

Write Up: Hacking Humans

Nicholas Duggins

06/14/2026

Write Up: Hacking Humans

The digitization of DNA creates a real conflict between the benefits of science and the risks to privacy. On one hand, direct-to-consumer DNA testing and genetic databases can actually be really useful. They help people learn about their ancestry, improve medical research, and even assist in solving cold cases. That's a major advancement and shows how valuable genetic data can be when it's used the right way. But at the same time, I don't think those benefits fully outweigh the risks of a permanent data breach. Unlike passwords or credit cards, DNA can't be changed or replaced once it's exposed, which makes the consequences long-term and potentially irreversible.

There are also serious concerns when it comes to corporate and employment privacy. If employers were ever able to access DNA information, it could easily lead to genetic discrimination. People could be judged or excluded based on health risks or traits they may never even develop or experience. Even if companies collect this data for legitimate reasons like research or healthcare programs, there's still the risk that it could be reused, shared, or exposed over time because of policy changes, mergers, or security breaches.

That's why I think there needs to be very clear limits on who can access genetic data and what it can be used for. These protections shouldn't just be general guidelines, but actual strict laws and enforceable policies that prevent companies from expanding the use of DNA data beyond what users originally agreed to. There should also be transparency about how long data is stored, whether it is shared with third parties, and what happens if a company is sold or merged with another organization. Without those kinds of safeguards, people basically lose control over some of the most personal information they have, often without even realizing it. Strong consent rules and the ability to opt out or delete data should also be a required part of any system that collects genetic information.

The idea of "hacking humans" really changes how I think about cybersecurity. Normally, the weakest link is human error like weak passwords or phishing, but with DNA, the problem is much bigger

because the data itself is permanent. A password can be reset, but DNA can't. That shifts the focus more toward prevention than recovery, and it shows why genetic data needs to be treated as highly sensitive from the start with strong encryption, strict access control, and tight regulations on how it's stored and shared.