a "fit" for a role. Discuss the potential for "genetic discrimination" in the workplace if these databases are accessed by unauthorized parties or used for purposes beyond their original intent.

Rizkallah raises an important concern about where society should "draw the line" regarding privacy. She questions whether employers should ever be allowed to request DNA information to determine whether someone is a good fit for a role. If genetic databases are breached or accessed beyond their intended purpose, employers could potentially discriminate against individuals based on inherited health risks or genetic traits. Such practices could unfairly limit opportunities and create a workplace environment where people are judged by factors beyond their control. The article suggests that strong privacy protections are necessary to prevent DNA data from being misused by organizations or criminals, to which I heavily agree.

Q: The text notes that humans remain the easiest "inroad" for hackers to break into corporate networks. How does the permanent nature of biological data change the way we should think about "human factor" security compared to traditional digital passwords?

The article also highlights that humans remain the easiest entry point for cyberattacks. However, the digitization of DNA changes the stakes because biological data is permanent. If a password is stolen, it can be changed. Yet if DNA is compromised, the exposure is lifelong and irreversible. This means organizations must treat genetic information as one of their most sensitive assets. Human-factor security should focus not only on preventing unauthorized access but also on protecting data that can never be recovered or replaced once it is exposed.