



Perspective

Sociogenetic Risks — Ancestry DNA Testing, Third-Party Identity, and Protection of Privacy

Thomas May, Ph.D.

The recent capture of the suspected Golden State Killer on “National DNA Day” was a startling public illustration of the reality that DNA information may be pertinent to people far

removed from the one who was tested — and the fact that information may derive from testing that an implicated person is not even aware has taken place. The suspect did not submit his own DNA sample for testing; his identity was inferred by tracing the family tree of the person whose DNA was found at crime scenes. Such use of DNA testing plays into public fears about the use of genetic information, particularly the fear of having conclusions drawn about oneself from tests performed on (sometimes distant) relatives.¹ DNA testing has tremendous potential as a public health tool, but realization of its benefits will require continued cognizance of its potential for misuse.

Although we might all like to

allow DNA testing to be used to catch criminals like the Golden State Killer, such testing unavoidably comes with a loss of privacy, and competing interests must be considered. The 2008 Genetic Information Nondiscrimination Act (GINA) addressed the need to regulate how genetic information is used, most notably protecting against discrimination in health insurance and employment. But GINA has serious limitations, including its lack of application to life insurance and long-term care insurance and to employers of fewer than 15 employees. In addition, GINA places the burden on victims of genetic discrimination to prove that their information was misused — which is as plausible an explanation for the dearth of

successful GINA cases as the possibility that the law has effectively discouraged such discrimination. This flawed mechanism, though well-intentioned, is hardly adequate to balance complex competing interests that might arise in DNA testing.

For years, adoptees have faced similar issues of privacy versus the utility of genetic information. For example, many states have been slow to open access to birth certificates, justifying this reluctance on the grounds of privacy protection; they may fear unintended consequences such as scandals, threats to immediate and extended birth-family relationships, and the possibility that women will simply choose abortion over adoption rather than risk such consequences. Although some people seek DNA testing to discover their geographic ancestry (which poses less risk to privacy), many seek to be “matched” to specific related people. In the latter context, one

company recently launched DNA Quest, an initiative offering pro bono services to adoptees to find birth relatives through DNA testing. The laudable ideal behind this effort is that adoptees have a right to access their basic birth records and heritage information. Yet there are myriad reasons why birth parents may not wish to have their identity revealed; our approach to assisting adoptees will have to grant birth parents' desires due respect and carefully address the psychosocial ramifications of revealing their identities.

Given these complexities, it's important to reach societal consensus on regulation of the way in which test results are returned, to whom, and for what purposes. For example, do genetic-testing organizations have a duty to verify the ownership of genetic samples? Our current regulatory approach to privacy in direct-to-consumer (DTC) genealogic testing has permitted the creation of a Wild West environment, in which companies send vials to consumers, who return DNA samples by mail. Reporters have shown how easy it is to send someone else's sample for testing and receive a full report on that person. The Golden State Killer case confirms this ease. Although Ancestry.com issued a statement immediately after the killer's arrest claiming that it "advocates for its members' privacy and will not share any information with law enforcement unless compelled to by valid legal process," willing cooperation from a testing company was probably not necessary. Apparently, the police simply sent the Golden State Killer's genetic data to GEDmatch and had it matched to relatives, then followed the family tree to the person who was eventually arrested.

In the health care context, we would not be so lax about a sample's chain of custody, nor return test results without following clear procedures for establishing who has a right to such information. Under the Health Insurance Portability and Accountability Act (HIPAA) and the Common Rule that guides human-subjects research, for example, laboratories are expected to adhere to strict guidelines to protect health-related information. Although genealogic testing is not health care, it was derived from health technologies and presents privacy risks similar to those associated with health-related genetic testing.

Failure to address concerns about misuse of genetic information will have important ramifications, not only in terms of unwanted intrusion into the lives of people who wish to remain anonymous, but for the continued advancement of genomic medicine. Even concerns about third-party privacy are not exclusive to ancestry testing. The U.S. Precision Medicine Initiative therefore explicitly recognizes the importance of trust and privacy for advancing large-scale population studies like "All of Us."^{2,3} Disincentives to participate will probably be exacerbated in minority populations with a history of being treated oppressively by law enforcement, who may hesitate to have their DNA included in databases or to participate in genomic research. And differential participation will threaten our ability to address widely recognized deficiencies in reference genomes and will limit the advancement of genetic science.

Requiring HIPAA-style verification and privacy protection would cripple the DTC testing industry, but some level of protection should be possible. We have mechanisms

that allow victims of identity theft, for example, to demand that banks require verification of identity from credit applicants using their name. Although there is no way to guarantee privacy, surely there are ways to mitigate risk. After all, questions about how to handle genetic information that the person who is the source of the DNA has not agreed to have investigated are familiar to the clinical genetics community. The relevance of information about an inherited disease — such as a positive *BRCA* result — for the tested person's relatives (from whom she may be estranged) and results from diagnostic parent-child triad testing that indicate misattributed paternity are two familiar examples.

The complexity of these issues is apparent from the countless pages of scientific literature devoted to secondary and incidental findings in genomic medicine, which led the American College of Medical Genetics and Genomics (ACMG) to recommend mandatory reporting of 56 (now 59) "actionable" findings; significant criticism of the recommendations motivated their rapid modification. Whereas the ACMG authors had expected objections to center on the specific actionable findings, critics instead focused on the investigation of variants that were not addressed in the consent procedure. The modifications centered on the addition of an "opt out," allowing patients to prohibit investigation of these secondary results.⁴ Notably, proponents of mandatory reporting in the original ACMG recommendations argued that requiring consent or allowing an opt-out would add such logistical complications as to effectively cripple laboratories; thus far, these concerns seem to have been unwarranted.

This approach seems to be working in the adoption community, as states have begun opening up access to birth records. Of the 29 states that now allow adoptees some access to their birth records, the majority do so with restrictions.⁵ Many states let birth parents choose whether to allow contact; for example, in Alabama, they can complete a preference form to allow direct contact, contact only through an intermediary, or no contact at all.

Whatever implementable mechanisms are identified, regulatory oversight is needed to ensure the privacy of genetic information, determine who should be allowed to submit someone else's sample

for testing and for what purposes, and guide the drawing of inferences from DNA results and the relaying of information to persons other than the DNA source who may be implicated by those results — but may be unaware that testing relevant to them has even occurred.

Disclosure forms provided by the author are available at NEJM.org.

From the Elson S. Floyd College of Medicine, Washington State University, Vancouver; and the Ethics and Genomics Program, HudsonAlpha Institute for Biotechnology, Huntsville, AL.

This article was published on June 20, 2018, at NEJM.org.

1. Seife C. 23andMe is terrifying, but not for the reasons the FDA thinks. *Scientific American*. November 27, 2013 (<https://www>

[.scientificamerican.com/article/23andme-is-terrifying-but-not-for-the-reasons-the-fda-thinks/](https://www.scientificamerican.com/article/23andme-is-terrifying-but-not-for-the-reasons-the-fda-thinks/)).

2. Precision Medicine Initiative: statement of privacy and trust principles. Washington, DC: The White House, November 9, 2015 (<https://allofus.nih.gov/sites/default/files/privacy-trust-principles.pdf>).

3. Precision Medicine Initiative: data security policy and principles framework. Washington, DC: The White House, May 26, 2016 (<https://allofus.nih.gov/about/program-overview/precision-medicine-initiative-data-security-policy-principles-and-framework-overview>).

4. May T. On the justifiability of ACMG recommendations for reporting of incidental findings in clinical exome and genome sequencing. *J Law Med Ethics* 2015;43:134-42.

5. State adoption legislation. Washington, DC: American Adoption Congress, 2018 (<https://www.americanadoptioncongress.org/state.php>).

DOI: 10.1056/NEJMp1805870

Copyright © 2018 Massachusetts Medical Society.