

# ‘There are no serious safeguards’: can 23andMe be trusted with our DNA?

Publication Date: 2024-02-17

Author: Alaina Demopoulos

Section: Technology

Tags: Data protection, Genetics, Hacking, US healthcare, Health, features

Article URL: <https://www.theguardian.com/technology/2024/feb/17/23andme-dna-data-security-finance>



What's next for 23andMe? Most people know the biotech company as a genetic testing service. Stories of people sending their cheek swabs off in the mail only to discover that a parent who raised them wasn't their biological one have become a kind of millennial horror genre. Of course, most 23andMe experiences aren't that dramatic: the company says more than 14 million people have used the service in hopes of learning more about their ancestry. But this month, 23andMe revealed it is facing major financial troubles, and more information came to light about a devastating security breach at the company last year. Now, customers might be wondering: can they trust 23andMe with their DNA? The DNA 'bait and switch' Last week, 23andMe reported dismal third-quarter fiscal results, tanking stocks in the company, CNBC reported. Its financial woes come down to a longevity problem: the company's most famous offering, the DNA ancestry test, is a one-and-done deal. After taking the test, there's no reason for consumers to keep spending money on 23andMe, which has led to a plateau of sorts. Nevertheless, the company's CEO, Anne Wojcicki, told Wired she remains "optimistic" about 23andMe's future. At-home DNA tests are so ubiquitous that you can order one for a dog. 23andMe was the first company to offer the (human) service, back in 2007, and now an estimated one in five Americans have tried at-home genetic testing. Some customers were handing over personal data that Wojcicki and company used for purposes other than inspiring family reunions. From 2018 to 2023, 23andMe partnered with the pharmaceutical giant GlaxoSmithKline, using customers' genetic information to help develop drug targets. (A drug target is a molecule that plays a role in a disease; researchers use them to develop therapies for certain diseases.) This year, the partnership became non-exclusive, which means 23andMe can strike deals with more pharmaceutical companies to milk more money out of its DNA trove. "It's a real resource that we could apply to a number of different organizations for their own drug discovery," Wojcicki said, adding that 23andMe was interested in studying inflammation immunology, particularly asthma. 23andMe already has two cancer drugs undergoing drug trials; those drugs came from users' genetic data. But 23andMe users may not understand that the spit they gave the company months or years ago is being used to make more money. As the health reporter Kristen V Brown wrote for Bloomberg in 2021: "It wouldn't be crazy for the 8.8 million 23andMe customers who once absently checked a box saying, yeah, sure, use my data for whatever, to feel like they've been bait-and-switched now that their genes are laying the groundwork for potential cancer cures." (Since 2021, the number of customers who have checked that box has risen to 10 million, according to Wired.) Customers can revoke consent Americans tend to believe that their health data is covered by Hipaa, the health privacy law – surely 23andMe, with its official-looking cheek swabs and far-off labs, must be, too. But 23andMe isn't a healthcare provider. The same rules do not apply. "There are no serious safeguards, no regulation around the collection and sale of really sensitive

personal data,” said Suzanne Bernstein, a law fellow at the Electronic Privacy Information Center. “For 23andMe, the nefarious [data] breach constitutes a security issue, but so does the company sharing your information with a party that you didn’t know about. Customers may technically consent to their data being shared by accepting the terms and conditions, but those are really long and a lot of people don’t read them.” Some people might find it honorable that their genes are being used for cancer research. Others might feel ripped off: they paid about \$229 for a DNA testing kit, but 23andMe is using their health data for free. Thorin Klosowski, a security and privacy activist at the Electronic Frontier Foundation, says 23andMe could do more to ensure that customers better understand this dynamic before they opt in. “The amount of people who are surprised by how much data goes elsewhere is a sign that 23andMe isn’t explaining things very clearly,” he said. Klosowski added that while users can opt out of their data being used by 23andMe long after they’ve sent away their DNA swab, their information may have already been used for research purposes. “You can ask 23andMe to stop using your information, but you can’t ask for data to be removed from a list once it’s been sold off,” he said. For its part, 23andMe maintains that users are asked to opt in to research at point of purchase, and all personal data is stripped of identifying information before it’s shipped off for analysis. Data isn’t used without this consent, and consent can be revoked. The company’s research wing is also overseen by an “independent, impartial” review board. (23andMe did not respond to a request for comment.) Data breach leads to class-action suit 23andMe’s security breach is still at the forefront of many customers’ minds, too. Last year, nearly 7m customer profiles were hacked. Over the course of five months, hackers were able to access health records, including carrier-status reports, as well as personal information from up to 5.5 million people who opted in to one of 23andMe’s best-known features: the chance to find relatives. Customers with Chinese and Ashkenazi Jewish heritage appeared to have been targeted in the breach and their information sold on the dark web, the New York Times reported. Some of those users recently filed a class-action suit against the company, saying 23andMe had failed to notify them about the exposure. As the Guardian reported on Thursday, 23andMe downplayed its responsibility for the hack in a letter to customers, arguing the health information accessed “cannot be used for any harm”. It also blamed customers who “negligently recycled and failed to update their passwords” – a response that one former customer criticized as “morally and politically very dumb”. Wojcicki didn’t speak directly about the leak due to pending litigation, but she told Wired that 23andMe had introduced two-factor authentication and made customers reset their passwords. “Data privacy and security has always been a really high priority and remains a high priority for the company and something that we are going to invest even more into,” she said. Are 23andMe’s security issues the death knell for a company that Time once hailed as the “invention of the year”? Whether or not customers’ privacy concerns are well-founded, the company’s financial fall has been swift, and CNN reports it could be delisted from Nasdaq if its stock price doesn’t go up. Dominic Sellitto, a clinical assistant professor at the University at Buffalo School of Management who focuses on digital privacy, believes that if 23andMe survives the year, it will be due to data mining. “There’s a lot of demand and money for data, especially quality healthcare data,” he said. “If 23andMe continues to monetize that, it will be their golden ticket in 2024.”