Canada August 15, 2016 7:00 am Updated: August 15, 2016 7:29 am

Privacy risks lurk in DNA tests, experts warn

By Patrick Cain

National Online Journalist, News Global News

A storage robot deposits samples in a blood and urine sample freezer at Biobank, near Manchester, northern England.

REUTERS

Where did my ancestors come from? What can my genes tell me about lurking health dangers? Is this child really mine?

Curiosity drives these questions, and some can be answered by sending a cheek swab away in the mail.

But others are curious about the complex, highly personal information about you coded in your DNA: drug companies, insurers, sometimes police.

And once you put your cheek swab in the mail, you risk permanently losing control over a complete copy of your genetic data, linked to your real identity.

Related

-  **Should insurers see the secrets locked in your genes?**
- **Liberal MP Rob Oliphant announces bill to prevent genetic discrimination**
-  **Internet of Things our 'biggest threat to privacy,' expert warns**

"I think you have to assume that you're going to lose control over that information," warns Ann Cavoukian, a former Ontario privacy commissioner who runs the Privacy and Big Data Institute at Ryerson University.

"Assuming that this information could be in the hands of many individuals, over which you have no control, are you comfortable with that? It will extend beyond just ancestry information — your full genetic code is there through that test, so perhaps other information can be gleaned, over which you have no control in terms of who has access to it."

READ MORE: Our digital privacy coverage

Whatever the privacy policies of any given company may say, you have no way of knowing whether they're being adhered to or what may happen to your sample as companies are bought and sold in the future, explains Trinity College Dublin legal scholar Andelka Phillips

"It is a commercial service," she says. "It's not really the same as entering into an academic research project, where the argument for altruism is much stronger. Sequenced genetic data has value to the companies."

> "It's not necessarily in our interests to have companies in control of that much data without any oversight."

WATCH: It was an unprecedented step taken by Manitoba RCMP in the hopes of catching a killer. A move police say could be used again in the future. Global's Brittany Greenslade looked into the ethics of this tactic.

Kate Black is chief privacy officer of **23andMe**, a genetic testing company that gives customers information about their health and ancestry. She points to the company's safeguards of customers' genetic information. But at the end of the day, she acknowledges, it's a trust relationship:

> "It's up to each individual to decide whether participating in our service is something that they're comfortable doing, and is the right fit for them or not."

Closing a 23andMe account doesn't necessarily mean the company's copy of your genetic data will disappear:

"We allow customers to close their accounts. It's a bit complicated by our regulatory compliance for laboratories in the United States, which requires that raw information be held for a minimum of 10 years. The information will be de-identified, but will continue to be stored for that set amount of time."

DNA is crammed with information.

Your genetic data can show your odds of getting diseases, like the **BRCA1** genetic mutation that can mean a much higher risk of breast and ovarian cancer. Some diseases, like Huntington's disease, are genetic, and susceptibility can be read from someone's genetic information. With the science of genetics in its infancy, it's impossible to know what can be told about you from your DNA in the future.

"With genetic data, it is very concrete, in terms of a road map to your physical conditions," Cavoukian says.

> "You're going to be stripped naked if someone has access to this information, in terms of what they know about you. That's what disturbs me."

The possible uses of someone's DNA are quickly expanding. Dutch scientists recently predicted the shape of a **reporter's face**, fairly accurately, based on nothing but a DNA sample, for example.

Unlike a compromised bank password, which can be changed, a privacy breach involving your DNA is irreversible, Phillips says.

Police have shown interest in the vast stores of DNA held by private companies.

Last year, police in Idaho Falls, Idaho investigating a murder obtained a **warrant** for the DNA of a murder suspect's father from **ancestry.com**, a popular genetic history site. (In an interesting twist, the DNA actually exonerated him.)

DNA storehouses may also be attractive to **hackers**, Phillips has **written**.

Paternity tests raise further questions about children's genetic privacy, Phillips points out.

"We are very clear that users own and control their data," ancestry.com spokesperson Patrick Erlich wrote in an e-mail. "They can download it, ask us to delete it and destroy the sample, and can revoke their opt-in consent to participate in research projects at any time."

"As disclosed in our policies, DNA samples are stored without personally identifying information at either a testing laboratory or other storage facility and may be kept by us unless or until circumstances require us to destroy the sample, or it is no longer suitable for testing purposes. "

So what should an individual do? Like any other decision about digital privacy, the answer really comes down to your own comfort level, and how you perceive the trade-off between some information now and a potential privacy breach in the future.