Christine Jessop's killer identified: Solved cold case raises questions about genetic privacy

October 23 2020, by Julia Creet

Credit: Pixabay/CC0 Public Domain

On Oct. 15, Toronto police announced that they had finally solved the 1984 murder of Christine Jessop using DNA evidence and genetic genealogy websites. Identifying Calvin Hoover as Jessop's killer has provided immense relief to the family and those close to the case, and in particular to Guy Paul Morin, who was wrongfully convicted and later exonerated after serving 18 months in prison.

The announcement highlights a conundrum: at risk is the genetic privacy of everyone who has uploaded—and, mostly, not uploaded—a DNA sample to a commercial genealogy site.

Genealogists never anticipated that their benign but passionate interest in tracking relations through records and DNA would ever lead to law enforcement's most potent cold case tool kit. In 2018, public awareness of law enforcement's mining of genetic genealogy came to light with the 2018 identification of the Golden State Killer. The identification of Joseph James DeAngelo relied on freely uploaded DNA results alongside painstaking genealogical research.

Data industry

Since then, law enforcement's mining of genealogical data has become an industry in itself, with hundreds of notorious cases solved and the emergence of celebrity genealogists and a reality TV series.

Even as we appreciate the profound relief that comes to families with the resolution of cases decades old and the prosecution of heinous criminals, it's important that we ask hard questions about genetic privacy and law enforcement's access to people who have never given away their DNA to commercial sites nor consented to have their DNA scrutinized.

At the heart of the problem is the nature of DNA. Our most intimate substance is a powerful identifier because each of us possesses an utterly unique combination. But our DNA doesn't belong just to us: it also belongs to everyone we are related to.

We have many more genetic relatives than we can possibly know. If we upload a sample of our DNA to a database that allows for police searches then we are making that decision for everyone who is related to us, past and future, known and unknown, rendering the notion of consent

nonsensical.

DNA fragments

A very degraded sample of DNA taken from semen found on Jessop's clothing was analyzed by Othram Inc., which specializes in human identification from difficult human DNA evidence. It's part of a growing industry known as the Human Identification Market.

Once DNA is analyzed, the forensics company uploads the results to GEDmatch and Family Tree DNA, the two genetic genealogy databases that explicitly inform their users that their DNA data may be searched by law enforcement. Most other large commercial databases such as Ancestry and 23andMe insist on warrants. Nonetheless, sales of genetic genealogy testing kits plummeted in the summer of 2019, in no small part because of the perception of privacy risks.

On May 18, 2019, consumers at GEDmatch were given the choice whether to opt in or out. That change made little difference. In November of 2019, the Orlando police obtained a warrant to search the entire database, rendering the notion of consent useless once again.

And in December 2019, GEDmatch, was sold to Verogen, a forensics company that services law enforcement because, ironically, the founders of GEDmatch could no longer manage the privacy issues that surfaced with each police use.

Solving crime, invading privacy

While there is public support for the idea that genetic genealogy should be used to solve violent crime, only 14 percent of GEDmatch users chose to make their DNA results available for law enforcement matches. This severely restricts the usefulness of the database to the police,

according to Anthony Redgrave, the forensic genealogist who identified Jessop's killer after six months of intensive research.

Redgrave is also the founder of the Trans Doe Task Force, created to research cold cases in which the subject's lived experience may not match given descriptions. He laments these restrictions as a failure of public education, even as he acknowledges that unethical use of the databases by police and other genealogists is still endemic.

Genetic privacy policies

So new is the question of law enforcement's access to genetic genealogy databases that privacy law has yet to catch up. Since the databases are located in the United States, U.S. privacy law applies.

In 2019, recognizing that the databases were vulnerable to misuse by law enforcement, the U.S. Department of Justice issued an interim policy on forensic genetic genealogical DNA analysis and searching. The policy contains two stipulations: first, that investigative agencies must identify themselves as police to genetic genealogy services, and second, these agencies can only search profiles that "provide explicit notice to their service users and the public that law enforcement may use their service sites to investigate crimes or to identify unidentified human remains."

Also crucial is the principle that: "A suspect shall not be arrested based solely on a genetic association generated by a [genetic genealogy] service." Any identifying information supplied to police must be corroborated by other means. While reassuring on paper, Redgrave suggested that police are still accessing the databases inappropriately and that the policy has no enforcement teeth.

Discretionary ethics

Steve Smith, the lead investigator on the Jessop case, agreed that the ethical use of genetic genealogy resources rests primarily with the police force working the cases. Unethical use of the databases has created a perception of privacy risks that has reduced the number of users who will allow their records to be searched.

Consumer consent is the linchpin, a notoriously slippery idea given the number of times we click agree without reading the terms of service.

In an interview with the CBC, Clayton Ruby, the lawyer for wrongfully convicted Morin, declared that it had been an open secret that the police were interested in these databases years ago, why hadn't they accessed them earlier?

When I corresponded with him over email, he wrote: "It would be easy to apply the same safeguards we use for Criminal Code Production Orders, [judicial authorization that compels people and organizations to disclose documents and records to the police], instead of leaving the decision to the commercial companies. We have not had enough time to figure out the ways the police will misuse this process. But they will."

In the absence of any regulation, and given the piecemeal approaches of police throughout Canada, Smith is setting up a genealogical working group to establish Ontario guidelines.

We are faced with the problem of regulating what Brenda McPhail of the Canadian Civil Liberties Union has called a "bulk surveillance technology," which fundamentally changes our social expectations of personal privacy.

The ethical questions abound: Should we forgo our privacy in the interests of solving violent crime, old and new? Or should we charge the government to limit access to these new forensic tools? The question of

the greater good of law enforcement access to genetic genealogy databases needs to be publicly and strenuously argued.

Provided by The Conversation