Submission to the Office of the Privacy Commissioner of Canada on draft guidance for processing biometrics

By Kate Robertson and Verónica Arroyo

FEBRUARY 16, 2024

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a "mixed methods" approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Contents

Dear Members of the Office of the Privacy Commissioner of Canada,

Re: Consultation on Draft Guidance for processing biometrics – for organizations and Draft Guidance for processing biometrics – for public institutions.

The Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto ("Citizen Lab"), is an interdisciplinary laboratory that focuses on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security. Our work relies on a "mixed methods" approach to research combining practices from political science, law, computer science, and area studies. Citizen Lab research has included, among other work: investigating digital espionage against civil society; documenting Internet filtering and other technologies and practices that impact freedom of expression online; analyzing privacy, security, and information controls of popular applications; and examining transparency and accountability mechanisms related to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

We welcome the opportunity to comment on the Office of the Privacy Commissioner's (OPC) helpful Draft Guidance for processing biometrics (including the versions for both public institutions and organizations) ("Draft Guidance"). For ease of reference, and given the overlap between the OPC's previous consultation regarding the use of facial recognition by police agencies, we are enclosing the previous submission by Citizen Lab researchers, Kate Robertson and Cynthia Khoo, on facial recognition technology. It is enclosed as **Appendix A**.

Our comments on the Draft Guidance are set out in the following recommendations, further elaborated below:

Recommendations

- **Recommendation 1: Under the "Biometric Technology" section, further elaborate the definition of biometric data, and include express reference to how biometric data is a form of personal information**
- **Recommendation 2: We recommend that the Draft Guidance provide further guidance in regards to how biometric data constitutes sensitive information**
- **Recommendation 3: We recommend that the Draft Guidance use the term "biometric data" as an alternative to "biometrics" where appropriate, including in defining sensitive information**
- **Recommendation 4: Review and potential clarification in regard to whether there is any interpretive significance to be attached to the sequence of the criteria used to assess the appropriateness of the biometrics program (i.e., Sensitivity, Necessity, Effectiveness, Proportionality, and Minimal Intrusiveness)**
- **Recommendation 5: Under the "Openness" section, incorporate public transparency and disclosure of which vendor a biometric processing technology was sourced from, if applicable**

Recommendation 1: Elaborate on the Definition of Biometric Data Under the "Biometric Technology" Section

Under the "Biometric Technology" section, further elaborate the definition of biometric data, and include express reference to how biometric data is a form of personal information

- We recommend that in elaborating the concept of biometric technology, the guidance should expressly include reference to how biometric data constitutes personal information[1]. For example, the European Union General Data Protection Regulation (GDPR) includes a short definition of biometric data in Article 4 (14), stating that it "means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person (...)". As such, this definition states clearly that biometric systems do not just process any type of data, but a specific type of personal information. In other words, we are dealing with data about an identifiable individual, who has the right to control how their data is processed.

---

1 For example, in the OPC's paper, "Data at Your Fingertips Biometrics and the Challenges to Privacy", dated February 2011, it states that "Biometric systems record personal information about identifiable individuals."

- We note, however, that in referencing Article 4(14) of the GDPR, we are not recommending that the current draft focus only on identification-focused biometric technology. We welcome the broadening of the definition of "biometrics", as defined in the current Draft Guidance, as going beyond only "unique" personal identifiers. Indeed, some biometric technology processes physical, physiological, or behavioural characteristics of a person which are not necessarily unique to that individual. In that regard, we welcome the draft's applicability to both biometric identification and categorization systems.

Recommendation 2: Biometric Data

We recommend that the Draft Guidance provide further guidance in regards to how biometric data constitutes sensitive information

- We would recommend reference to the following additional considerations when providing guidance in regard to the sensitivity of biometric data:

- Intrinsic or immutable characteristics: We recommend inclusion of the intrinsic or immutable nature of biometric data as a relevant factor that affirms its special sensitivity. While one may—albeit at great inconvenience and potential hardship—opt not to share the kinds of personal data collected through social media websites, or refrain from sharing personal information with a brick-and-mortar store, for example, it is not similarly possible to simply leave one's face, voice, gait, or DNA at home when going out in public. As noted in the Draft Guidance, in many instances, biometric data can be easily collected from individuals without their knowledge.

- The nature of the information that may be revealed by biometric data: We would recommend further elaboration of the discussion of the heightened sensitivity of the information that some forms of biometric data can reveal. Often, public debate regarding biometric data centers around its capacity to reveal individual identity. The current Draft Guidance recognizes, for example, that facial image data can be revealing of the individual's activities. We would encourage further elaboration of the nature of the other information that can be revealed by biometric data, including personal traits, demeanor, aptitudes, activities, health information, information about protected characteristics (such as race, disability, or gender identity or expression), and information about biological family relationships. With regards to the use of biometric data in conjunction with location monitoring, the use of biometric data processing can reveal highly sensitive information about the individual's activities, such as if they have "accessed particular types of healthcare, attended religious services, or attended political or union meetings." All this information is an intrinsic part of the person's private life. As noted in the OPC's Interpretation Bulletin: Sensitive

Information, the sensitivity of this information carries important implications for the level of protection that must be afforded to it under Canadian privacy law. While the availability of these types of inferences is referred to elsewhere in the Draft Guidance, we recommend it be specifically included in the Sensitivity section.

- Accessibility and exclusion: We also note that the sensitivity of the use and processing of biometric data may also be heightened by the fact that biometrics programs may be exclusionary for certain individuals or groups. For example, the World Bank notes that in deciding the set of biometrics to use, special attention needs to be given to issues of accuracy and accessibility, given the potential for biometrics programs to be exclusionary to some segments of the population. Their guidelines note the following potential exclusions:
    a. People who cannot physically provide an acceptable biometric (e.g., amputees, survivors of leprosy, etc.) to enroll in the first place
    b. People for whom acquiring reliable biometric samples is difficult (e.g., manual laborers, elderly people, children, people with visual impairment, persons with albinism, etc.) which could make enrollment or authentication difficult
    c. People who decline to provide their biometrics (e.g., because of religious or cultural constraints, such as the appropriateness of data capture techniques that require physical contact to get accurate readings).

- Family, community, and population-scale impacts: We urge for recognition that the privacy impacts of biometric programs may be felt not only at the individual level, but also at a family, community, or population-level scale. For example, the Draft Guidance refers to the use of DNA as a form of biological biometric. The use of DNA in biometrics systems is an particularly sensitive form of biometric data, not only because of the extent of the personal information contained in DNA, but also due to the overlapping privacy interests contained in DNA information that are shared within families and communities through a variety of data processing methods, including genealogy. For example, a 2018 study noted that "a genetic database needs to cover only 2% of the target population to provide a third-cousin match to nearly any person." It is now postulated that virtually all Americans of European descent are identifiable from their DNA profiles, due to the growing popularity of direct-to-consumer genetic testing services, even though only a fraction of that population has elected to participate in direct-to-consumer genetic testing. While family, community, and population-scale impacts are indeed relevant to the sensitivity of the biometric data, these considerations should also be noted under the proportionality analysis of the biometrics program.

- Risk of harm under human rights law: We recommend that the Draft Guidance include

express recognition of human rights risk as a potential form of "harm" mentioned in the "Sensitivity" section of the Draft Guidance. While it may well be commonly understood that human rights impacts may be a consequential form of harm occasioned by the inappropriate use of biometric data, we recommend that the Draft Guidance expressly acknowledge human rights risks as a potential harmful impact when considering the sensitivity of biometric data. As recently stated in the Joint Statement on Privacy and Democratic Rights, privacy is an essential precondition for other fundamental freedoms and is key for democracy. Therefore any interpretation of the recommendations should also consider the risks of exclusion, discrimination, surveillance, and chilling effects that a biometric system without safeguards and accountability can create. Since biometric data can easily help to distinguish people based on body characteristics, it facilitates the implementation of policies or actions targeted to specific people.

Recommendation 3: Defining the Term "Biometric Data"

We recommend that the Draft Guidance use the term "biometric data" as an alternative to "biometrics" where appropriate, including in defining sensitive information

- Both Draft Guidance documents state that "'Biometrics' refers to the quantification of human characteristics into measurable terms". Further, both documents state that "Biometrics are a category of sensitive information". We recommend that the Draft Guidance instead define and employ the term "biometric data", rather than only biometrics. Generally, biometrics only refers to the measurements and techniques to process human characteristics. As it refers to a field of endeavour, it does not inherently constitute a category of sensitive information. To further illustrate, according to ISO/IEC 2382-37:2022, the use of "biometric" as a noun to mean a characteristic is deprecated. Therefore, we suggest that the draft guidance instead use the term biometric data ("biometric data is a category of sensitive information").

Recommendation 4: Assessing the Appropriateness of the Biometrics Program

Potential clarification in regard to whether there is any interpretive significance to be attached to the sequence of the criteria used to assess the appropriateness of the biometrics program (i.e., Sensitivity, Necessity, Effectiveness, Proportionality, and Minimal Intrusiveness).

- We further recommend review and potential clarification in regard to whether there is any interpretive significance to be attached to the sequence of the criteria used

to assess the appropriateness of the biometrics program (i.e., Sensitivity, Necessity, Effectiveness, Proportionality, and Minimal Intrusiveness). We note, for example, that the sequence under the Draft Guidance differs from that employed in the OPC's Guidance on inappropriate data practices: Interpretation and application of subsection 5(3). In that instance, for example, the order of the topics for assessment was different, and placed the "proportionality" assessment at the end of the list. In some human rights frameworks, the overall sequence or structure of a framework can carry analytical significance if it intends to signal prerequisite conditions to further stages of analysis.

Recommendation 5: Incorporate Public Transparency Under The "Openness" Section

Under the "Openness" section, incorporate public transparency and disclosure of which vendor a biometric processing technology was sourced from, if applicable

- Under the Openness section, the Draft Guidance states: "Be open and transparent with individuals about how you manage personal information." This line sets the tone and the priority of openness in the entire section. In that sense, the "must" and "should" recommendations that follow are designed to provide information only to individuals, with the exceptions of the two recommendations regarding the post of the privacy policy for organizations, and specified public reporting for public institutions. Particularly given the potential for family, community, or population-level impacts, we recommend that the Draft Guidance incorporate recommendations to facilitate public transparency in order to better protect privacy and access to information rights. Having information disseminated publicly avoids allocating the burden about potential rights-infringing uses on individuals, and better enables democratic dialogue, meaningful accountability, and oversight to protect public trust.

- In this regard, we recommend more alignment with the OPC's guidance on the use of facial recognition, given it refers to the need for public transparency, as well as more specific disclosures surrounding the use of facial recognition technology. For example, in addition to disseminating information publicly, we also recommend that the Draft Guidance expressly refer to the need to disclose which technologies are in use (including which vendor the technology was sourced from, if applicable) when biometric data is collected or processed. The Draft Guidance for organizations does refer to the need to provide information in regard to processing of information by third party service providers. However, in some circumstances, the biometric data may be processed by a public institution or organization without sharing biometric data with a third party vendor. Nevertheless, it is important for individuals to know which technology is in use by public institutions or organizations given the potential

that there may be significant variances in accuracy, reliability, or bias between various biometric processing technologies.

- We also reiterate the additional transparency measures recommended in Part 3 of Appendix A to this submission.

Thank you for the opportunity to comment on the OPC's Draft Guidance. We appreciate the efforts that are being undertaken through the draft and consultation, and we hope that the aforementioned points will be useful in the development of the final version. We are available for any questions or further comments on the points raised above.

Contacts

Signed:

Kate Robertson, Senior Research Associate, Citizen Lab

Verónica Arroyo, Research Assistant at the Citizen Lab and privacy lawyer

Primary contact: Kate Robertson <kate@citizenlab.ca>

Appendix A

Kate Robertson and Cynthia Khoo, Submission to the Office of the Privacy Commissioner of Canada and the Information and Privacy Commission of Ontario regarding draft guidance for police services on facial recognition, dated October 22, 2021