PRIVACY

JUNE 2025

Guardrails for Police Use of Investigative Genetic Genealogy in Ontario

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

This guidance by the Office of the Information and Privacy Commissioner of Ontario (IPC) is intended to enhance understanding of rights and obligations under Ontario's privacy laws respecting police use of investigative genetic genealogy. It should not be relied upon as a substitute for legislation itself or as legal advice. It does not bind the IPC's Tribunal that may be called upon to independently investigate and decide upon an individual complaint or appeal based on the specific facts and unique circumstances of a given case. For the most up-to-date version of this guidance, please visit **ipc.on.ca**.

Acknowledgement

The Office of the Information and Privacy Commissioner of Ontario (IPC) consulted with a broad range of interested parties prior to publishing this guidance, including:

- Academic researchers and lawyers
- Civil society and human rights organizations
- Experts in forensic science and pathology
- Experts in genomics and bioethics
- Experts in strategic foresight methodology
- First Nations technology leaders
- Privacy, human rights, and victims' rights regulators
- Federal, provincial, and municipal police services
- Provincial justice sector ministries

The IPC would like to thank these experts and organizations for their valuable feedback and input into the process of developing this guidance.

Contents

Introduction

Investigative genetic genealogy (IGG)[1] is an investigative technique that is being used to help expand and accelerate the search for persons of interest in cold or unresolved murder cases.[2] IGG combines new forms of deoxyribonucleic acid (DNA) analysis, private sector DNA databases, genealogical research methods, and an undercover police tactic involving the collection of "cast-off," "discarded," or "abandoned" DNA, which we refer to as the DNA surveillance tactic.[3] While IGG is gaining prominence for its potential to help police services (police) solve serious cases and advance public safety, it also raises significant privacy and human rights issues associated with the use of new sophisticated genetic sequencing techniques. It is important that when novel techniques are integrated into policing practice that the privacy and human rights implications are well understood and that the appropriate risk mitigations be identified and implemented up front.

In addition, IGG is not subject to clear or comprehensive legislative oversight. The IPC has developed policy guardrails and additional measures to help mitigate this regulatory gap. They are intended to help police in Ontario address the privacy-related risks associated with IGG in a manner that preserves the public's trust, until such time when clear, binding rules are established in law.

Benefits and risks of IGG

IGG can advance public safety objectives when used responsibly and in the right circumstances. There is a strong public interest in seeing justice done, including by resolving cold cases and bringing long awaited answers to grieving families and communities. Resolving cold cases can also support criminal justice goals of denunciating, deterring, and punishing criminal activity and holding offenders to account for serious crimes. In addition, IGG can be used to exonerate people wrongly accused or convicted of serious crimes.

IGG relies on DNA analysis. Canadian courts have long recognized that our DNA is among the most sensitive types of personal information.[4] DNA and DNA-derived information[5] can reveal core aspects of our identity. Police use of IGG raises significant privacy and human rights risks because it:

- involves the use of new sophisticated genetic techniques without clear or comprehensive legislative oversight

1 IGG is sometimes referred to as forensic investigative genetic genealogy or forensic genetic genealogy.

2 One of the first publicly known examples of police use of IGG is related to the 2018 identification of the **Golden State Killer**.

3 The term DNA surveillance tactic is used to reflect the fact that the relevant collection practices typically involve the police deploying undercover officers to surveil individuals and surreptitiously collect discarded objects to obtain their DNA.

4 *R. v. S.A.B.*, 2003 SCC 60 *(S.A.B.)*.

5 DNA-derived information includes all personal information collected by police or their agents through their use of the IGG technique, including results of DNA analysis, sex, ancestry, certain physical traits, biological relationships, genealogical family trees, and other information collected through IGG.

- largely relies on foreign-based third party service providers that operate in jurisdictions with different privacy regimes than in Canada
- can discern and map out an extensive and detailed picture of our known and unknown familial relationships
- relies on the consent of some family members to access and use DNA and DNA-derived information of other family members who share parts of their genetic code and yet have not consented to such use[6]
- can lead to broader communities, including Indigenous and racialized communities, becoming part of a police investigation simply because of shared DNA[7]
- is likely to result in police retaining the information of hundreds of innocent individuals in police investigative files, where it may be used for secondary purposes
- can reveal previously unknown information about biological relationships that can have a significant, abrupt, or even harmful impact on individuals and families

Current legal landscape

Key legal issues concerning police use of IGG are in dispute, including the extent to which IGG intrudes on a reasonable expectation of privacy, whether its use is authorized, and the conditions under which police should be using this investigative technique.[8] While police use of IGG in Ontario is subject to the common law and laws such as the Canadian Charter of Rights and Freedoms (Charter),[9] the Criminal Code,[10] and Ontario's privacy laws,[11] these laws do not explicitly authorize IGG or provide sufficient guardrails around its use. It will likely take several years before many key privacy issues are properly considered and addressed by relevant courts, tribunals, and legislators.

6 See, for example, *R. v. Wright, 2022 ONSC 6756 (Wright)* and *R. v Cochrane*, 2023 ABKB 160 *(Cochrane)*.

7 See *R. v Ali*, 2023 BCSC 2438 *(Ali)*. In *Ali*, police provided Parabon NanoLabs (Parabon), a U.S. based private sector forensic laboratory, with a crime scene DNA sample (Male #1) for SNP analysis. While Parabon's analysis did not produce any familial leads, it did generate biogeographical ancestry-related information that indicated that Male #1 was likely of Kurdish descent. Thereafter, police used the DNA surveillance tactic on attendees of a local Kurdish event. Undercover officers, posing as market researchers offering cups of tea, collected "discard" DNA samples from 144 people at the event. After sending those samples for SNP analysis, police learned that one of the 144 individuals was the brother of Male #1.

8 See, for example, *Wright*, which is on appeal to the Ontario Court of Appeal (Court file #COA-24-CR-0036); *Cochrane*; and the report of the Standing Senate Committee on Legal and Constitutional Affairs, "Public Protection, Privacy and the Search for Balance: *A Statutory Review of the DNA Identification Act*", June 2010. In addition, note that while the police use of the DNA surveillance tactic has, for quite some time, been upheld by the courts on the basis that people abandon their right to genetic privacy when they discard objects that may contain traces of their DNA (the *abandonment doctrine*), recent caselaw provides support for the public's reasonable expectation of privacy in their DNA, including after police collect it from a discarded object. Cases accepting the *abandonment doctrine* include *R. v Stillman*, [1997] 1 S.C.R. 607 *(Stillman)*; *R. v. Patrick*, 2009 SCC 17 *(Patrick)*; *Barlow v. the Queen*, 2004 CarswellOnt 11494 *(Barlow)*; *R. v Marini*, 2005 CanLII 55694 (ON SC); *Cochrane*; *R. v. Macauley*, 2025 ONSC 335 *(Macauley)*. Cases supportive of the public's reasonable expectation of privacy in DNA collected by police from a discarded object, include Justice Abella's dissent in *Patrick*; Justice Vauclair's dissent in *D'Amico c. R.*, 2019 QCCA 77 *(D'Amico)*; *R. v Bhogal*, 2020 ONSC 7327 *(Bhogal)*; and *Wright*.

9 Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

10 Criminal Code, RSC 1985, c C-46.

11 *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31 (FIPPA) and *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c M.56. (MFIPPA).

In the meantime, some police have begun to develop their own IGG policies or procedures.[12] While setting local rules is an important step, and may be used to help mitigate privacy risks, they are insufficient to ensure province-wide consistency, and they do not provide for sufficient scrutiny or oversight. In addition, they generally leave important legal and policy decisions to a closed internal process, rather than a more open, inclusive, and transparent public debate on questions like what kinds of cases are to be deemed serious enough to justify the use of IGG and what guardrails should be in place around the collection, use, retention, destruction, and disclosure of DNA and DNA-derived information.

Mitigating the gap with IGG guardrails

To help mitigate the current regulatory gap in Ontario, the IPC has worked collaboratively with many other interested parties to develop policy guardrails around the responsible use of IGG by police in the context of criminal investigations. These guardrails cover overarching principles of legality, accountability, transparency, necessity and proportionality, all of which are critical for building public trust. They also consider the need for robust IGG governance frameworks, the importance of oversight, and the crucial need for public consultations, especially with Indigenous and equity-seeking groups.

These guardrails are intended to help police in Ontario mitigate the privacy-related risks associated with this investigative technique in a manner that preserves the public's trust, until such time when clear, binding rules are established through formal legal instruments.

The following twelve guardrails incorporate key privacy requirements and best practices around police use of IGG. The IPC may refine these guardrails over time as key developments come to our attention.

The twelve guardrails are:

1. Lawful authority and activity
2. Necessity and proportionality
3. Accountability
4. Third party procurement
5. Data minimization and purpose limitation
6. Retention
7. Data security
8. Controls for surreptitious DNA collection
9. Openness and transparency
10. Individual access and privacy rights
11. Public consultation
12. Ethical disclosure guidelines

12 While the U.S. Department of Justice has published its **Interim Policy Forensic Genetic Genealogical DNA analysis and searching**, it appears that police and forensic centre policies on IGG that have been or are being developed in Canada have yet to be made publicly available.

Beyond these twelve guardrails, the IPC has identified three additional measures to help ensure a consistent approach to IGG governance in Ontario: an independent IGG advisory committee, the localization of IGG methodologies, and regular public engagement to help evaluate the impacts of IGG.

Process of development

To develop these guardrails, the IPC conducted in-depth research and environmental scanning of police use of IGG as part of its strategic priority on ***Next Generation Law Enforcement***. The IPC's main goal in this priority area is to contribute to building public trust in law enforcement by working with relevant partners to develop the necessary guardrails for the adoption of new technologies in ways that advance public safety, while safeguarding Ontarians' access and privacy rights.

Building on this extensive body of research, the IPC initiated a strategic foresight exercise on police use of IGG in the context of criminal investigations. Our office held various meetings and workshops with a broad range of interested parties to learn more about their different perspectives on IGG and to seek their input into the development of proposed guardrails. The effect of these active engagements with leading experts and organizations was a better understanding of parties' perspectives on IGG and what should be included in an appropriate and well-balanced policy governance framework.

Scope and purpose of guidance

These IGG guardrails apply to Ontario police, their supervisory authorities,[13] and their agents who use IGG in the context of criminal investigations. The Ontario Provincial Police (the OPP) and its supervising authority, the Ministry of the Solicitor General, are subject to Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA). Municipal police and police service boards that supervise them are subject to the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).[14]

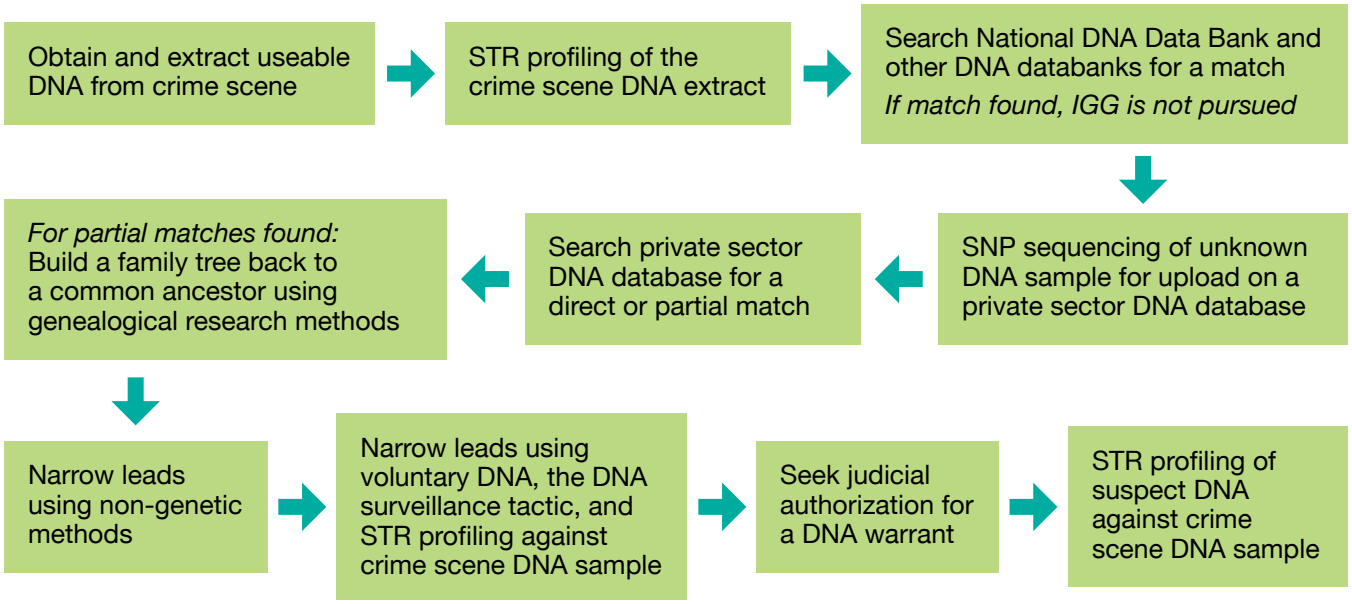
These guardrails do not address the use of IGG by other organizations. They are not intended to apply to the use of IGG for humanitarian purposes, such as to identify unidentified human remains associated with a natural disaster or to identify an unidentified person whose death may have resulted from the commission of a criminal offence. Different legal and policy considerations may apply to any use of IGG that falls outside the scope of these guardrails.

13 The supervisory and oversight-related responsibilities assigned to police service boards with respect to police, and to the Solicitor General and the Ministry of the Solicitor General with respect to the OPP, are set out under Parts IV and V of the *Community Safety and Policing Act*, 2019, S.O. 2019, c. 1, Sched. 1 (CSPA).

14 Until July 1, 2025, FIPPA and MFIPPA were essentially the same in terms of their privacy requirements imposed on regulated institutions. However, as a result of Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act* (2024), the privacy obligations of provincially regulated police under FIPPA are now more robust than those imposed on their municipal counterparts.

These guardrails are not an endorsement of police use of IGG. This guidance also does not replace the need for a broader public debate on how laws should be established or updated to govern police use of this investigative technique. Rather, it is our hope that these guardrails will contribute to the ongoing policy discussion and help inform decision-making about whether and how police may responsibly use IGG, while respecting the rights of persons, Indigenous communities, and diverse groups in Ontario. Like other advanced investigative techniques, police use of IGG in Ontario should be governed by clear, formal, and binding legal rules that effectively address safety, privacy, accountability, transparency, and human rights.

What is investigative genetic genealogy?



Pre-IGG: STR sequencing of crime scene DNA

In some criminal investigations, bodily samples[15] of an unknown person, such as blood, saliva, or human tissue, are collected from a crime scene and DNA extracted from it. The crime scene DNA extract can then be used to create a unique DNA profile using a decades old process called short tandem repeats (STR) DNA profiling. That process involves measuring the length of a small number (e.g., one or two dozen) of repeating segments or loci of DNA to help identify the unique DNA profile and biological sex of the person. STR DNA profiling can also provide some insights into the donor's ethnicity and relatedness to immediate family members. However, STR DNA profiling does not yet appear capable of revealing information like the person's physical traits, susceptibility to disease, or ancestry.

15 In this guidance, a "bodily sample" is also referred to as a "DNA sample."

In defined circumstances, the federal *DNA Identification Act*[16] authorizes the Royal Canadian Mounted Police (RCMP) to compare the STR DNA profile derived from a crime scene DNA sample against the STR DNA profiles held in the National DNA Data Bank (NDDB) for identification purposes. The NDDB contains several indices of STR DNA profiles.[17] As of June 2025, the NDDB contained over 720,000 STR DNA profiles that can be compared against an unknown STR DNA profile for purposes permitted under the act.[18] In appropriate circumstances, the RCMP can then communicate the results of that comparison (e.g., a match) to the relevant forensic laboratory and the police.[19]

Where a match in the NDDB — or other government DNA database such as the Centre of Forensic Sciences' (CFS) "discard index"[20] — is not found, police are starting to pursue the use of IGG. It is our understanding that police in Ontario are using IGG to help resolve cold cases involving murder.

IGG's reliance on SNP sequencing and SNP files

Since the early 2000s, Canadians, and people in other countries, have been providing DNA data to private sector DNA databases for the purposes of identifying unknown biological relatives, building out their family trees, learning more about their ancestry, or for other recreational purposes. Private sector database operators like GEDmatch and FamilyTreeDNA have since expanded the use of these kinds of DNA databases to facilitate IGG.[21] The discovery of biological relationships is made possible by the use of new sophisticated techniques, typically single nucleotide polymorphisms (SNP) sequencing.

In contrast to the narrow focus of STR DNA profiling, involving one to two dozen loci, SNP sequencing involves the examination of tens or hundreds of thousands, or even millions of genetic markers.[22] SNP sequencing provides a much more comprehensive view of a donor's genetic code that is used to generate a SNP file. The resulting SNP file is then compared against private sector databases containing other SNP files to reveal partial familial

16 *DNA Identification Act*, SC 1998, c 37.

17 These indices include: a convicted offenders index, a crime scene index, a victims index, a missing persons index, a relatives of missing persons index, a human remains index, and a voluntary donors index. Some of these indices are subject to different conditions when it comes to, for example, adding new samples, searching existing samples, communicating the results of comparisons to others, removing access to DNA profiles, and storing or destroying bodily samples.

18 **National DNA Data Bank statistics, Royal Canadian Mounted Police**.

19 Key sections governing the operation of the *DNA Identification Act* include s. 2 and s. 5-11.

20 *Barlow*; Ontario Office of the Independent Police Review Director, **Casting the Net: A Review of Ontario Provincial Police Practices for DNA Canvasses**, pg. 45-46 and 80 *(Casting the Net)*; Canadian Civil Liberties Association **letter** regarding Systemic review of OPP DNA Sampling, pg. 12-14 *(CCLA systemic review letter)*; and the discussion of local "Discarded Sample Index" databanks at para 46-47 of *D'Amico*.

21 GEDmatch and FamilyTreeDNA's DNA database have at least two purposes: to help people trace ancestors and lineage and permit police access to user data for the purpose of IGG (e.g., GEDmatch provides services through "GEDmatch PRO" and FamilyTreeDNA provides services through "Investigative Genetic Genealogy Matching"). In recent years, other third party service providers (e.g., Othram Inc.) have established private sector DNA databases for the sole purpose of police use of IGG.

22 Typically, STR profiling looks at 15 short tandem repeat loci to identify individuals (see *Granger v. Ontario*, 2024 ONSC 6503 *(Granger)* at para 25). In contrast, SNP analysis involves methods such as whole genome sequencing, where the entire genome of the DNA sample is sequenced (i.e., several million SNPs), or SNP microarrays, which detect known genetic variants across a genome (e.g., approximately 600,000 SNPs on a microarray). Additionally, there are other SNP methodologies that take a more targeted approach, such as ForenSeq Kintelligence, which examines 10,230 SNPs specifically for kinship determination.

matches. Unlike the one-to-one matching performed in the NDDB, these IGG searches in private sector databases look for partial matches, implicating hundreds of family members, including many distant unknown relatives.

Private sector DNA database operators are not subject to any of the binding guardrails and privacy protections that apply to the NDDB under the *DNA Identification Act*.[23] There are now millions of individuals' SNP files in these private sector DNA databases. While some private sector database operators provide police with access to their databases on receipt of a court order or subpoena, companies like GEDMatch and FamilyTreeDNA have taken a different approach. These DNA database operators generally encourage individuals to share their SNP files with police. Under this approach, individuals have been left to either opt-in to allowing police access to their DNA related information, or to opt-out of such access, in the latter case, with the effect of permitting police access by default. Either way, these kinds of private sector DNA database operators provide police access to or use of their databases without a court order or subpoena.

How IGG works

IGG starts with police transferring a DNA sample or extract from a crime scene to a third party service provider, such as Othram Inc., or Parabon NanoLabs (both based in the U.S.) for SNP sequencing. The resulting SNP file is then cross-referenced against a database(s) containing SNP files, for example, private sector databases such as GEDmatch or FamilyTreeDNA (also based in the U.S.). This in-depth genetic scrutiny allows investigators to find partial matches between an unknown individual's genetic code and the genetic codes of close and distant relatives.[24] In addition to revealing detailed information about individuals' ancestral relationships, SNP sequencing can also be used to reveal information about certain health and physical traits.[25]

---

23 For example, the *DNA Identification Act* (and the related *Criminal Code* provisions) restricts the types of offences that can trigger inclusion of DNA profiles into the convicted offenders' index. The Act also safeguards privacy by: (i) limiting the collection, use, and retention of bodily samples and DNA-related information in its various indices; (ii) limiting the forms of DNA analysis that can be done (e.g., only use non-coding or "junk" DNA to identify matches as between one DNA profile and another); (iii) regulating who may receive the results of DNA analysis and for what purposes; (iv) controlling access to information in the NDDB; (v) requiring timely destruction of DNA samples and results in defined circumstances; (vi) establishing offence provisions related to the misuse of this information; and (vii) creating a National DNA Databank Advisory Committee that must report annually on matters related to the operation of the NDDB. Appellate courts have recognized that these controls are essential in cases such as *R. v. Briggs*, 2001 CanLII 24113 (ON CA), at para 8-39; *S.A.B.* at para 48-52; and *R. v. Rodgers*, 2006 SCC 15, at para 11-13, and 39-42.

24 The matching process used by private sector DNA database operators, like GEDmatch and FamilyTreeDNA, generally involves the use of a proprietary algorithm to determine degrees of relatedness between a crime scene SNP file and the SNP files held in private sector databases. The algorithm produces a list of database users who appear to be most closely related to the crime scene SNP file. The approximate closeness of the relationship between two SNP files is assessed by looking for "long stretches of identical DNA shared between the crime scene SNP file and other SNP files. When two SNP files share segments of DNA above a certain length (calculated in "centimorgans"), the algorithm concludes that the two SNP files have some genealogical relation to each other" (see *Cochrane* at para 11-15).

25 See, for example, *Wright* and *Ali* which reveal that police have sought and used SNP-derived information from Parabon that includes a composite image predicting a person's face, a description of predicted physical traits (e.g., information associated with freckling and eye, hair, and skin colour), and estimated biogeographical ancestry (e.g., ethnic regional origin). Also see the discussion of SNP's capacity to "show statistical and causal connections to various diseases" in *Granger*.

If a partial match is found in a private sector DNA database, a genealogist is then tasked with building a comprehensive family tree back to the point of a common ancestor.[26] The tree can extend to multiple generations and branches of a family, including hundreds of relatives — some of whom are alive and others who died decades or even centuries before the crime occurred. The resulting family tree can span many different communities or countries.

Once a comprehensive family tree is developed and provided to the police, it is entered into the investigative file. Police will then work to narrow down the potential leads to a smaller branch of the family tree. In some cases, leads can be narrowed down based on the biological sex of the unknown person of interest or based on who was known to be alive or in the country when the crime occurred.

Often the process of narrowing down individuals in the family tree can be more difficult and require additional investigative steps by police. These steps may include seeking consent from additional family members to voluntarily provide a DNA sample to further an investigation (e.g., to exclude or identify a person(s) of interest or portions of a family tree). In many other cases, police will use the DNA surveillance tactic, which typically involves undercover officers surveilling a narrower group of persons of interest to surreptitiously collect a DNA sample from an object they discard. For example, undercover police officers may collect a bodily sample from a discarded drinking cup, piece of gum, pizza crust, or cigarette butt. In some cases, police go a step further by staging a fictitious event in order to collect DNA from persons of interest.[27] Police will then provide the CFS with the surreptitiously collected DNA sample for STR comparison against the crime scene DNA sample to identify a match, or conversely, eliminate the individual as a suspect in the investigation.

Post–IGG: DNA warrant and STR sequencing

Once police confirm a match with the surreptitiously collected DNA sample, police will typically proceed to the next step. This involves seeking judicial authorization to ensure that they can lawfully detain the suspect, re-acquire their DNA pursuant to a DNA warrant, charge the suspect, and present the suspect's DNA as evidence in court to help secure a criminal conviction.

26 This often involves accessing, using, or scraping genealogical records, historical records, and various other kinds of records systems, some of which have been made "publicly" available online for particular purposes (e.g., in relation to obituaries, birth, marriage, and death records, wills, census data, electoral registers, news articles, and social media).

27 Some uses of the DNA surveillance tactic have involved police arranging a false business meeting or conducting fictitious market research (see *D'Amico* at para 41, *Ali* at para 7, and *R. v. Delaa*, 2009 ABCA 179, at para 6).

Some concerns arising from police use of investigative genetic genealogy

Reliance on individual consent

Private sector DNA database operators and their police clients that rely on the consent of one individual to authorize their IGG-related activities risk undermining the privacy rights and interests of non-consenting individuals.[28]

GEDmatch and FamilyTreeDNA's combined consent-based SNP DNA databases have the potential to facilitate the identification of 90 to 95 per cent of Americans of European descent — and millions of Canadians — to a third cousin or closer, or 60 per cent of people to a second or closer biological relative without their knowledge or consent.[29] Just because some individuals choose to provide their DNA and DNA-derived information to a third party does not mean that non-consenting relatives have no privacy rights or interests in this shared information. Moreover, we have little to no power to control who our relatives are, the decisions they make, or the fact that we all share significant portions of our DNA with known and unknown relatives.

IGG, therefore, involves those who did not themselves knowingly volunteer any DNA or DNA-derived information, but who become part of a criminal investigation indirectly through relatives who may have chosen to do so. This detailed, expansive collection and search of sensitive information brings innocent individuals within the scope of a police investigation without any particular suspicion. Even in situations where police do not (or no longer) consider a non-consenting individual to be a person of interest, suspect, or do not charge them with a criminal offence, their personal information is likely to become part of the police investigative file. So long as their personal information is retained, it is at risk of theft, loss, or unauthorized use or disclosure.[30] In addition, it may be used for secondary purposes (e.g., use in a separate, unrelated investigation).

Moreover, IGG may inadvertently reveal information that is highly intrusive and may infringe upon the privacy interests of individuals and communities, including Indigenous communities and other affected communities. For example, IGG may reveal familial information unknown to the individual and their families and biological relatives — personal information that someone may have kept secret or that others may have chosen not to know. If inadvertently disclosed, this previously unknown information could cause significant harm and upend people's lives.

28 *Canada (Privacy Commissioner) v. Facebook*, Inc., 2024 FCA 140 at para 74-83.

29 **Verogen and Gene by Gene Form Groundbreaking Partnership to Accelerate Adoption of Forensic Investigative Genetic Genealogy**.

30 FIPPA, s. 40.1.

In light of these overlapping privacy rights and interests in shared genetic information, police should be cautious about relying on the consent of a volunteering relative. This caution is grounded in Charter jurisprudence that has rejected the notion that one individual can consent to the waiver of the privacy interests shared with another person.[31]

The question of informed consent is further complicated by the fact that private sector DNA databases, particularly those located outside of Canada, take very different approaches to consent and privacy. Terms of service may change unilaterally without sufficient notice to individuals, and they may lack the regulatory oversight, transparency, and accountability mechanisms our laws require. In some cases, organizations could change hands[32] or file for bankruptcy with little clarity on what happens to consumers' DNA and DNA-derived information thereafter.[33]

Use of the DNA surveillance tactic

IGG often involves the use of the DNA surveillance tactic to surreptitiously collect DNA from a person(s) of interest or their biological relative(s) without their knowledge or consent. Until recently, courts have held that people abandon their right to genetic privacy when they discard objects such as coffee cups, tissue paper, and chewing gum.[34] As a result, this surveillance technique has been available to police without any binding guardrails, including those needed to protect the privacy of individuals who have been eliminated as suspects.

More recently, however, some Ontario courts have questioned this *abandonment doctrine* and concluded that a person can retain a reasonable expectation of privacy in their DNA found on a discarded object.[35] This jurisprudence suggests that while an individual may choose to discard, for example, a tissue or empty cup, it is not reasonable to conclude that they are also choosing to discard the traces of their DNA found on those items, including because individuals have no choice but to shed their DNA in the course of their everyday activities. This raises the question as to whether individuals can be said to be legally abandoning their privacy rights or interests in their genetic information revealed from discarded items, let alone the genetic information of their biological relatives.

These developments raise questions about the lawfulness of the collection, use, retention, and disclosure of "discard" DNA by police and forensic laboratories and the need for guardrails. For example, authorities may be over collecting DNA through the use of the DNA surveillance tactic, particularly if their collection practices are not subject to sufficiently rigorous thresholds or other privacy controls up front. In addition, public forensic laboratories, like the CFS, are compiling, retaining, and using the bodily samples and/or DNA profiles of individuals whose DNA was collected surreptitiously in the context of a criminal investigation long after they have been eliminated as suspects.[36]

---

31 *R. v. Cole*, 2012 SCC 53; *R. v. Marakah*, 2017 SCC 59 *(Marakah)*; and *R. v. Reeves*, 2018 SCC 56.

32 **A message to Verogen customers about the GEDmatch partnership, Verogen**.

33 **23andMe filed for bankruptcy. What it means for your data : NPR**; **Chairman Ferguson letter regarding 23andMe, Federal Trade Commission**; and **Bankrupt DNA testing company 23andMe to be bought by Regeneron**.

34 See the discussion of the DNA surveillance tactic in footnote 8.

35 See the discussion of the DNA surveillance tactic in footnote 8.

36 *Barlow; Casting the Net*, pg. 45-46 and 80; *CCLA systemic review letter*, pg. 12-14; and the discussion of local "Discarded Sample Index" databanks at para 46-47 of *D'Amico*.

Security risks

Ontario police rely on the services of third parties when undertaking IGG. For example, they may use third parties for SNP sequencing, to access large-scale private sector DNA databases, and to conduct genealogical research. Police and their supervisory authorities remain accountable for any third party errors, omissions, or inadequate safeguards around the handling of DNA and DNA-derived information from IGG, including security and operational deficiencies resulting in significant security and privacy breaches.[37]

Some private sector DNA databases may have insufficient information controls or incorrect access permissions that could enable police or their agents to conduct searches of their DNA databases without individuals having provided consent. For example, in a 2020 data breach, all profiles on GEDmatch's DNA database were visible to the police for a number of hours, irrespective of whether individuals had provided consent for police to access and use of their information.[38] Concerns have also arisen around third party forensic laboratory service providers (e.g., Parabon NanoLabs) exploiting a loophole in a DNA database operator's system (e.g., GEDmatch), and obtaining unauthorized access to DNA-derived information of individuals who explicitly opted-out of sharing their information with police.[39] It may also be challenging for individuals who have provided their DNA and DNA-derived information to know of such searches, and private sector DNA database operators may similarly be unaware of their information security failures.

Misuse of IGG could also involve a person submitting, or asking someone else to submit, a SNP file to a private sector DNA database as if the file was their own. In one case, researchers were even able to submit artificial DNA profiles to GEDmatch to infer the genetic sequences of other DNA database users.[40] While such uses may be against a private sector DNA databases policy, since IGG involves consumer-facing technologies, with little to no oversight, these security lapses may be difficult to detect.

Indigenous perspectives

Indigenous perspectives about genetic information can differ from western or settler concepts of DNA. First Nations, Inuit, and Métis peoples may conceive, understand, and honour ancestral relationships, community membership, and the bodies and tissues of their deceased differently from organizations working in the criminal justice, forensic, and private sectors.

---

37 For example, a 23andMe data breach led to the unauthorized access of personal and familial information belonging to over 5 million users. Canadians impacted by the breach are suing 23andMe, claiming that there were inadequate security and privacy safeguards and that their highly sensitive information was sold over the dark web. The cross-jurisdictional impact of the breach has prompted a joint investigation by the Office of the Privacy Commissioner of Canada and the United Kingdom's Information Commissioner's Office. See **Announcement: Privacy authorities for Canada and the United Kingdom launch joint investigation into 23andMe data breach** and **Joint letter on privacy protection during bankruptcy proceedings involving 23andMe Holding Co**.

38 **GEDmatch confirms data breach after users' DNA profile data made available to police**.

39 **GEDmatch Loophole Gave Police Access to Private DNA Data**.

40 Ney, P., Ceze L. and ohno, T. (2018). *Computer security risks of Distant Relative Matching in Consumer Genetic Databases*. Cornell University.

Police IGG practices that are premised on conceptions of individual privacy and consent may not reflect the cultural value placed on group or shared rights or the inherent sovereignty of Indigenous peoples over their data.[41] Indigenous communities may be particularly concerned about the potential impact of using DNA and DNA-derived information in determining individuals' status in their communities,[42] their attachment to their land, and their exercise of treaty rights. Disclosure of previously unknown information about kinship could also have adverse impacts in Indigenous communities by raising unresolved intergenerational trauma suffered as a result of the Sixties Scoop and the residential school system.

Too many First Nations, Inuit, and Métis communities have been — and continue to be — over policed and underserved across Canada.[43] If police use IGG responsibly and under the right circumstances, it could help advance Ontario's commitment towards truth and reconciliation, for example, by helping to bring closure to Indigenous families and communities with respect to missing and murdered Indigenous women and girls and other historical injustices. To align with constitutional rights and the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP), police and their supervisory authorities should assess and meet their responsibility to consult with First Nations, Inuit, and Métis peoples. Consultations should be conducted in a meaningful and culturally appropriate manner.

Guardrails for police use of investigative genetic genealogy in criminal investigations

Given the concerns outlined above, clear guardrails are essential to guide responsible use of IGG by police in the context of criminal investigations. The following twelve guardrails are designed to be part of a robust IGG governance framework. They are meant to help police respect the privacy and human rights of individuals and affected communities, protect the security of their information, ensure transparency and accountability, and secure trust and confidence in law enforcement and the administration of justice.

Police and their supervisory authorities must ensure that their IGG programs are in full compliance with relevant laws and police should seriously consider adopting privacy best practices, including to help address any gaps in the law.

41 See, for example, the First Nations Information Governance Centre's **First Nations principles of Ownership, Control, Access, and Possession**.

42 Crown-Indigenous Relations and Northern Affairs Canada, **Background on Indian registration** and **Remaining inequities related to registration and membership**.

43 David, J. D., & Mitchell, M. (2021). *Contacts with the police and the over-representation of Indigenous peoples in the Canadian criminal justice system*. Canadian Journal of Criminology and Criminal Justice, 63(2), 23-45.

1. Lawful authority and activity

To ensure compliance with privacy requirements and adherence to best practices for IGG, police and their supervisory authorities should begin from the foundational premise that members of the public generally have a reasonable expectation of privacy in their DNA and DNA-derived information from IGG.

In this context, police should identify and document their independent legal authority for their IGG-related information handling activities (e.g., authority found under the common law or a statute other than FIPPA or MFIPPA).[44] In addition, police have an obligation to avoid collecting personal information and data from a third party where that party collected or compiled that information contrary to law.[45]

2. Necessity and proportionality

It is critical that police address the privacy principles of necessity and proportionality when using or considering the use of IGG. Due to its high level of privacy invasiveness, IGG should only be used for a pressing and substantial identification-focused purpose. In particular, IGG should only be used to investigate the most serious criminal offences and only when other investigative means have been tried and failed or are unlikely to succeed (e.g., after an unsuccessful search in the NDDB). The collection, use, retention, and disclosure of DNA and DNA-derived information from IGG should be proportional to the benefit gained. In making these assessments, all relevant factors should be considered, including the nature of the privacy intrusion(s) and the impacts of IGG on affected individuals and communities.[46]

Police should also assess whether their use of IGG is effective and minimally impairing. DNA and DNA-derived information from IGG should only be collected, used, retained, or disclosed to generate leads that can significantly advance a criminal investigation. These information handling activities should be tailored to be narrow in scope to help limit the intrusion of privacy to what is reasonably necessary to conduct the investigation. Police should not arrest a person of interest or suspect based solely on genetic association generated by an IGG service provider.[47]

Police should employ a rigorous prior approval mechanism to ensure that any case being considered for IGG meets all legal requirements and is properly vetted against the criteria set out in this guidance.

---

44 Where the collection, use, retention, or disclosure of personal information attracts a reasonable expectation of privacy, compliance with privacy legislation requires that its collection, use, retention, or disclosure be independently authorized under the common law or a statute. See *Marakah*; *R. v. Spencer*, 2014 SCC 43; *R. v. Orlandis-Habsburgo*, 2017 ONCA 649; *R. v. El-Azrak*, 2018 ONSC 4450; *R. v. Otto*, 2019 ONSC 2514; *R. v. Jones*, 2017 SCC 60; *R. v. Tran*, 2018 ONSC 132; and *R. v. S.S.*, 2023 ONCA 130.

45 **IPC Privacy Complaint PI21-00001**; **IPC Order MO-2225**; and the Office of the Privacy Commissioner of Canada's Special Report: ***Police use of Facial Recognition Technology in Canada and the way forward***.

46 Factors to consider when assessing the benefits versus the risks around IGG use may include, for example, whether the police investigation: (i) involves methodologies that have been scientifically validated and peer reviewed; (ii) involves information about immediate or distant relationships; (iii) extends to predictions about individuals' face, physical traits, biogeographical ancestry, or health status; (iv) involves targeted as opposed to sweeping surveillance; and (v) is more or less likely to have a prejudicial or discriminatory impact on Indigenous or racialized individuals or communities.

47 U.S. Department of Justice, ***Interim Policy Forensic Genetic Genealogical DNA analysis and searching***.

3. Accountability

Police and their supervisory authorities are responsible for DNA and DNA-derived information from IGG under their custody or control and should be able to demonstrate their compliance with all legal requirements and adherence to privacy best practices. This includes the following:

- **Privacy impact assessment (PIA):** Conduct a program level PIA before any IGG pilot project, program or initiative is launched to assess, address, and mitigate the potential privacy and security risks involved.[48] The PIA should be reassessed and updated as necessary, including before making any significant change to the purpose for which any DNA or DNA-derived information will be collected, used, retained, destroyed, or disclosed.
- **Privacy-compliant governance framework:** Establish an IGG governance framework with clear structures, policies, systems, procedures, and properly documented accountability measures to assign privacy responsibilities, coordinate privacy work, manage privacy risks, and ensure compliance with the Charter, privacy laws, and any other applicable laws.
- **Training:** Develop and implement a privacy-specific training program for police involved in the use of IGG. Training should address specific privacy risks and considerations and controls around handling DNA and DNA-derived information from IGG. Track and document that staff complete the program successfully before participating in any IGG-related activity.
- **Notice regime:** Take reasonable steps to provide written notice at the appropriate time (e.g., within 90 days of the conclusion of the relevant investigation(s)) to, at a minimum, persons whose DNA has been collected, used, retained, or disclosed during an IGG-related criminal investigation. Establish a process for documenting and keeping track of when such written notice should and has been given.
- **Oversight:** The Ministry of the Solicitor General and police service boards should establish clear directives and policies and other mechanisms to ensure that IGG programs are designed and governed in compliance with relevant laws and the guardrails set out in this guidance.
- This should include a requirement to conduct regular compliance audits to assess overall compliance with applicable law and continued alignment with privacy requirements and evolving best practices. At a minimum, compliance audits should assess:
    - ongoing compliance with lawful authority and other legal requirements
    - whether the IGG pilot project or program continues to be necessary and proportional
    - ongoing compliance with IGG policies and procedures

48 As of July 1, 2025, s. 38 of FIPPA provides that PIAs are mandatory for provincial institutions, like the OPP.

- the sufficiency and frequency of updates made to IGG policies and procedures, including updates to public information and reporting about an IGG pilot project or program
- compliance with legal, policy, and procedural requirements regarding the retention and destruction of DNA and DNA-derived information
- any public complaints received about the IGG pilot project or program and how they were handled
- any privacy breaches that occurred and how they were handled
- third party compliance with privacy obligations concerning the IGG pilot project or program
- identify what remedial action has been taken or is planned to address any instances of non-compliance with law, policy, or procedure

- Regular program reviews should also be conducted to measure the overall effectiveness of the IGG pilot project or program, including whether it is achieving the intended objective and adhering to privacy requirements and best practices.[49]
- Results and recommendations of compliance audits and pilot projects or program reviews should be considered, documented, and implemented as appropriate, and should be provided to the Ontario Ministry of the Solicitor General or police service boards to support rigorous vetting and oversight of IGG.

4. Third party procurement

Police and their supervisory authorities remain accountable for their use of IGG when outsourcing components of the investigative process to third parties. Agreements between police and third parties should contain terms and conditions that ensure compliance with all laws and best practices applicable to police in Ontario, including applicable access, privacy, and security requirements. Among other things, agreements should address limitations on the collection, use, retention, and disclosure of personal information, destruction requirements, third party compliance audits or inspections, and breach notifications.[50]

Third parties who provide commercial IGG-related services must comply with applicable Canadian private sector privacy laws. Police and their supervisory authorities should independently inform themselves of the lawfulness of the collection and information handling practices of third parties and conduct their own due diligence review. Police should not accept general compliance assertions made by a third party.[51]

49 Program reviews should also weigh and consider the statistical reports outlined in guardrail 9.

50 The IPC's guidance on ***Privacy and Access in Public Sector Contracting with Third Party Service Providers*** sets out recommended best practices for exercising due diligence and ensuring accountability for privacy and access to information when contracting third party service providers. It provides guidance throughout the entire procurement process from planning, tendering, vendor selection, and agreement management and termination.

51 **IPC Privacy Complaint PI21-00001**; **IPC Order MO-2225**; and the Office of the Privacy Commissioner of Canada's Special Report: ***Police use of Facial Recognition Technology in Canada and the way forward***.

5. Data minimization and purpose limitation

Police should limit the collection, use, retention, and disclosure of DNA and DNA-derived information from IGG to only what is reasonably necessary for a lawful IGG program. In addition, DNA and DNA-derived information from IGG should not be used when other less intrusive means are available. Police and their agents should not use DNA or DNA-derived information from IGG to determine an individual's genetic predisposition for disease or any other medical condition or psychological trait, or for any other secondary purposes that fall outside of the scope of the police's lawful authority.[52]

6. Retention

DNA and DNA-derived information of any individual that comes under IGG scrutiny must not be retained for longer than is necessary to fulfill the purposes of an investigation and related court proceedings. Retention of DNA and DNA-derived information must comply with all record keeping and access to information requirements.[53] The CFS, police, and their supervisory authorities must ensure records retention schedules are in place and implemented consistent with legal requirements, including those mandating the destruction and permanent removal of the bodily samples, DNA samples, DNA profiles (e.g., the results of forensic DNA analysis), SNP files, and related records of all excluded persons of interest who provided their DNA sample on a voluntary basis.[54]

The CFS and police should ensure they take the same approach with respect to individuals whose DNA was collected surreptitiously using the DNA surveillance tactic and used to eliminate them as suspects, (see guardrail 8).

7. Data security

DNA and DNA-derived information from IGG that is stored physically or electronically must be protected by appropriate administrative, technical, and physical safeguards.[55] These safeguards must ensure the security, integrity, and confidentiality of records under custody or control of an institution or its agents, (see guardrail 4). The CFS, police, and their agents should periodically test and confirm the adequacy and effectiveness of their data security controls.

The CFS, police, and their agents should implement protective security safeguards and measures commensurate with the high sensitivity of DNA and DNA-derived information from IGG, consistent with privacy requirements and evolving best practices.

52 U.S. Department of Justice, ***Interim Policy Forensic Genetic Genealogical DNA analysis and searching***.

53 FIPPA, s. 40(1); FIPPA *General Regulation*, RRO 1990, Reg 460; FIPPA *Disposal of Personal Information*, RRO 1990, Reg 459; MFIPPA, s. 30(1); MFIPPA *General Regulation*, RRO 1990, Reg 823; and the *Archives and Recordkeeping Act*.

54 *Criminal Code*, s. 487.09(3); *Granger*.

55 FIPPA R.R.O 1990, *Regulation 460*, s. 4(1) and MFIPPA R.R.O. 1990, *Regulation 823*, s. 3(1). Additionally, as of July 1, 2025, FIPPA explicitly requires institutions, such as the OPP, to take reasonable steps to ensure personal information is protected against theft, loss, and unauthorized use or disclosure (see FIPPA, s. 40(5)).

8. Controls for surreptitious DNA collection

It is critical that police institute controls to protect the privacy and human rights and interests of individuals and their biological relatives impacted by the use of the DNA surveillance tactic. Police should only collect DNA surreptitiously once they are satisfied that, at a minimum, they have reasonable grounds to suspect that the relevant person(s) of interest is connected to the serious criminal offence under investigation.

Over time, the appropriate legal threshold ("reasonable grounds to believe" or "reasonable grounds to suspect") in the context of IGG may be settled by an appellate court or by the legislature. Given the reduced protection of the lower suspicion-based standard, it is all the more crucial that the surreptitious DNA collection be followed by a proper DNA warrant process.[56] That process must ensure that the court is provided with a full description of all the investigative steps and their impact on the privacy of affected individuals and communities.

The CFS, police, and their agents should destroy without delay an individual's surreptitiously seized bodily sample, DNA sample, DNA profile (e.g., the results of the forensic DNA analysis) once the results of forensic analysis establish that the crime scene DNA sample is not from that individual. Any electronic access to the DNA results of those eliminated from the focus of the investigation should also be permanently removed.

9. Openness and transparency

Police must be open and transparent to the public about their use of IGG, including how they collect, use, retain, and disclose DNA and DNA-derived information from IGG and when they destroy it.[57] This responsibility includes being transparent about their use of any agents to process or handle personal information on their behalf. Police should make their program level IGG policies and practices publicly available and accessible on their website.

Police should publish meaningful annual statistics concerning their use of IGG to reflect on the state of compliance, effectiveness, and appropriateness of IGG programs. At a minimum, these reports should contain:

- the total number of cases which were considered as potential candidate cases for IGG
- the number of these cases that were permitted or rejected to proceed as IGG cases
- the types of offences involved and the numbers of IGG investigations per each offence category
- the total number of cases resulting in one or more investigative leads and the total number of leads generated

56 *Criminal Code*, s. 487.05.

57 S. 44-46 of FIPPA and s. 34-35 of MFIPPA establish transparency requirements with respect to "personal information under the control of [an] institution that is organized or intended to be retrieved by [an] individual's name or by an identifying number, symbol or other particular assigned to the individual."

- the number of individuals whose DNA was subsequently collected on a voluntary basis and a non-voluntary basis
- the total number of arrests, charges, convictions, and exonerations
- the names of third party service providers used by the police during an IGG pilot project or program
- other information of public interest that may emerge[58]

10. Individual access and privacy rights

Individuals have a right to request access to, and correction of, their personal information.[59] They may also file a privacy complaint related to the collection, use, retention, destruction, disclosure, and safeguarding of their DNA and DNA-derived information for IGG purposes.[60] Police must ensure a process is in place to fulfill access and correction requests, as well as address any privacy complaints. That process should explain how individuals can exercise their access to information and privacy-related rights under FIPPA, MFIPPA, and other applicable laws. Police should also provide information on how individuals can file access requests or privacy complaints under those laws, including the contact information of the IPC to whom they can appeal if they are not satisfied by the initial police response. Consideration should also be given to providing information about redress mechanisms under, for example, legislation dealing with policing, victims' rights, and human rights.[61]

11. Public consultations

Police and their supervisory authorities should conduct meaningful public consultations with affected communities, equity-seeking groups, and interested parties before launching an IGG pilot project or program, and anytime significant changes are made to the program. Consultations, at a minimum, should include the intended scope, use, and objective for IGG, and how fundamental rights, including privacy and human rights, will be protected. In the case of current or ongoing IGG programs, public consultations should still occur even if police have not conducted this necessary engagement work during the early stages of launching or piloting their IGG program.

To align with constitutional rights and UNDRIP, police and their supervisory authorities should also assess and meet their responsibility to consult with First Nations, Inuit, and Métis peoples. Completing this step will help police and their supervisory authorities conduct the required consultations in a meaningful and culturally appropriate manner that advances our collective responsibility towards reconciliation.

58 See examples of reporting requirements under the federal **National DNA Data Bank** and the U.S. Department of Justice, ***Interim Policy Forensic Genetic Genealogical DNA analysis and searching***.

59 FIPPA, s. 47 and MFIPPA, s. 36.

60 FIPPA, s. 40.1(4)-(6), s. 49.0.1(1), and 59(f) and MFIPPA, s. 46(f).

61 CSPA; *Victims' Bill of Rights*, 1995, S.O. 1995, c. 6; and *Human Rights Code*, R.S.O. 1990, CHAPTER H.19.

12. Ethical disclosure guidelines

Police should develop ethical guidelines to ensure proper consideration is given to the effects of IGG on the rights and interests of the victim, persons of interest, and affected relatives, loved ones, and communities.[62]

Guidelines should inform police interactions with affected relatives to avoid needlessly or inadvertently disclosing sensitive personal information about a family member. This may require careful considerations regarding historical and cultural differences around how an investigation should be handled, the implications of police investigative questioning, and careful navigation of information about unknown biological relations obtained and discovered during an investigation.

Additional measures to support trust in police use of investigative genetic genealogy

To help ensure a consistent approach to IGG governance, the IPC recommends that three additional measures be implemented as soon as possible. Establishing these measures will require leadership from the government of Ontario and the involvement of police, regulators, and affected communities, among others. In particular, the IPC recommends that the government:

- Establish an independent, province wide IGG advisory committee with the requisite interdisciplinary expertise, akin to the National DNA Data Bank Advisory Committee.[63] This committee should include the IPC as an *ex officio* member and serve to provide general strategic guidance and overall direction on police use of IGG in Ontario.
- Localize IGG-related DNA sequencing to an accredited public forensic laboratory based in Ontario that is subject to Canadian law, including relevant access and privacy laws. Invest in sufficient research and operational resources to build genealogical expertise and capacity in Ontario, in compliance with forensic IGG standards, to reduce police reliance on services based in the U.S. or other jurisdictions.
- Hold regular, meaningful, and transparent consultations with Indigenous and other equity-seeking groups, privacy and human rights advocates, victims' rights groups, and other interested parties to ensure consideration and integration of a broad range of perspectives on the privacy and broader human rights impact that police use of IGG can have on affected individuals, groups, and communities in Ontario. Key learnings should be documented and communicated to the public.

62 Kim, J., Scully, J.L., Katsanis, S.H. (2016). *Ethical Challenges in Missing Persons Investigations*. In: Morewitz, S., Sturdy Colls, C. (eds) Handbook of Missing Persons. Springer, Cham.

63 **National DNA Data Bank Advisory Committee, Royal Canadian Mounted Police**.

Guardrails for Police Use of Investigative Genetic Genealogy in Ontario

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

2 Bloor Street East,
Suite 1400
Toronto, Ontario
Canada M4W 1A8

www.ipc.on.ca
416-326-3333
info@ipc.on.ca

June 2025