

FROM GDPR TO GOLDEN STATE KILLER, DNA SHARING PRESENTS PRIVACY CHALLENGES

Collaborations between popular consumer genetic testing companies like 23andMe and pharmaceutical giants like GlaxoSmithKline to develop new drugs raise data privacy concerns for in-house lawyers, who must navigate this murky compliance landscape largely through privacy policies.

BY KRISTEN RASMUSSEN

Seeking insight into ancestral backgrounds or clues into various health risks have led millions to direct-to-consumer genetic tests.

The market for such private genetic testing is expected to grow to \$310 million by 2022, up from \$99 million in 2017, according to researcher Kalorama Information.

For the individual consumers, that means that for anywhere from less than \$50 to more than \$200, they can swap their saliva for information ranging from fun—their food preferences, for example—to sober, including whether they have a genetic variation associated with a higher risk of a number of incurable diseases.

But the profit in the consumer genetic health testing market doesn't come from the consumers alone but also from the wider trend of data monetization. For example, 23andMe Inc., one of the leading consumer DNA test companies, announced last July that it would supply drug company GlaxoSmithKline with its genetic research for four years to help develop new medicine. For its

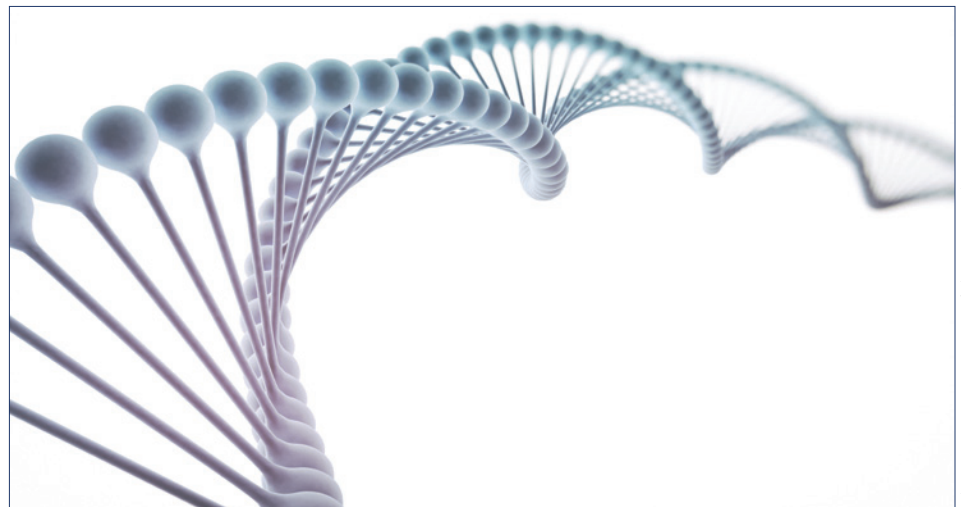


Photo courtesy: Jezper/Shutterstock.com

part, GSK made a \$300 million equity investment in the genetic testing company, and the two businesses will split costs and profits from the development of new drugs and treatments equally.

The Mountain View, California-based startup previously announced a similar deal with pharmaceutical giant Pfizer Inc.

Such collaborations, however, raise serious concerns about the privacy implications of providing big pharma with one's most sensitive personal information. And to

make matters complicated, the industry operates in a space where the law hasn't wholly caught up with the technology yet, leaving in-house attorneys to navigate a murky compliance landscape.

The Gray Area in U.S. Law

Days after 23andMe announced its collaboration with GSK, a number of private genetic testing companies, including 23andMe, collectively issued privacy guidelines for the private sector management of genetic information.

Essentially a set of best practices, the guidelines incorporate many of the protections codified in 23andMe's privacy statement, terms of service and other documents. They encourage greater transparency over how genetic data are used by genetic testing companies and recommend companies obtain express consumer consent before processing or sharing personal genetic information.

According to its privacy statement, 23andMe complies with the European Union's General Data Protection Regulation, the expansive law that went into effect last May and imposes new rules on any entity that offers goods and services to people in the European Union or that collects, processes or stores data tied to EU citizens.

Article 9 of the GDPR classifies genetic data such as DNA as "special category data" that require a heightened level of protection, said **Stephen Breidenbach**, an associate at Long Island, New York-based **Moritt Hock & Hamroff** and former cybersecurity professional.

Companies are prohibited from collecting these data, unless "explicit consent" that is both informed and specific has been obtained.

"When you get consent, you have to inform, and failure to do so can void the consent," **Breidenbach** said.

Added Leeza Garber, adjunct professor at Drexel University Thomas R. Kline School of Law specializing in privacy and cybersecurity: "The GDPR helps up the ante for privacy law in general so hopefully that heightened standard is leading to heightened awareness, especially around this type of information, and hopefully the U.S. will follow."

Beyond the GDPR, however, the relevant privacy law for genetic testing companies remains "a patchwork," Garber said.

That is, despite a number of federal and local laws regulating genetic information in the United States, there are few laws directly regulating what private companies can or can't do with the genetic data they collect.

The Health Insurance Portability and Accountability Act of 1996, for example, has provisions that govern the permissible uses and disclosure of genetic data in certain cases. However, HIPAA would not apply to businesses such as 23andMe, said Linn Freedman, a partner who practices data privacy and security law, cybersecurity and complex litigation at Robinson & Cole.

"23andMe, as a commercial entity, is getting this information directly from consumers in a consumer setting, not a health care setting, who are voluntarily providing this information," she said.

Also on the federal level is the Genetic Information Nondiscrimination Act, or GINA, but it prohibits discrimination in the employment and health insurance contexts. Many of those provisions, however, are echoed in numerous state laws, which also either require a person's consent before his or her genetic data are disclosed or retained, or require consent before genetic information is disclosed, but do not require consent for retention.

"A lot of privacy laws are still operating on the state level," Garber said. "The states are really advancing the ball, but federal law has to step up to the plate."

Garber predicts that much of that guidance will come from the Federal Trade Commission, which she said is "taking a pivotal role" in the debate.

U.S. Senate Minority Leader Chuck Schumer, D-New York, in November 2017 advised the agency to take a closer look at the privacy policies of private companies that sell genetic tests to "ensure that these companies have clear, fair privacy policies and standards for all kinds of at-home DNA test kits."

To date, though, the FTC has not publicly opened any investigation into any private company offering genetic testing, though it has advised consumers to be aware of the privacy implications of purchasing genetic testing kits.

"As strong as the FTC is, there's still not this high-standing federal law that's tested and proven to address these privacy problems," Garber said. "And you can't bake privacy back in. Once it's out there, it's out there. It's hard to put these measures back in."

A Reliance on Privacy Policies

At least in the case of 23andMe, many of these privacy concerns are seemingly addressed in the company's comprehensive privacy policy, but as legal experts pointed out, few consumers likely read its 9,000 words.

Representatives from 23andMe did not respond to Corporate Counsel's email and phone requests for comment from in-house lawyers about what measures the company takes to ensure that genetic data shared with other companies are protected.

Brennan Torregrossa, senior vice president and head of global

litigation at London-based GSK, said via email that in-house lawyers there declined to discuss the matter. A spokeswoman from Pfizer, which entered into a similar collaboration with 23andMe in 2015, said that in-house attorneys there were unavailable for comment.

Under 23andMe's policy, customers can voluntarily allow or restrict their genetic information from being shared with "other third parties, such as non-profit foundations, academic institutions or pharmaceutical companies." And if they do opt to share it with GSK, the policy also makes clear that consent to this use is required and that the information is de-identified and summarized across many users.

The policy is in line with two issues that the public and regulatory entities are most concerned about—appropriate consent and data de-identification, said Kate Black, 23andMe's former global privacy officer and senior counsel and now a partner at Greenberg Traurig's San Francisco office.

Other issues, she added, include the government's access to information for crime-solving purposes, an issue that raised public outcry after police in California used an open-source genetic database to find, through a familial DNA search, the notorious man who had become known as the "Golden State killer."

"Each company should be making proactive decisions about their

company's approach to sharing data with government agencies," Black said, adding that consumers' other significant concerns are the company's other uses for and sharing of the data and their ability to control and delete the information.

"As a baseline, your privacy policy should lay out all the specific uses of any information about a consumer that you collect and make clear that if you'd like to use it for something that is outside of what is anticipated, you must notify the consumer and get specific consent," she said.

"Companies have to have clear policies in place for those issues that are most relevant to their specific customers."

In addition, although the information held by genetic testing companies like 23andMe is highly unique from consumer data held by other businesses, the mechanisms for protecting the information—identification encryption, access limitations, specific uses and holistic training—are the same, Black said.

Once those procedures are in place, she added, "you train to them, enforce them and uphold those standards throughout the company at every level."

Data privacy legal experts said in terms of transparency 23andMe has one of the better privacy policies, though, as Robinson & Cole's Freedman said, "the devil is always in the details."

For example, the issue of consent, or lack thereof, of consum-

ers' blood relatives, whose privacy—as the "Golden State killer" case strongly demonstrates—is also implicated, is not addressed, she said. In addition, although the privacy policy publicly states that 23andMe will not provide an insurance company or employer with genetic or non-genetic data, it also makes clear that

"Personal Information may be subject to processing pursuant to laws, regulations, judicial or other government subpoenas, warrants, or orders."

"They say if they are legally compelled, they may disclose that information," Freedman said. "What happens when a subpoena comes in?"

At this point, she said, the question of what private companies can or can't do with the genetic data they collect remains one of philosophy and policy rather than law.

"Unless there is some security incident, there is not a whole lot to enforce right now," Freedman said. "I'm not sure consumers actually understand [23andMe's privacy policy], but they are actually quite transparent in what they're doing with the data, and their entire business model is to protect it, so from a legal perspective, I don't see anything to enforce here."

Kristen Rasmussen is an Atlanta-based reporter who covers corporate legal departments and in-house attorneys, Georgia government and health care.