Analysis on Hacking Humans and the Threat of DNA Cybercrime

Harold Vernon

Old Dominion University

CYSE495_27976

Professor Charles Kirkpatrick

April 2, 2026

As the tools used for authentication evolve, DNA matching may be required in many cases to prove that a given person has authorized access to data or a location. Since DNA is stored as data by several organizations, it can be stolen by malicious people used for a variety of crimes. It can also be held by a threat actor as a permanent way to impersonate a victim. Both these threats are unique due to the fact that a person's DNA is uniquely theirs and cannot be changed. For this reason, cybersecurity professionals must take particular precautions when guarding data related to DNA.

The impact of DNA data being compromised is less immediately noticeable than something such as a password or credit card number but can arguably be far more devastating due to the permanence of DNA in comparison to several other forms of personally identifiable information. Since DNA is unique to a person and inseparable from them, it is a permanent form of personally identifiable information. This means that the impact on privacy is perhaps more severe than other PII being compromised because once it is acquired, it is perpetually valid.

The digitization of DNA means that it is immediately exposed to privacy risks. This is because there are no ways to specially protect a DNA database more than any other database. Therefore the protections that a given organization uses for their regular data such as customer information are also being used for stored DNA. This means that if the DNA database is compromised, threat actors could use the data stored therein to reconstruct a victim's DNA for their own ends (University of Portsmouth, 2025.)

Avoiding digitization, however, adds a significant degree of security to DNA. This is because by not storing the DNA on a computer, the entire metaphorical game changes. With the DNA not digitized, a threat actor has to either convince their victim to give up their DNA by finding a victim interested in a DNA analysis service and then rerouting or intercepting the

delivery, or they have to carry out some sort of physical theft operation of either hair or of DNA stored by a company. Unless the person has already given their DNA up, however, it is useless in all of these cases because it has not been tracked back to them yet. This means that a great way to ensure DNA is a non-factor regarding privacy is to simply make sure it is never digitized and tied to an individual.

There are numerous ways criminals can use a person's DNA against them. The most direct way is by simply selling the DNA on the black market to less than reputable data collectors. These collectors can then, assuming the DNA has not already been analyzed, run their own analyses on stolen DNA data to figure out the specific conditions that a person might be prone to and then send this data to advertisers. Additionally, this DNA data is oftentimes packaged with conclusions drawn by the organization that was storing it that can impact other behaviors besides medicine. This makes DNA a highly lucrative asset for advertisers to possess in order to better personalize advertisements and increase the chances of someone buying a given product.

The threat of DNA data by itself being used to frame an individual for a crime is largely overstated. This is because the DNA would have to be not just in the form of data but somehow planted at the scene of a crime in order to frame the victim. Not to mention the sheer expense involved in such an action. This threat has been even further relegated to yesterday's science fiction by the fact that, if a criminal is interested in framing someone for a crime, they could use generative artificial intelligence tools to create fake imagery or even videos to incriminate that person. The watermarks attached to the images and videos created by AI tools such as Gemini and Sora could be easily filed off through basic photo or video editing software. Overall this is a

much more practical approach to false evidence than the DNA which was a widespread fear when services mapping client's genomes first became widespread in the 2010s.

Not even the use of DNA to fake access is necessarily a problem in and of itself. This is because, like with the problem of planting evidence, faking access requires physical access to a given site. This means that the DNA alone is not sufficient and must come oftentimes in the form of saliva in the rare instances where DNA is used to verify that a person is authorized to access a given location or artifact. Until a way to reproduce DNA in saliva is found, this remains a non-threat. This is compounded by the fact that DNA is generally a highly rare authentication method.

DNA cybercrimes generally fall under the theft of DNA stored as digitized data. This can involve either directly hacking the networks that companies such as 23andMe use which contain the databases where customers' data is stored or employing social engineering tactics to gain access to customer DNA without potentially tripping cybersecurity systems through an attempted hack. As is the case in most of cybersecurity, social engineering remains the ultimate priority threat in terms of allowing unauthorized access because a successful social engineer could convince the right people to lower whatever defenses may have been erected. Stolen DNA can be used for a variety of things such as being sold to advertisers to analyze and find not only what products a person might need based on their DNA records' vulnerabilities to specific diseases, but also how exactly to advertise them if an advertiser takes a more advanced approach by analyzing DNA to figure out a decent portion of a given person's personality.

The utility of DNA to criminals mostly applies only if the DNA has been matched to a person. Without this match, the DNA is largely useless. If this match has been made, then efforts must be taken to ensure that DNA data is not access by criminals. This can be done by destroying

the DNA sample itself and deleting the data once the requested service is complete. Though this still leaves a window of time for criminals to access DNA data they wish to steal.

To conclude, the main cybercrime threat regarding DNA is the theft of information and how it can be used for intrusive personalization of advertisements. The threat of using DNA to frame a person for a crime has been mitigated by the much greater convenience of generative AI tools for this purpose while the threat of using DNA to feign authorization is mitigated by the rarity of DNA-based authentication methods and the fact that with these methods, the DNA data itself is never enough to gain access. To protect against the very real threat of intrusive advertising using people's DNA data, the best course of action would be to adopt a blanket policy of destroying DNA samples and wiping databases containing the sequences themselves once the requested service has been completed.

References:

University of Portsmouth. "Our DNA is at risk of hacking, warn scientists." ScienceDaily. ScienceDaily, 16 April 2025. <www.sciencedaily.com/releases/2025/04/250416135745.htm>.