Using voice printing for authentication purposes – takeaways from the Rogers decision

October 24, 2022

Faced with ever-increasing risks of fraud, a growing number of organisations, including banks and telecom companies, are considering implementing voice-printing technologies to authenticate their customers. A voiceprint is a digital model of an individual's unique vocal characteristics and is considered biometric data. As such, it can be used as an " audible fingerprint" to identify or authenticate a person, using a biometric analysis. Contrary to passwords and traditional identifiers, which are increasingly subject to data breaches and hence available to threat actors, voice printing technologies rely on biometric information which are by nature unique to an individual and can hence provide an enhanced level of security.

However, voiceprint authentication technologies can also be perceived as a privacy-intrusive practice by concerned individuals, as evidenced by a decision issued earlier this year by the Office of the Privacy Commissioner (OPC) against Rogers Telecommunications Inc. (Rogers) (PIPEDA Findings #2022-003).

In addition to regulatory risks, we note that the unlawful use of biometric technologies is a fertile ground for class actions, as illustrated by the numerous class actions filed recently in the Southern District of California against banks using voice printing for customer authentication purposes and by the first decision on the merit applying the Illinois Biometric Information Privacy Act, which pertains to the use of employees' fingerprints for identification purposes (awarding USD 228 million in damages against their employer).

To assist organisations navigating this evolving legal landscape and mitigate associated risks, this article summarizes findings of the Rogers decision and provides compliance tips to be considered prior to implementing a voice printing authentication program.

The Rogers decision (PIPEDA Findings #2022-003)

In the Rogers case, a complaint was filed by a customer who alleged that she had improperly be enrolled in Rogers' voiceprint-based biometric authentication program, Voice ID. Specifically, despite having declined consent when asked by a Rogers customer service representative (CSR) during a first call, the claimant found out during a second call that she had been enrolled in Voice ID. She stated her desire to opt-out and

to have her voiceprint deleted. The voiceprint was deleted as per her request but several months later, after a "third call"; she was enrolled again in the Voice ID program. Rogers once again deleted the voiceprint and removed her from the program.

The OPC decision provides first an analysis of active voice (using a passphrase repeated several times by the individual, which the software analyses to create a voiceprint) and passive voice (which runs in the background of al call and builds a general algorithmic pattern of the individual's voice and speech) authentication technologies to explain that Voice ID being a passive voice technology, it could be used by Rogers in a covert manner. A third party supplier, Nuance FreeSpeech, provides this technology.

To collect voiceprints, the solution engages in a "tuning" process after the customer passed through Rogers' interactive voice response system (during which they answer questions regarding the purpose of their call and identify their account). If no existing voiceprint is associated to the account, the CSR is presented with an option to proceed to enrolment after manually authenticating the customer. Pursuant to Rogers' policy and training documentation, the CSR must explain the Voice ID program to the customer and obtain their express consent before associating the voiceprint to the account.

If the customer does not opt-in, the "tuning" voiceprint is discarded and no voiceprint is retained. Conversely, if a customer who has previously enrolled, subsequently chooses to opt-out, the voiceprint is retained in Rogers' system for "security purposes".

After a voiceprint has been associated to the account, the software uses this pattern to attempt to authenticate callers during subsequent calls in relation to that account. When matching a caller's voice to the voiceprint database, it applies a "confidence interval", indicating the closeness of the match. If the voice matches the voiceprint, the system will authenticate the user ("one to one check"). If a negative or "mismatch" response is returned, the system conducts a one-to-many check against a separate "fraud database" consisting of voiceprints from callers whom Rogers has identified, after a review by its fraud team, to have fraudulently enrolled in the Voice ID program on another individual's account ("one to many check").

The complainant alleged that Rogers used Voice ID for an inappropriate purpose. She also claimed that Rogers failed to obtain valid and meaningful consent to the collection and use of her voice samples and did not provide an adequate mechanism for the withdrawal of consent.

The OPC concluded that the purpose for which Rogers implemented the proposed authentication program was reasonable. However, it also found that Rogers had failed to obtain valid and meaningful consent and to comply with other requirements. These findings can be summarized as follows:

- **Securing accounts and combatting fraud constituted an appropriate purpose.** Reinforcing the security of Rogers' customer authentication program by using Voice ID was for an appropriate purpose under section 5(3) PIPEDA. To reach this conclusion, the OPC applies its four-part reasonableness test:
  The decision carefully highlights the specificities of threats faced by telecom companies and the seriousness of harms resulting from a misuse of consumers' accounts.

1. that using Voice ID as an additional measure to secure its customers' accounts was a legitimate need and a bona fide business interest of Rogers;
2. that the solution, presented as being 99 per cent accurate, was likely to be effecting in achieving such purpose;
3. that no other less privacy-invasive option providing comparable results were available to Rogers; and
4. that the loss of privacy for individuals was proportional to the benefits provided by the solution.

- **Express consent was required to collect and use voiceprints** . The OPC concludes that Rogers failed to obtain meaningful consent from its customers. Specifically, express consent from customers was required in advance of "tuning", as well as enrolment, since:

1. voiceprints represent sensitive biometric information; and
2. an individual would not, when calling Rogers, reasonably expect their voice to be captured and used to create a biometric representation of their voice. The OPC points out that the potential benefits of Voice ID does not relieve the organization from its obligation to obtain express consent.

- **Transparency requirements.** The decision also criticizes Rogers for failing to adequately inform its customers about the use of Voice ID and of its opt-out process. Rogers was relying on an on-line recorded message indicating that "recordings" can be used for "identification purposes" and described the mechanism to opt-out in a "Frequently Asked Questions" document on its website. The OPC concluded that such an approach was not meeting applicable requirements regarding meaningful consent.
- **Voiceprints must be deleted upon consent withdrawal** . Retaining voiceprints after opt-out on the basis that Rogers may be using them for security purposes (which did not occur) was unlawful. The OPC indicates that Rogers should have deleted the voiceprints immediately upon opt-out.
- **Customer-facing employees must be appropriately trained.** Finally, the decision emphasizes that Rogers had not implemented adequate training materials and failed to monitor its customer service representatives to ensure that they were respecting express consent and opt-out protocols. The OPC insists on the fact that such measures are particularly important when consent is obtained orally by employees who may face pressure related to speed or customer satisfaction.

In response to the OPC's recommendations, Rogers agreed to obtain express consent from individuals before tuning going forward; more clearly inform customers of their ability to opt-out; delete voiceprints of individuals who previously opted out of Voice ID; implement significant changes to its process documents and training, as well as associated monitoring to ensure compliance; and reconfirm consent for previously enrolled individuals as they call in.

Compliance tips

In light of the Rogers decision and of past cases and guidance pertaining to biometrics, organizations seeking to implement a voiceprint program to authenticate individuals should consider the following steps:

1. Involve the organization's privacy office in the early stages of the proposed program.
2. Conduct a privacy impact assessment to assess the reasonableness of the proposed program in light of the OPC Guidance on inappropriate data practices: Interpretation and application of subsection 5(3). Such PIA should involve the supplier of the voice printing technology (if sourced from a third party).
3. Be transparent about the use of such a technology by providing a meaningful explanation about the creation and use of voiceprints, in line with the OPC Guidelines for obtaining meaningful consent.
4. Obtain express consent of concerned individuals prior to the collection of any voice sample, and ensure that consent is sought separately from other information.
5. Make the voiceprint program optional (without being denied a service or being subject to restrictions/sanctions) and provide an easily accessible option for individuals to opt-out of the collection and use of their voiceprint.
6. Ensure that voiceprints are immediately deleted upon opt-out (unless they are used for another lawful purpose) and that this retention/deletion requirement is reflected in the organisations' retention policy.
7. Provide customer-facing employees who are tasked with enrolling customers in a voiceprint program with adequate protocols and training, which must be sufficiently clear and precise. Compliance with such protocols must be monitored by the organization (see on this point the recent Fido decision PIPEDA Findings #2021-004).
8. Ensure the robustness of the applicable security measures, whether maintained by the organisation and/or its supplier.
9. Finally, if a voiceprint program is deployed in the province of Québec, file a declaration with the Commission d'accès à l'information prior to its activation, in accordance with sections 44 and 45 of the *Act to establish a legal framework for information technology*. We refer to our recent bulletin on this topic.

By

Elisa Henry, Daniel-Nicolas El Khoury

Expertise

Banking & Financial Services, Cybersecurity, Privacy & Data Protection, Financial Services

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749