MEDIA FIELDS
JOURNAL

"Your Personal Information is Being Requested"
Ancestry Testing, Stunt Coding, and Synthetic DNA

Simone Browne

In July 2015, an app posted to the repository hosting service GitHub claimed to use genetic data culled from the ancestry testing company 23andMe to potentially limit a user's access to particular segments of the Internet. Called Genetic Access Control, this app utilized the "open" nature of 23andMe's application programming interface (API) to generate a third-party authentication application that the developer promised could restrict access to certain websites "based on traits including sex, ancestry, disease susceptability [*sic*], and arbitrary characteristics associated with single-nucleotide polymorphisms (SNPs) in a person's genotype."[1]This app would enable websites to request access to a user's 23andMe profile for verification purposes upon login. (See Figure 1). Once permission to share the data with this third-party app was approved, the app would then allow or disallow the user access to the site. Or, as the app developer put it in a list of possible uses, the app could create "'safe spaces' online where frequently attacked and trolled victim groups can congregate, such as a female-only community" and "[g]roups defined by ethnic background, e.g. Black Panthers or NAACP members."[2] Posted to GitHub under the username "offensive-computing," this anonymous developer also suggested that "[e]thnoreligious sects" that "wish to limit membership, e.g. Hasidic Jewish groups restricting access to Ashkenazi or Sephardic maternal haplogroups with the 'Cohen' gene" might employ the application.[3] Within days of Genetic Access Control's appearance on GitHub, 23andMe restricted the app's access to its APIs. It cited non-

compliance with 23andMe's Terms of Service agreement, which forbids the use of its APIs in applications that promote "hate materials."[4]

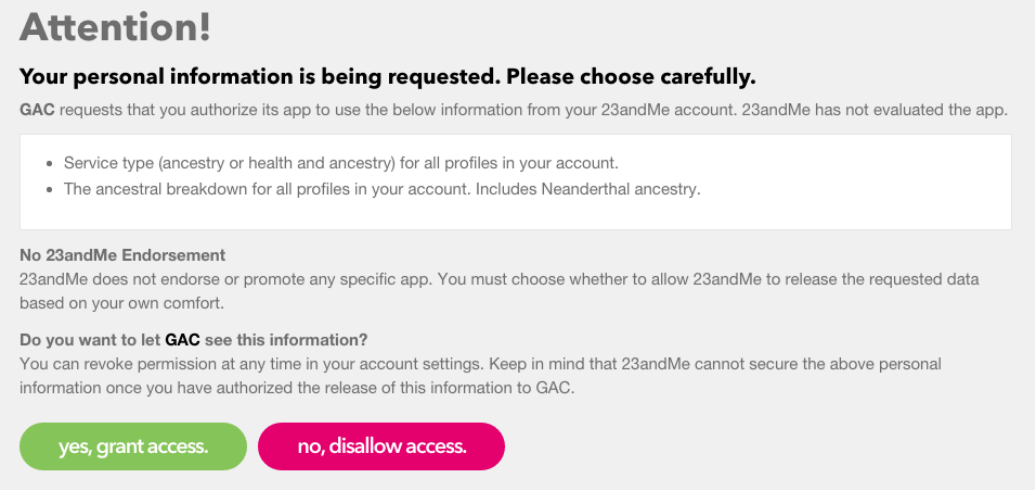

Figure 1. Screen shot from Genetic Access Control's GitHub repository

Although Genetic Access Control's anonymous developer noted on GitHub that "traits such as ancestry composition are speculative and statistical in nature, not precise,"[5] this application reveals the fault lines that become apparent when genetic technologies make use of DNA to reveal certain truths about the human body and the limits of making such sensitive data available to any interested parties. Such putative truths often hinge on a reification of fixed biological notions of race and other markers of identification and social location. Perhaps this was GitHub user offensive-computing's point. The developer's app may be an act of trolling 23andMe's Privacy Statement's section on consumer choice, drawing attention to the sharing of personal genetic data and consent despite the ancestry testing company's statement that it "will have no responsibility or liability for any consequences that may result because you have released or shared personal information with others."[6] Offensive-computing's user name could also imply both senses of the homonym "offensive"—meaning both "insulting" and "attacking"—and might betray a tongue-in-cheek play on the type of discriminatory surveillance practices that such an app enables.[7] Put another way, what would it mean for the hashtag #BlackLivesMatter if Twitter required a 23andMe profile for login authentication and denied access to users with less than the permitted European ancestry? (See Figure 2.)

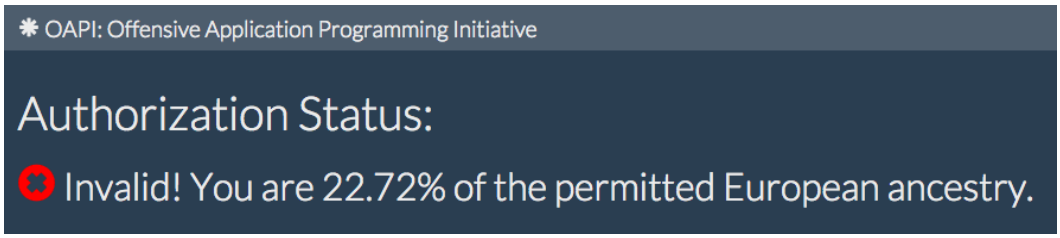

Figure 2. Screen shot of an invalid authorization status on Genetic Access Control.

23andMe began in direct-to-consumer personal genomics by issuing health reports that itemized a user's disease risk. However, at the behest of the US Food and Drug Administration, it ceased disease risk testing due to regulatory restrictions in 2013. Inciting the consumer to "bring your ancestry to life with DNA," 23andMe provides its paying users the choice to share their genetic personal data and any intellectual property derived from such data to non-profit and commercial organizations. This information is used for research purposes, including the formation of "disease communities" "to understand, through genetics, why people respond differently to disease treatment options and drugs."[8] Such personal genetic file-sharing is part of an increasingly interconnected system of knowledge about the human body collected in databases and used to track habits and movements, to profile, and to accumulate information for commercial applications. For example, Procter & Gamble's Olay brand partnered with 23andMe in a multi-decade and multi-ethnicity focused study that sought to understand the role of ethnic ancestry in women's skin aging. The researchers isolated a "unique skin fingerprint" among what they termed "exceptional skin agers" to see if, indeed, black don't crack and to "determine what's possible when it comes to cosmetic skin care and looking ageless."[9]

Regarding the possible "flaws" of the Genetic Access Control app, offensive-computing states that users could falsify their profiles by obtaining "a genetic testing kit for about $100 and submit[ting] a saliva sample from a person who would normally fit the criteria for granting access."[10] The developer also lists, but does not explain, what he or she terms the "unresolved ethical issues regarding trans-*-identifying persons such as transgender and transethnic users."[11] Another potential flaw is the issue of authentication that arises with the introduction of artificial DNA. This flaw is the topic of a 2010 study in which researchers questioned what will happen when current forensic procedures like molecular cloning or whole genome amplification cannot distinguish artificial or synthesized DNA from a genuine DNA profile that is derived from natural biological material.[12] Such an instance would

necessitate procedures that can authenticate genuine DNA. That same year, researchers at Nucleix, Ltd. patented a process that they said could differentiate between artificial and natural DNA. Their technology reportedly distinguishes between *in-vivo*-generated DNA (culled from natural biological material) and *in-vitro*-generated DNA (manufactured in a controlled setting). These researchers used volunteers' biological samples sourced from blood, saliva, skin scrapings, and used cigarette butts (elements that one might plant at a crime scene to set someone up for the fall) and blood from a consenting donor. Using a process of centrifugation, the donor blood was then "washed," or separated into DNA-containing white blood cells and DNA-free red blood cells. Following this, the researchers applied a process of whole genome amplification to expand the DNA of the person they wanted to frame from say, traces of saliva found on a coffee cup into a larger sample size and inserted this amplified DNA into the donor's DNA-free red blood cells. Ultimately, this procedure results in blood that is a genetic profile match—although fabricated—of the framed individual, not the donor. To discern between fabricated and authentic DNA, forensic scientists will look for a differentiation in methylation patterns. A lack of methylation signifies a fabricated or synthesized DNA; *in vitro*/synthesized DNA is completely unmethylated, while *in vivo* DNA is completely methylated.[13] Synthesizing DNA could provide another fault line for a third-party authentication app like Genetic Access Control, as biometric technology is put to use for other identification purposes.

I'm far from a geneticist. I first learned about Nucleix, Ltd. through an episode of the police procedural drama *Law and Order: Special Victims Unit* that aired in 2009.[14] I raise Nucleix, Ltd.'s DNA Authentication Assay[15] here to think of it alongside the open-source Genetic Access Control App. Notably, both technologies leave us with important questions to contemplate regarding consent, the regulation of data generated from biological matter and markers, and what could happen when such data is deployed for the purposes of surveillance. Ancestry testing and police databases situated in disproportionately policed and disproportionately represented communities present us with spaces for questioning the expanded uses, or "surveillance creep," of databasing DNA.[16]

Notes

1 Offensive-computing, "Genetic Access Control," *Github*, July 20, 2015, https://github.com/offapi/rbac-23andme-oauth2.
2 Ibid.
3 Ibid.
4 Stephanie M. Lee, "Your 23andMe DNA Can Be Used In Racist, Discriminatory Ways," *Buzzfeed*, July 22, 2015, http://www.buzzfeed.com/stephaniemlee/your-23andme-dna-can-be-used-in-racist-discriminatory-ways#.us9lAP3ENE.
5 Offensive-computing, "Genetic Access Control."
6 "Full Privacy Statement," *23andMe*, Dec. 7, 2015, https://www.23andme.com/about/privacy/#Full.
7 In an interview with *Motherboard*, "stunt coder" offensive-computing stated that posting the Genetic Access Control app on GitHub was part of the "Offensive Application Program Initiative," which is "an organization where people can contribute artistic and functional open source code that sparks debate about the ethical implications of software that hurts people's feelings." Here, third-party authentication software that could deny users access due to their race, gender, or ethnicity is understood as causing hurt feelings rather than representing the outcome of institutional, political, social, and technological practices and policies. Jordan Pearson, "Racial Segregation for Websites is "Very Easy," Stunt Coder Says," *Motherboard*, July 24, 2015, http://motherboard.vice.com/read/racial-segregation-for-websites-is-very-easy-stunt-coder-says.
8 "Research," *23andMe*, https://www.23andme.com/en-int/research/.
9 "Olay Discovers Unique Skin Fingerprint Among Those Who Look Exceptionally Younger Than Their Actual Age," *Olay*, June 9, 2015, http://www.olay.com/en-us/skin-care-tips-and-articles/olay-discovers-unique-skin-fingerprint.
10 Offensive-computing, "Genetic Access Control."
11 Ibid.
12 Dan Frumkin, Adam Wasserstrom, Ariane Davidson, and Arnon Grafit, "Authentication of Forensic DNA Samples," *Forensic Science International: Genetics* 4 no. 2 (2009): 95-103.
13 Ibid., 4.
14 "Perverted," *Law and Order: Special Victims Unit*, NBC, (New York: Nov. 18, 2009).
15 Adam Wasserstrom and Dan Frumkin, "Methods for distinguishing between natural and artificial DNA samples," US Patent 20120190023, filed July 1, 2010 and issued July 26, 2012, http://patents.justia.com/patent/20120190023.
16 Jacques Ellul's term "surveillance creep," which builds on Langdon Winner's concept of "function creep," is discussed in David Lyon, *Surveillance Studies: An Overview* (Cambridge, UK and Malden, MA: Polity Press, 2007), 52.