Office of the Information and Privacy Commissioner for British Columbia

2025/26 - 2027/28 Strategic Plan

Trust in the Age of Information

oipc

OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

October 2025

WHO WE ARE

Established in 1993, the Office of the Information and Privacy Commissioner provides independent oversight and enforcement of BC's access and privacy laws, including:

•The *Freedom of Information and Protection of Privacy Act* (FIPPA), which applies to over 2,900 public bodies, including ministries, local governments, schools, crown corporations, hospitals, municipal police forces, and more; and

•The *Personal Information Protection Act* (PIPA), which applies to any private sector organization (including businesses, charities, non-profits, and political parties) that collects, uses, and discloses the personal information of individuals in BC. PIPA also applies to any organization operating in BC that collects, uses, or discloses personal information of any individual inside or outside of BC. PIPA does not apply to federal works, undertakings, and businesses.

Michael Harvey is BC's Information and Privacy Commissioner.

The Office of the Information and Privacy Commissioner for BC respectfully acknowledges that its offices are located on the traditional territories of the Lekwungen people of the Songhees and Esquimalt Nations.

As an Officer of the Legislature, the work of the Commissioner spans across British Columbia, and the OIPC acknowledges the territories of First Nations around BC and is grateful to carry out our work on these lands.

TABLE OF CONTENTS

Commissioner’s message 4

Transparency & Information in Today’s BC 8

Plan at a glance 9

Strategic priorities 10

Trust and transparency 12

Trusted innovation 14

Enhancing rights 16

Moving forward 18

Resources 20

What we heard 22

COMMISSIONER’S MESSAGE

I arrived in British Columbia and was sworn in as Information and Privacy Commissioner a little more than a year ago. Since then, I have been impressed by information and privacy professionals, inside the OIPC and in other organizations, working in an environment of rapidly changing and increasingly complex technology. The sheer pace of changing technology which touches every part of the office’s mandate under the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act* sometimes means that we are tempted to chase after every new emerging problem. Yes, we need to be responsive and agile, but we also need to be coherent. Focus is called for with the broad scope of the office’s mandate – covering both transparency and privacy, and almost every sector of our economy and society.

This strategic plan, in many instances, does not reflect new work being undertaken by the office. While there are certain new focus areas that have emerged, more often, strategic planning drew out themes that cut across our work. These kind of themes are sometimes easy to see at the executive level, but difficult to implement coherently across a complex organization. Strategic planning has helped us draw out those themes that unite us all in our common mission – like trust, transparency, maximizing the benefits of emerging technologies, the importance of rights, and the need for equity – and help us identify coordinated actions. In this way, our strategic plan is intended to help us advance our mandate as a team.

The way that we have developed this plan is almost as important as the plan itself. Its priorities are not simply the Commissioner’s priorities, but “our” priorities. And here our is intended to mean the entire staff of the OIPC – we developed this plan with the involvement of all staff and the office’s senior leadership over a number of months and using multiple methodologies, and then validated what we came up with.

“Our” is also meant to mean the people of this province. For my first year, I engaged in an intentional but informal engagement, meeting with all manner of people, including politicians and public officials, businesses, professional associations, civil society organizations, students and academics. Starting in the spring of this year I pivoted to a more open and transparent formal engagement, inviting online submissions and travelling the province to seven different cities. In this way I was able to appreciate British Columbia in its diversity. The priorities in this plan reflect what I have heard people living in British Columbia, across many walks of life, identify about what matters to them in the areas of transparency and privacy.

People are concerned about how fast technology is changing and what that means for our society.

People that have kids, are kids, or were kids all were united in wanting to protect the children and youth of British Columbia online. Where once it was observed that our youth are spending increasing amounts of their time online, now even this idea – that there are distinct offline and online worlds – seems outdated. The online world for our kids, just as for all of us, is integrated into every aspect of our lives. The new technologies that are available to them open up possibilities that we could barely have dreamt of when we were children ourselves. But much of the promise of the internet involves the collection and use of their personal information in ways that we now know can cause great harm.

We want to make sure that these new technologies work for our kids rather than the other way around. Proper childhood development requires autonomy. We owe our kids nothing less.

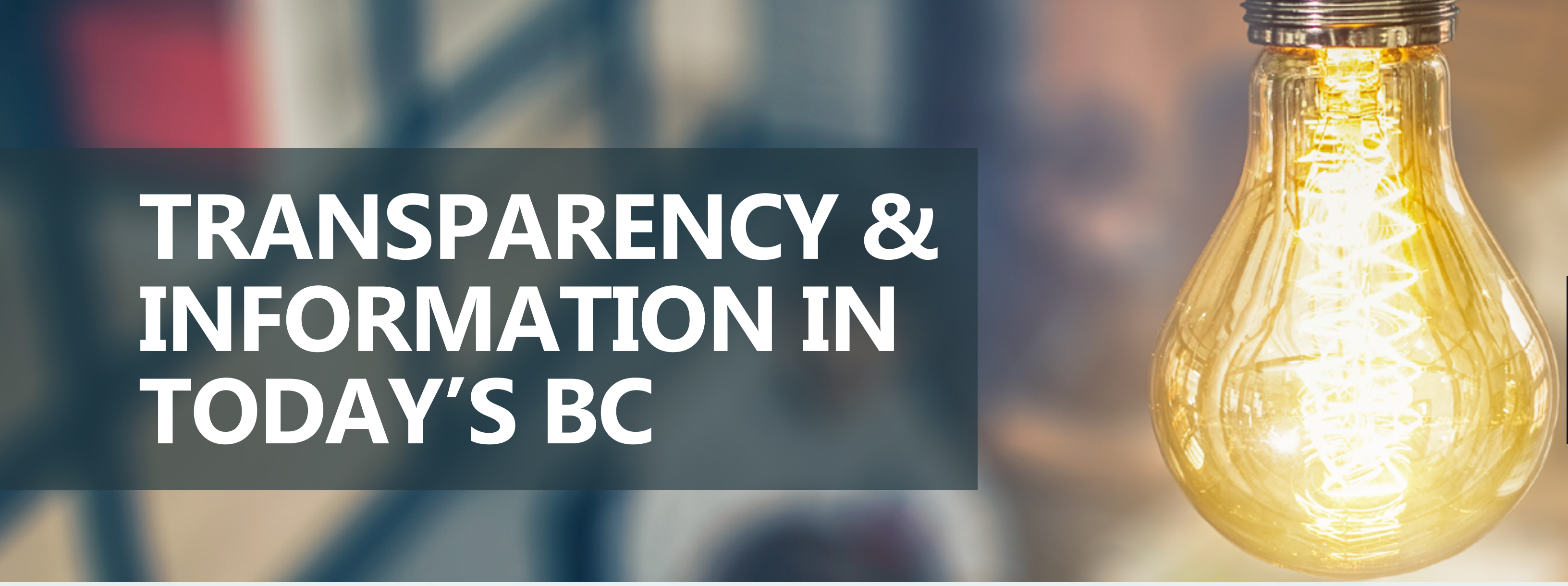
And this unease extends to other domains. We heard concerns about how transparent public bodies are. This resonates with a number of investigations that the OIPC has done that have found that FOI system implementation is not meeting the aspirations of FIPPA for public bodies such as government departments, health authorities, post secondary institutions and municipalities. At the same time we know that we can be doing better to improve the timeliness of our own operations.

Playing into this is a sense that technology may be slipping out of our control. Artificial Intelligence is changing the landscape of the Information Society by changing the way that a computing system works at its very nature: the way that algorithms change themselves over time based on many iterations of inputs and outputs means that our visibility into how they work – their transparency and thus our accountability – can not work in the same way that it used to. Also, these systems are voracious for data to train and refine their systems, and much of this data is personal information. There is excitement about the potential of AI to transform our economy and public services. We share it, and indeed are exploring how to use these technologies ourselves. But we also share concern about whether we have the statutory and regulatory tools to make sure that, to echo the notion above, AI works for us rather than vice versa.

A final sense of unease that we encountered was not one that I expected to be a hot topic – video surveillance. People in British Columbia, in communities large and small, and from our hospitals to our schools to stratas and street corners and retail stores, are concerned about social disorder. Their concerns are real and valid. In many instances, increased surveillance has been proposed as a solution. But as often as it is raised as a solution, it has been identified as a problem. There is little question that there are certain situations in which certain surveillance technologies – with the right use cases – can be appropriate and proportionate. However, we have known for generations that an over-surveilled society is one in which the social fabric will begin to fray. Moreover, today's technologies are far more powerful than they once were. Only a few years ago if there was a drone that could see you, you could see it and know someone was looking at you. Now it's possible for a drone to see you with high enough resolution to use facial recognition technology and read your body's temperature, from far enough away so that you don't see it.

British Columbia is one of the most prosperous and advanced provinces in one of the most prosperous and advanced countries in the world. We have it within our abilities to respond to the transformations that our world is experiencing today to build the society that we want to live in, and for the next generation. We should together be striving for a society that has a strong level of trust built on a foundation of democratic accountability and individual, equitable autonomy. The OIPC is committed to do its part. This three-year plan is intended to take us down that path. We are privileged to be walking it with British Columbians.

Michael Harvey
Information and Privacy Commissioner
for BC



TRANSPARENCY & INFORMATION IN TODAY'S BC

The OIPC's understanding of the operational context against which this plan is set is based on feedback received throughout an internal and external engagement process that occurred in the first half 2025. The external process included an in-person seven-city listening tour and a written submission component that sought feedback from anyone interested in providing insight as to what they think the OIPC's priorities should be in the next three years.

Need for enhanced trust in social/economic/political systems

- Political polarization, a decline in the civility of discourse, a surge in demand for OIPC services, and the spread of misinformation and disinformation reflect a fraying of political trust in our society. Transparency is needed to build trust for people in British Columbia - in their political systems, and in knowing what the public bodies who serve them are doing.

Need for legislative reform

- BC can no longer wait to follow the federal government's lead on modernizing provincial privacy and access laws to deal with challenges brought on by growing mistrust in institutions and rapid technological change.

Rapid pace of technological change

- Technological innovation is redefining all aspects of our society and the collection, use, and disclosure of personal information is at the center of this change. British Columbia has an opportunity to support trusted private and public sector innovation through entrepreneurship and investment - and ultimately excellence in public service delivery. British Columbia must act to support this economic development through strategic regulatory infrastructure.

Resource constraints

- Economic pressures, and a charged environment that demands greater accountability and transparency mean that people on the frontlines of privacy and access are often left feeling overwhelmed and under-resourced. These challenges are especially daunting for small or medium sized organizations and public bodies.

High demand for OIPC education/services

- The OIPC works with public bodies, private sector organizations and the public to provide guidance and support around areas including what new technologies mean to people's privacy rights, minimizing damage and strengthening systems following privacy breaches, and accountability around FOI responses.

- Rapid technological changes mean that privacy complaints and the office's own investigations and adjudications involve more complex issues that require specialist knowledge.

PLAN AT A GLANCE

VALUES

Impartiality Expertise Dedication Respect Innovation

VISION

A province where people in BC have protection of their rights to access to information, privacy, and transparency, and that those protections enable them to achieve their aspirations and participate in a democratic society.

STRATEGIC PRIORITIES

Trust & transparency

Goals

- Timely and effective regulatory oversight
- Promote transparency through timely FOI management by public bodies
- Foster resilient and trusted institutions in a changing world

Trusted innovation

Goals

- Support organizations in adopting privacy-aware approaches to:
  - AI
  - surveillance technologies
  - digital health tools

Rights equity

Goals

- Enhance the privacy rights of children and youth
- Promote Truth and Reconciliation with Indigenous peoples
- Promote an inclusive and equitable approach to privacy and access rights

STRATEGIC PRIORITIES

Strategic Priority 1

Trust and Transparency

A healthy democracy is based on strong levels of trust in public institutions. This trust is fostered when people feel like they can know how their public bodies are working in their interests, that their concerns are heard, they can make a difference, and that there is accountability.

Trust therefore requires transparency. In challenging times at home and internationally, economically, socially and politically, shoring up trust through transparency needs to be a top priority for all of us. It is a strategic priority of the OIPC to promote greater transparency by encouraging public bodies to be transparent by default in their policy and program design; to publishing as much information about their activities with maximum accessibility, and to effectively administering the freedom of information system as required by the law.

For our part, an effective FOI system is backstopped by effective, high quality, and timely regulatory oversight that prompts public bodies to meet their obligations and provides individuals with an opportunity for review of FOI decisions to confirm that they are compliant with the law, and recourse when they wish to complain if there has been a lack of compliance. Effective regulatory oversight of public and private organizations and compliance with the privacy parts of the act is also critical for promoting trust through transparency

Goal 1: Timely and effective regulatory oversight

- People are increasingly concerned about their access and privacy rights and are seeking out the office's services more than ever before.

- As the volume of cases coming before the office increases and grows in complexity, the OIPC is committed to continuous improvement to respond to those demands in a timely and efficient manner.

- The office will continue to refine its internal systems for efficiency, build on early resolution successes, and enforce policies that prevent any one individual from overwhelming the OIPC's resources at the expense of other people's rights.

Strategic Priority 1

Trust & Transparency

Goal 2: Promote transparency through timely FOI management by public bodies

- OIPC investigations and audits have found that many public bodies are failing to meet their basic obligations under the *Freedom of Information and Protection of Privacy Act.*

- The office will focus on challenges in areas often involving small public bodies, health authorities, and post-secondary institutions, where access requests are often most frequent and critical to people's everyday lives.

- The overarching aim is to encourage a culture where transparency is the default, and to see that priority reflected at all levels of a public body's operations, including from service design to delivery.

Goal 3: Foster resilient and trusted institutions in a changing world

- British Columbia is the only jurisdiction in Canada where political parties' personal information practices are regulated by the privacy commissioner.

- The OIPC will continue to prioritize its efforts as the lead regulator in this important area, as part of our office's wider efforts to foster accountability in election campaigns and our wider democratic process and institutions.

- The OIPC will also work with other regulators across Canada and through national, regional, and international forums to strengthen our democracy by bolstering trust in public institutions.

Summary of where we will start

- Examine internal workflows to identify continuous improvement opportunities

- Review internal processes for issues that require extensive OIPC resources

- Review and support compliance of public bodies, specifically small municipalities, post-secondary institutions, and health authorities

- Advocate for measures that broadly support greater trust and transparency in democratic institutions

Strategic Priority 2

Supporting trusted innovation for a strong economy and excellence in public services

We are now a quarter century into a millennium that has been dominated by a transition to an economy and society that is centred around the exponentially increasing creation, collection, and use of vast amounts of information about individuals. In the Information Society, information about us is everything. We need to harness these technologies to make sure that they work for us... rather than us working for them.

Privacy is about control of our information - and that is what makes us free and autonomous, rights-bearing individuals. Without transparent, inclusive, and independent governance and effective oversight, there is risk that these technologies will, instead of enabling us to have greater control over our destinies, be used to control us. As part of BC's critical regulatory infrastructure we will focus on developing strategic foresight to support trusted innovation in the public and private sector in priority domains of Artificial Intelligence, surveillance and digital health.

Goal 1: Support organizations in adopting a privacy-aware approach to AI

- Artificial intelligence offers significant benefits for public service delivery and BC's economy, but also challenges basic privacy principles, such as obtaining proper legal authorization to collect and use personal information to train algorithms and promoting transparency and accountability in how personal information is used by them, particularly as they learn and adapt over time.
- The OIPC is committed to working with public bodies, organizations, and other regulators to so that AI develops along the right track – one that empowers innovation to benefit people in BC, while protecting people's privacy rights.

Strategic Priority 2

Trusted Innovation

Goal 2: Support organizations in adopting a privacy-aware approach to surveillance technologies

- Surveillance technologies such as facial recognition and CCTV systems are becoming more common and more advanced in both public and private spaces due to social challenges and safety concerns.
- The OIPC recognizes these pressures and that these systems have valid uses in defined and limited circumstances. However, history tells us that an over-surveilled society is one in which the social fabric gets frayed.
- The OIPC will continue to work with private organizations and public bodies so that the use of these systems is justified, limited, and proportional to the need addressed, rather than used as a default response to more complex social issues.

Goal 3: Support entities in adopting a privacy-aware approach to digital health tools

- Through transparent, independent, and inclusive governance and effective oversight, there is an opportunity to maximize the value of digital health while increasing the control and autonomy that people have over their personal health information. This can build trust for the maximal use of health data for clinical purposes and the public benefit by authorized users for health system improvement, research and innovation.
- The OIPC will work with public bodies and private sector health organizations to review programs and develop practical guidance that supports innovation in healthcare, while confirming that sensitive health information is protected.

Summary of where we will start

- Develop internal capacity to understand the challenges and obstacles to support tech innovation
- Review and prioritize outreach, education, and engagement strategies for AI, surveillance technologies, and digital health tools
- Advocate for legislative reform that accounts for the use of changing technologies in a way that protects privacy

Strategic Priority 3

Enhancing rights equity

Privacy and access rights are based in statutes, and have been recognized by the courts as either constitutional or quasi-constitutional. At the OIPC we consider them fundamental in our democratic society because they provide the basis for, respectively, our individualism and our ability to exercise our constitutional democratic rights. And while all individuals enjoy equal rights before the law in our society, we know that in reality there are people in our society that, for a variety of reasons, are not able to exercise these rights equitably.

Some, such as children and youth or seniors, are more vulnerable to having their privacy rights violated. A person's home has often been considered a private domain - but people without stable housing face entirely different privacy considerations. With respect to access, some are very capable of understanding how to navigate the freedom of information system and other avenues to get access to their own information and public information, while others face much greater challenges. It is a priority for the OIPC to advance equity in rights protection and empowerment for all people of this province. We will start with a concerted effort on the privacy rights of children and youth.

Further, our colonial past has left a legacy where the Indigenous people in this province do not have adequate ownership, control, access, or protection of their information. It is a priority for the OIPC to explore how we can support Indigenous peoples in their aspirations for Indigenous data sovereignty as we pursue the goals of Truth and Reconciliation so that Canada can achieve its full potential.

Goal 1: Enhance the privacy rights of youth and children

- The majority of websites and apps targeting children and youth use deceptive design techniques to manipulate them into sharing more personal information than necessary.
- The office will center compliance efforts on identifying and addressing violations of children and youth's privacy rights under existing laws, while advocating strongly for legislative amendments to better address their needs.
- The OIPC is also committed to learning directly from young people about their challenges and views on privacy.

Strategic Priority 3

Rights equity

Goal 2: Promote Truth and Reconciliation with Indigenous peoples

- True reconciliation with Indigenous peoples requires ongoing learning and changes in how services are delivered to these communities.
- The OIPC is committed to deepening staff's knowledge on Indigenous rights issues, and particularly in learning more about Indigenous legal processes and data sovereignty principles.
- The OIPC aims to move beyond understanding to action by developing working relationships to support the aspirations of Indigenous peoples for Indigenous Data Sovereignty.

Goal 3: Promote an inclusive and equitable approach to privacy and access rights

- Privacy and access rights are for everyone in BC regardless of their background, personal circumstances or the barriers they face in exercising their rights.
- The OIPC is committed to removing language barriers to our services, improving accessibility, and letting people know about and understand how we can support them.
- The OIPC is committed to listening and learning from groups including seniors, people new to the province, unhoused communities, and others who may have challenges exercising their rights.

Summary of where we will start

- Prioritize enforcement, engagement, and advocacy on issues related to children and youth
- Develop working relationships to support aspirations of Indigenous peoples for Indigenous Data Sovereignty
- Identify key access and privacy needs of key demographics including seniors, new Canadians, persons with disabilities, incarcerated individuals, and unhoused populations

MOVING FORWARD

Over the next three years, the OIPC will prioritize initiatives, investigations, education, and enforcement actions that align with the strategic priorities set out in this document.

This plan serves as a high-level road map for the work of the office, and is not intended to reflect or limit individual objectives or actions associated with the plan. We have identified actions for each goal in the plan for this first fiscal year, and will report out on our progress in our Annual Report and Service Plan.

The OIPC would like to thank everyone who participated in our consultation period that laid the foundation for this report, including those who attended in-person sessions around BC in May. A summary of those consultations, in the form of a *What We Heard* review, can be found at the end of this document.

N
NE
E
SE
S
SW
W
0
20
40
60
80
100
120
140
320
340

RESOURCES

Getting started

- Access to data for health research
- BC physician privacy toolkit
- Developing a privacy policy under PIPA
- Early notice and PIA procedures for public bodies
- Guide to OIPC processes (FIPPA and PIPA)
- Guide to PIPA for business and organizations
- Privacy impact assessments for the private sector
- Privacy management program self-assessment

Access (General)

- Common or integrated programs or activities
- Guidance for conducting adequate search investigations (FIPPA)
- How do I request records?
- How do I request a review?
- Instructions for written inquiries
- PIPA and workplace drug and alcohol searches: a guide for organizations
- Proactive disclosure: guidance for public bodies
- Requesting records of a deceased individual
- Section 25: The duty to warn and disclose
- Time extension guidelines for public bodies
- Tip sheet: requesting records from a public body or private organization
- Tip sheet: 10 tips for public bodies managing requests for records

Privacy (General)

- Direct-to-consumer genetic testing and privacy
- Disclosure of personal information of individuals in crisis
- Employee privacy rights
- Guide for organizations collecting personal information online
- Identity theft resources
- Information sharing agreements
- Instructions for written inquiries
- Obtaining meaningful consent
- Political campaign activity code of practice
- Political campaign activity guidance
- Privacy guidelines for strata corporations and strata agents
- Privacy-proofing your retail business
- Privacy tips for seniors: protect your personal information
- Private sector landlord and tenants
- Protecting personal information away from the office
- Protecting personal information: cannabis transactions
- Reasonable security measures for personal information disclosures outside Canada
- Responding to PIPA privacy complaints
- Securing personal information: A self-assessment for public bodies and organizations

Comprehensive privacy management

- Accountable privacy management in BC's public sector
- Getting accountability right with a privacy management program

Privacy breaches

- Privacy breaches: tools and resources for public bodies
- Privacy breach checklist for private organizations
- Privacy breach checklist for public bodies
- Privacy breaches: tools and resources for the private sector

Technology and social media

- Guidance for the use of body-worn cameras by law enforcement authorities
- Guidelines for online consent
- Guidelines for conducting social media background checks
- Mobile devices: tips for security & privacy
- Tips for public bodies and organizations setting up remote workspaces
- Use of personal email accounts and messaging apps for public body business

Infographics

- FIPPA and the application fee
- How to identify deceptive design patterns
- How to make a complaint
- How to make an access request
- How to request a review
- Identifying and mitigating harms from privacy-related deceptive design patterns
- Responsible information sharing in situations involving intimate partner violence
- Requesting records of deceased individuals
- Tips for requesting records
- Transparency by default: information regulators call for a new standard in government review

LISTENING, LEARNING & PLANNING

What we heard from stakeholders and staff to inform strategic direction for the OIPC and the ORL

Prepared for

The Office of the Information and Privacy Commissioner for British Columbia
and the Office of the Registrar of Lobbyists

Prepared by

Hayden Public Relations

July 31, 2025

Introduction

This report summarizes input gathered through a province-wide, external and internal engagement process led by the Office of the Information and Privacy Commissioner for British Columbia (OIPC) and the Office of the Registrar of Lobbyists (ORL). It is intended to inform the development of a new multi-year strategic plan for both offices.

The insights aim to reflect what was shared by stakeholders, expert advisors, written contributors, members of the public and staff. These voices brought a wide range of perspectives on the OIPC and ORL's work to advance privacy, access to information and lobbying transparency, as well as the role of oversight in a challenging and changing environment.

This report is not a strategic plan, nor does it represent final decisions. It is a tool: an account of the input received, along with recommendations, to support the Commissioner and his team in determining their priorities in the years ahead.

About the OIPC and ORL

The OIPC and the ORL are independent Offices of the Legislature, both led by Commissioner Michael Harvey. The OIPC provides oversight of access to information and privacy compliance across more than 2,900 public bodies under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and oversees privacy obligations in the private sector under the *Personal Information Protection Act* (PIPA). The ORL is responsible for enforcing the *Lobbyists Transparency Act* (LTA) and maintaining the public registry of lobbying activity in the province.

The OIPC operates with the vision of a community where privacy is respected in both public and private sectors, access to information rights are robustly exercised, and public institutions are open and accountable. Its work is guided by five core values: impartiality, expertise, dedication, respect and innovation. Work is guided by those served, including the public, the Legislative Assembly of British Columbia, public bodies and organizations covered by FIPPA and PIPA, and lobbyists and public office holders under the LTA. Although each office has a distinct legislative mandate and publishes separate annual reports and service plans, they operate with shared leadership and collaborate in areas such as staffing, planning and digital infrastructure.

Context

Commissioner Michael Harvey was appointed in May 2024 to lead both the OIPC and the ORL. In the months that followed his appointment, Commissioner Harvey focused on understanding the organization, the environment and the communities served. He then launched a strategic planning initiative centered on listening to a wide range of groups including staff and expert advisors, local and provincial governments, civil society organizations, professional associations, Indigenous-serving organizations, journalists, small businesses, academics and members of the public.

During the spring and summer of 2025, the OIPC and ORL carried out an extensive engagement process. This included a multi-city listening tour, internal planning sessions, staff team interviews, an external advisory board meeting, stakeholder conversations, written submissions and an environmental scan.

The planning process underway is an opportunity to shape a multi-year strategic direction for both offices that reflects the current privacy, access and transparency landscape in British Columbia. The process was designed to consider and reflect on the dual mandates and bring in perspectives from across the province, including voices not always heard in public policy work. The OIPC and ORL wanted to know what issues and risks to pay attention to, where there are barriers to compliance and how their oversight, guidance and enforcement could be more effective. They asked about what is working well, where laws or processes are unclear and what support is needed to help people understand and exercise their rights. They also invited perspectives on how to improve public trust, reduce burdens for smaller organizations and make their work more inclusive and responsive across different regions and communities.

This report is based on a close review and analysis of the input via notes, transcripts and written materials from all engagement activities. We start by focusing on what we heard and learned, organized by theme, and then make recommendations.

What we heard and learned

Strains on the FOI system are undermining trust and transparency

Across listening tour sessions, written submissions, stakeholder interviews and internal reflections, participants described a FOI system under strain, one that too often fails to support timely or meaningful access. While many continued to express strong support for the right of access, they said delays, inconsistent processes and unclear outcomes are undermining trust in how the system works. These concerns were especially acute for people trying to access their own information. The OIPC's 2024-25 Annual Report reflects this challenge and notes the importance of embedding "transparency by default" into government decision-making and service delivery.

The most consistent concern was delay. Individuals, families, advocates and public servants described requests for records taking months (or sometimes years) to be resolved. There was particular concern about how long it takes to access personal information. In areas like child welfare, health and education, participants said delays can undermine advocacy, decision-making and trust in public institutions. Internal analysis confirmed the scale of the problem. One public body accounted for over a quarter of all government time extension requests last year, and across the system, the number of deemed refusals continues to rise.

Several participants said that FOI laws are increasingly used in ways that depart from their intended purpose. Some said requests are being weaponized, filed strategically to intimidate, punish or burden. Others raised concern that access rights are used by individuals in situations involving complex legal circumstances, which can overwhelm small teams or be difficult to manage compassionately. These issues were especially pressing in smaller public bodies, where a single request or applicant could generate hundreds of pages of records and weeks of work.

> There may be some value in assessing the barrier in allowing those types of requests to stand out, not as a way to end transparency for those who have legitimate requests, but the frequent flyers make it difficult for everyone else trying to exercise their rights.

At the same time, participants raised equity concerns. Several noted that the FOI system can be difficult to navigate for some people, such as those with low literacy or disabilities.

Others said the process favours those with resources, especially when cost estimates are used as a deterrent. Some journalists described being treated as commercial applicants or facing inconsistent fee calculations. Others said that high estimates, combined with long timelines, make it hard for FOI to be used effectively for public-interest accountability. Internal and external voices also raised concern about how FOI laws are being interpreted. Several said that some public bodies apply provisions of FIPPA too broadly or inconsistently, limiting access without clear justification. Participants asked whether stronger expectations, clearer definitions or centralized guidance might help ensure that disclosure decisions are applied more consistently across the system.

There were also repeated calls to reduce burden at the source. Some suggested expanding proactive disclosure obligations to reduce the need for routine FOI. Several said that the current system is neither sustainable nor fair — placing significant strain on public servants without improving outcomes for the people seeking access.

Organizations have difficulty keeping up with advances in technology

Across consultations, submissions and internal planning sessions, participants raised concerns that new technologies are being introduced faster than organizations can confidently respond to them. Privacy laws remain broadly applicable, but the tools and interpretation frameworks available to apply them are not keeping pace. The input all pointed to the same core problem: systems for managing privacy risk have not evolved as quickly as the technologies driving that risk.

Artificial intelligence (AI) was a consistent focus. Participants asked when the use of AI requires a privacy impact assessment (PIA), how algorithmic tools are assessed for bias or risk and what responsibilities apply when public or private organizations rely on third-party systems. Several raised questions about metadata, prompts and training data, and whether existing privacy frameworks cover these inputs. There were specific requests for provincial guidance on AI in areas such as automated decision-making and meaningful consent. Caseload analysis confirms these concerns are already emerging in practice. The OIPC is seeing a growing number of complaints and review requests involving surveillance, automated systems and uncertainty about what constitutes personal information in digital environments.

Surveillance concerns were also prominent. Participants described increasing use of monitoring technologies across housing, healthcare, education and public spaces. Examples included the growing use of doorbell cameras and privately owned surveillance systems that capture activity in shared or public areas. Some acknowledged these tools are often introduced for safety reasons, but they questioned whether people understand when they are being recorded or have any real ability to opt out. Several said that surveillance is becoming normalized without adequate oversight and that privacy risks are often invisible to the people who may be most affected.

> Much of the data that is collected from these devices is done explicitly for the purposes of developing a secondary stream of revenue for companies and packaged under the guise of improved functionality.

Internal planning reflections echoed these points and identified a gap in capacity to support complex technology files, especially where legal precedent is limited or context specific. Staff noted that without stronger internal capability and clearer expectations, regulated organizations may avoid new technologies entirely or rely on informal workarounds that carry legal or ethical risk.

Participants said they do not expect the OIPC to solve every technology issue but do want leadership in helping define appropriate standards and clarifying how privacy law applies in digital systems. Some emphasized that privacy should support, not block, responsible innovation. Others said the absence of clear direction may discourage good actors while allowing inconsistent practices to continue unchallenged.

> We would welcome input and guidance in terms of how best to address and possibly harmonize operational policies related to information sharing at regional interagency tables where the federal Privacy Act, FOIPPA and PIPA come into play.

Participants were clear that what is needed is not just more guidance, but guidance that is usable, specific and matched to real-world needs. Several emphasized the importance of tools such as model clauses for contracts, templates, annotated PIAs and checklists for determining when disclosures are permitted under law.

Smaller organizations in particular asked for sector-specific examples and plain language summaries that could be used without legal support. Staff confirmed that these types of requests are common, but said they are often unable to provide consistent or up-to-date tools in response.

Education was also seen as essential for the public. People do not always understand their privacy or access rights, how to exercise them or where to turn for help. This was said to be especially true for newcomers, seniors, people with limited digital access and those unfamiliar with how the laws apply in daily life. Suggestions included community-based education, partnerships with trusted intermediaries and plain language materials that help people understand not just the law, but how to use it.

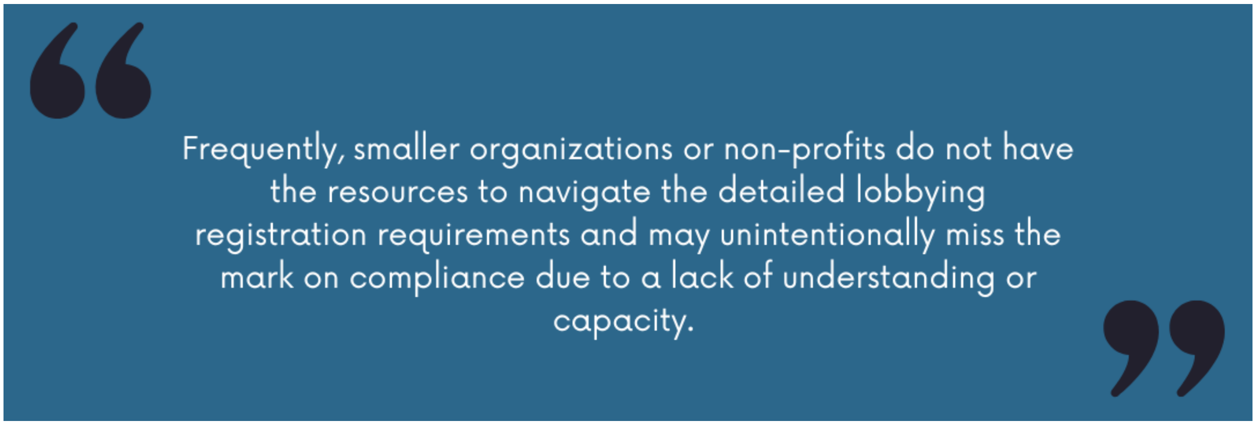
Others raised concerns that public education also needs to address the broader digital environment. It should not just focus on rights, but how personal data is collected, inferred and used in ways people may not fully understand. Areas of concern included social media, profiling, targeted advertising, AI-enabled surveillance and digital systems used in housing, education and public spaces. Some noted that opting out is often not realistic, especially for those relying on public services. Raising awareness about privacy issues and risks was seen as key to building digital literacy, autonomy and informed participation.

Across all groups, participants expressed that better education, clearer materials and more responsive outreach would improve understanding and reduce conflict. Several said this work is especially important for public-facing institutions, where confusion about the rules can erode confidence in the systems that are meant to protect privacy and promote transparency.

Many organizations are not equipped to fully meet their obligations

Participants across the engagement process described widespread capacity challenges that limit how organizations meet their privacy and access obligations. These concerns came up in listening sessions, internal interviews, written submissions and stakeholder discussions. This was not about unwillingness. It came down to practical constraints. Staff, time, funding and records infrastructure were all flagged as barriers.

The most acute concerns came from smaller organizations. Many said they have only one person, sometimes part-time, tasked with all access and privacy work. Internal staff confirmed that current oversight models assume a baseline capacity that many organizations do not meet.



> Frequently, smaller organizations or non-profits do not have the resources to navigate the detailed lobbying registration requirements and may unintentionally miss the mark on compliance due to a lack of understanding or capacity.

Participants emphasized that while FOI timelines are one symptom of the issue, the core problem is deeper. Limited records management capacity was described as a fundamental obstacle to both transparency and privacy compliance. Some said they cannot reliably search, redact or assess risk across their systems. In some organizations, privacy-related records are scattered across paper files, personal drives, inboxes and cloud folders, with no consistent structure or digital tools.

OIPC staff noted that records management gaps are a common thread in privacy complaints. Even in cases that begin as privacy disputes, the root issue is often an inability to locate, verify or manage records. There were also concerns about data governance across teams and systems, especially where staff turnover or informal practices make it difficult to track personal information use over time.

There was a sense, particularly among lower-resourced organizations and those handling sensitive data, that contacting the OIPC for support could carry risk. Some expressed concern that seeking advice could trigger formal scrutiny.

Input across sources also pointed to the absence of a proactive or preventive support model. Several noted that there is currently no clear mechanism to identify or assist organizations that may be struggling before issues escalate. The overall approach was described as largely reactive, with tools and outreach developed in response to problems rather than through an ongoing strategy to build capacity and confidence.

Laws are misaligned with how today's systems and services work

Several stakeholders expressed concern that several of BC's core privacy, access and lobbying laws do not reflect how information is created, stored or shared in practice. While the underlying principles of these laws remain valued, many suggested that the way they are written no longer fits the realities of digital systems, complex service delivery models or cross-organizational workflows.

Challenges with key statutory concepts such as custody and control, meaningful consent and reasonable search were raised across stakeholder interviews, public engagement sessions and internal feedback. These concepts were described as increasingly difficult to apply in the context of cloud storage, shared platforms, artificial intelligence and third-party service providers. Additional concerns were expressed about the tension between FOI timelines and the operational needs of service delivery, particularly when records span multiple systems or jurisdictions.

Several staff said these structural issues often lead to delays, hesitation or conflicting interpretations. Some described routinely navigating around gaps in the legislation because it does not align with the way systems actually function. These challenges were often linked to environments involving sensitive data, emerging technologies or service delivery across multiple partners or systems.

> “PIPA should be updated with mandatory privacy management programs and privacy impact assessments, along with fines for non-compliance.”

There was also concern about the limits of PIPA. Multiple stakeholders said the Act is outdated, lacks enforcement mechanisms and does not require structured privacy programs. Some called for updates that would bring BC in line with other jurisdictions, such as Quebec's Law 25 or proposed federal reforms. Suggestions included mandatory privacy management programs, stronger breach reporting rules and the authority to issue fines.

While FIPPA was updated in 2021, concerns raised across external and internal input suggest that many foundational elements still do not account for how digital systems and public bodies function today. These concerns were rooted not in a lack of guidance or understanding, but in the structural limitations of the legislation itself.

The rights of children and youth are constrained

There was clear concern across the input received that BC's current privacy laws and practices do not reflect the realities children and youth face when interacting with digital platforms and public systems. Feedback highlighted risks in education, health care, housing, and other institutional settings, particularly where services involve multiple agencies or long-term involvement by the state.

Many noted that privacy frameworks often assume adult users and fail to reflect the ways young people engage with technology or receive services. Consent processes were described as legalistic and inaccessible, with forms written at an adult reading level and applied without consideration of a young person's comprehension or circumstances. Families and young people are often left without a clear understanding of who holds their information, how it is used, or how to challenge it.

> As children's personal data is being harvested and monetised at unprecedented pace and scale, a robust data protection framework is crucial for ensuring children's privacy, safety, and agency in the digital environment.

Youth records remaining on file for years was another recurring concern and these records could influence how young people are treated by institutions long after the original context has changed. In many cases, there appears to be no path to correct or update that information, even when it affects access to services or supports.

Information sharing between agencies was identified as a source of confusion and risk. Teams working in child protection, policing, Indigenous service delivery and education described uncertainty about which laws apply in shared settings. Different legal obligations can result in hesitation, delays or conflicting interpretations. Several

> In our experience, the statutory timelines related to information requests have been essentially meaningless.

Questions were also raised about how decisions are made to proceed with or decline files. Some questioned whether intake decisions consistently reflect the potential impact or urgency of the issues raised. Internal feedback noted differences in how thresholds are interpreted across teams. Clearer criteria and stronger triage processes were suggested to support more even and transparent decision-making.

Time extension practices were also raised as a concern. The OIPC was seen as sometimes granting extensions to public bodies without consistent documentation or visible follow-up. Some viewed this as a double standard, with oversight timelines appearing more flexible than those imposed on others. Internally, there were calls for clearer standards and more deliberate oversight of extension requests.

Adjudication processes were also seen as inconsistent and difficult to navigate. Timelines could stretch for months, and next steps sometimes depended on whether applicants followed up. In some cases, matters were delayed or reset due to process changes or staff turnover. These patterns were described as undermining confidence, accessibility and transparency in the oversight process.

The OIPC's 2024–25 Annual Report and Service Plan acknowledges many of these issues. Planned reforms include improved triage procedures, updated adjudication templates and revised performance targets. Some changes have already been made, including the addition of registrar support and internal reviews of how extensions and deemed refusals are handled. While these efforts are underway, feedback suggests that further attention is needed to ensure predictable and trusted oversight processes.

Fewer concerns were raised about the operations of the ORL, however, the Registry's online interface was described as intimidating and complex to navigate. Some internal material noted that ORL staff have supported OIPC workflows during periods of high demand.

B.C.'s privacy and access systems do not serve everyone equally

There was consistent recognition that privacy and access systems in B.C. do not serve all communities equally. This included concerns about how people access their rights, how those rights are supported in real-world contexts and whether oversight systems reflect the needs of those most affected.

Systemic barriers were identified that make it more difficult for some individuals and communities to navigate privacy and access frameworks. These include language, literacy, disability, unstable housing, limited internet access and lack of institutional trust. People are often expected to locate the right channels, complete formal paperwork and understand legal entitlements without support. Those facing social or economic marginalization may be less likely to take these steps, especially when there is fear of being disbelieved or further scrutinized. Some pointed to power imbalances that affect groups such as children in care or people who are incarcerated, raising questions about how those least likely to assert their rights are heard and supported.

Concerns were also raised about the experience of tracking and surveillance of marginalized populations. Monitoring is more common in some service environments, including housing, education and social supports, but individuals affected may have limited ability to question or influence how their personal information is collected or used. Others noted that those who feel comfortable being surveilled are often those least likely to face discrimination, and that this sense of safety reflects privilege, not shared experience.

There was also uncertainty about whether equity-related data collection efforts are leading to meaningful change. While intended to support inclusion or track outcomes, input received suggested that collecting more data does not always result in better service, protection or representation. Some questioned whether this information is being retained or repurposed in ways that reinforce rather than reduce marginalization.

Indigenous data sovereignty was identified as a significant and ongoing gap. Input emphasized the need to align privacy oversight with Indigenous-led governance models, with OCAP principles and with the rights affirmed in UNDRIP. Submissions called for long-term access to data on terms defined by Indigenous communities, control over how information is stored, accessed and reported, and sustained resourcing to support these practices.

> Data Sovereignty is not the work of any organization other than the sovereign Nations within themselves.

There were also calls for the OIPC to embed equity more explicitly across its functions, including in outreach and intake processes. This included suggestions to improve how the office engages with and serves communities that face barriers in accessing privacy and access systems, such as newcomers, people with disabilities and those working in low-resourced settings. There were also concerns that guidance and public education materials may not be fully accessible to all audiences, particularly those with disabilities, lower literacy or limited digital access. The OIPC was encouraged to work with trusted intermediaries, develop plain language and culturally appropriate materials and ensure that services reflect the lived realities of those most affected.

oipc

OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

PO Box 9038, Stn. Prov. Govt.
Victoria, BC V8W 9A4

Telephone: 250.387.5629
Toll-Free in BC: 1.800.663.7867

Email: info@oipc.bc.ca

oipc.bc.ca