THE PRIVACY COMPLIANCE GAP

A Practical Guide to Understanding Your Privacy Risk, Before Regulators Do

By Sukhpreet Singh *Senior Privacy Specialist | 8+ Years | 150+ Privacy Impact Assessments*
Mosaic Effect Inc.

HOW TO USE THIS GUIDE

This guide contains real scenarios of Canadian organizations that faced privacy failures—and what it cost them.

Here's how to use it:

1. **Scan the Table of Contents** — Look for scenarios that sound familiar to your organization
2. **Read the chapters that resonate** — Don't feel obligated to read everything
3. **Take the Privacy Maturity Assessment**— Score yourself honestly
4. **If you find gaps** — Book a discovery call to discuss solutions

This is NOT a sales document. This is a diagnostic tool.

If none of these scenarios apply to your organization, we're probably not a fit. If you find yourself in multiple chapters, let's talk about closing those gaps before they become headlines.

TABLE OF CONTENTS

PART 1: THE REALITY OF PRIVACY RISK IN CANADA

- Chapter 1: The $100 Million Problem Nobody Talks About
- Chapter 2: Why "We Have IT Security" Isn't Enough

PART 2: BREACH CASE STUDIES — WHAT WENT WRONG

- Chapter 3: When Technology Outpaces Governance (RCMP & Clearview AI)
- Chapter 4: The Multi-System Integration Disaster (Saskatchewan eHealth)
- Chapter 5: The $235,000 Email Mistake (Ottawa Public Health)
- Chapter 6: Vulnerable Data, Vulnerable People (City of Toronto Shelters)
- Chapter 7: The Province-Wide Shutdown (Newfoundland Healthcare)
- Chapter 8: The Insider Threat Nobody Saw Coming (Desjardins)

PART 3: WHERE ORGANIZATIONS FAIL

- Chapter 9: No Legal Authority — The Silent Killer
- Chapter 10: Over-Collection — The Data You Didn't Need
- Chapter 11: The Vendor You Never Assessed
- Chapter 12: Retention Without Limits
- Chapter 13: The PIA You Never Did

PART 4: THE PRIVACY MATURITY FRAMEWORK

- Chapter 14: The 5 Levels of Privacy Maturity
- Chapter 15: Where Do You Stand? (Self-Assessment)

PART 5: WHAT TO DO NEXT

- Chapter 16: The Path Forward
- About Mosaic Effect
- Book Your Discovery Call

PART 1: THE REALITY OF PRIVACY RISK IN CANADA

Chapter 1: The $100 Million Problem Nobody Talks About

Every year, Canadian public-sector organizations—from federal departments to municipalities, health authorities to Crown corporations—experience significant privacy breaches.

These aren't theoretical risks. They're operational disruptions, public scrutiny, costly investigations, regulatory findings, and reputational damage that takes years to rebuild.

The numbers are staggering:

The average cost of a data breach in Canada is approximately **$6 million**. But that's just the average. The outliers are what should concern you:

- A single provincial healthcare cyberattack: **$65-100 million**
- A major financial institution insider breach: **$350-400 million**
- A ransomware attack on a health authority: **$12-15 million**

And these are just the breaches that made headlines.

The hidden costs nobody tracks:

For every major breach, there are hundreds of smaller incidents that never reach the news but still cost organizations:

- Emergency response and forensics
- System rebuilds and modernization
- Legal fees and regulatory engagement
- Patient/client notification
- Reputational damage to digital initiatives
- Lost productivity during recovery
- Staff turnover from burnout

The pattern is consistent:

Organizations that experience significant privacy failures share common characteristics:

- Technology deployed faster than governance could keep up
- Multi-system integrations without proper privacy assessments
- Legacy systems holding sensitive data without modern controls
- Third-party vendors with unvetted access
- Retention practices that kept data far longer than necessary

If any of these sound familiar, keep reading.

Chapter 2: Why "We Have IT Security" Isn't Enough

Let's address the most common misconception in privacy: **Security is not the same as privacy.**

Cybersecurity protects systems. Privacy protects people.

Here's what that means in practice:

A healthcare organization can have:

- Enterprise-grade firewalls
- Multi-factor authentication everywhere
- Encrypted data at rest and in transit
- 24/7 security monitoring
- Annual penetration testing

And still have a **catastrophic privacy failure** because:

- They collected more data than they needed
- They kept it longer than they should have
- They shared it with vendors who weren't properly vetted
- They didn't have legal authority for how they were using it
- They couldn't tell individuals what was happening with their data

The RCMP learned this the hard way.

In 2020-2021, the RCMP—with all their security infrastructure—was found to have used Clearview AI facial recognition without conducting a Privacy Impact Assessment, without proper authority under the Privacy Act, and without verifying the legality of the technology.

The Office of the Privacy Commissioner ruled they violated multiple privacy principles.

Total estimated cost: **$1.35 million** in investigation, compliance rework, policy overhaul, and reputational damage.

They had security. They didn't have privacy governance.

The question isn't whether you have security.

The question is: Do you have the governance, the assessments, and the controls to ensure you're handling personal information in a way that's lawful, transparent, and defensible?

PART 2: BREACH CASE STUDIES — WHAT WENT WRONG

Chapter 3: When Technology Outpaces Governance

Case Study: RCMP and Clearview AI (2020-2021)

The Scenario

The RCMP needed facial recognition capabilities for investigations. Clearview AI offered a solution—a system that scraped billions of images from social media to build a massive facial recognition database.

The technology worked. It was deployed. Cases were solved.

There was just one problem: **Nobody conducted a Privacy Impact Assessment.**

What Went Wrong

- No PIA was completed before deployment
- No proper authority under the Privacy Act was established
- No verification of the technology's legality was conducted
- Canadians were exposed to unwarranted surveillance
- The Office of the Privacy Commissioner investigated

The Real Problem

This wasn't a security failure. The system was secure. This was a **governance failure**.

When technology moves faster than your privacy program can assess it, you create liability. Even federal law enforcement—with full legal teams, established protocols, and institutional knowledge—got caught.

The Cost

Category	Estimated Cost
Internal investigation & forensics	$450,000
Compliance rework & mandatory PIAs	$200,000

Policy & training overhaul	$300,000
Reputational damage management	$400,000
Total Estimated Impact	**$1.35 million**

The Lesson

A robust PIA process—automated, repeatable, and auditable—prevents this.

If your organization is deploying new technology, especially anything involving biometrics, AI, or automated decision-making, you need a privacy assessment before you flip the switch. Not after.

Chapter 4: The Multi-System Integration Disaster

Case Study: Saskatchewan eHealth Cyberattack (2020)

The Scenario

Saskatchewan's eHealth system—one of the largest provincial health data repositories in Canada—was hit by a ransomware attack. Patient and employee personal information across multiple systems was compromised. Files were stolen, encrypted, and posted online.

What Went Wrong

- Legacy systems weren't properly assessed for privacy risk
- Vendor integrations lacked adequate privacy controls
- Multi-system data flows created exposure points nobody mapped
- No comprehensive PIA covered the integrated environment

The Real Problem

This is what happens when you have **data silos that suddenly connect** without proper governance.

Each system might have been reasonably secure on its own. But when they integrated—when patient data started flowing between hospital systems, administrative databases, and third-party vendors—the attack surface exploded.

Nobody had done the privacy analysis to understand: Where does this data go? Who can access it? What happens if one system is compromised?

The Cost

Category	Estimated Cost
Emergency cyber response	$2.5 million
System rebuild + modernization	$7-10 million
Legal + OPC engagement	$1 million
Patient notification	$350,000-$500,000
Reputational impact on digital health strategy	Significant
Total Estimated Impact	**$12-15 million**

The Lesson

PIAs for multi-system integrations are not optional.

Every time you connect systems, you create new data flows. Every new data flow creates new risk. If you're integrating legacy systems with modern platforms, if you're connecting internal databases with external vendors, you need privacy analysis that maps the full picture.

Chapter 5: The $235,000 Email Mistake

Case Study: Ottawa Public Health (2019)

The Scenario

An Ottawa Public Health employee was sending COVID-19 test notifications to affected individuals. Simple task. Routine communication.

They used CC instead of BCC.

Hundreds of test contacts were exposed to each other. Names, email addresses, and implicit health status—all visible to everyone on the list.

What Went Wrong

- Human error in a routine process
- No technical controls to prevent mass CC exposure
- No PIA-driven standard operating procedures for sensitive communications

- No automated safeguards in the email workflow

The Real Problem

This wasn't a sophisticated attack. It wasn't a system vulnerability. It was someone having a busy day and clicking the wrong field.

Most breaches are this simple.

80-90% of privacy breaches come from avoidable workflow gaps. Not hackers. Not nation-state actors. Just people doing their jobs without the right controls in place.

The Cost

Category	Estimated Cost
Notification & OPC reporting	$75,000
Policy reform & staff retraining	$120,000
External privacy consulting	$40,000
Total Estimated Impact	**$235,000+**

Plus significant damage to public confidence in health authority communications during a pandemic.

The Lesson

PIAs identify these gaps before they become incidents.

A proper privacy assessment of communication workflows would have flagged: What happens if someone uses CC instead of BCC? What technical controls prevent this? What training ensures staff understand the risk?

The solution isn't expensive. It's a policy. A technical control. Training. But you only implement these if you've done the assessment that identifies the gap.

Chapter 6: Vulnerable Data, Vulnerable People

Case Study: City of Toronto Shelter Data Exposure (2021)

The Scenario

An employee email error exposed personal data of residents in Toronto's shelter system. Names, contact information, and other identifying details of some of the city's most vulnerable people—visible to unintended recipients.

What Went Wrong

- Manual email processes for sensitive data
- No automated controls for handling vulnerable population data
- Reliance on individual staff vigilance rather than system safeguards
- No elevated privacy protocols for high-sensitivity information

The Real Problem

Not all personal information is equal. Data about vulnerable populations—shelter residents, mental health patients, domestic violence survivors—carries amplified risk.

When this data is exposed, the harm isn't just reputational or financial. There can be physical safety implications.

Municipal governments handle enormous amounts of sensitive data about people in difficult circumstances. The privacy controls need to match the sensitivity.

The Cost

Category	Estimated Cost
Third-party investigation	$150,000
Notification & communications	$50,000
Operational disruption	$200,000
Rebuilding trust with NGOs & community groups	Ongoing
Total Estimated Impact	**$400,000+**

The Lesson

Municipalities struggle with manual workflows. Automated privacy governance reduces reliance on error-prone processes.

If your organization serves vulnerable populations, your privacy controls need to be stronger than baseline requirements. A PIA for these programs should identify the elevated risks and implement corresponding safeguards.

Chapter 7: The Province-Wide Shutdown

Case Study: Newfoundland & Labrador Healthcare Cyberattack (2021-2022)

The Scenario

A major cyberattack hit Newfoundland and Labrador's healthcare system. Not one hospital. Not one database. The entire provincial healthcare infrastructure.

Hospital operations shut down. Patient data was exposed. Clinical and HR systems required complete rebuilds. Recovery took years.

This was the largest attack on a Canadian health system in history.

What Went Wrong

- Data governance maturity was insufficient for the threat landscape
- System-level privacy assessments were incomplete or absent
- No comprehensive understanding of where sensitive data resided
- Recovery plans weren't adequate for province-wide failure

The Real Problem

Healthcare systems are prime targets because they hold the most sensitive data and often have the weakest governance. Electronic health records, diagnostic results, mental health notes, HIV status, genetic information—all in systems that were designed for clinical efficiency, not privacy resilience.

When you haven't done the foundational work—mapping your data, assessing your risks, building your governance—you're not prepared for an attack of this scale.

The Cost

Category	Estimated Cost
System rebuild	$50-75 million
Forensics & recovery	$10 million
Notification & identity protection	$5 million
Litigation exposure	Tens of millions

Total Estimated Impact	**$65-100 million+**

The Lesson

No privacy program can survive without strong governance and system-level PIAs. Cyber risk and privacy risk are inseparable.

This wasn't a privacy failure in isolation. But it was enabled by inadequate privacy governance. When you don't know where your sensitive data is, how it flows, who has access, and what your retention practices are—you can't protect it.

Chapter 8: The Insider Threat Nobody Saw Coming

Case Study: Desjardins Data Breach (2019-2022)

The Scenario

A single rogue employee at Desjardins—one of Canada's largest financial cooperatives—exfiltrated personal information of **4.2 million members**.

Not a hack. Not a system vulnerability. An employee with legitimate access who decided to steal data.

What Went Wrong

- Excessive access permissions beyond what was necessary
- Insufficient monitoring of data access patterns
- No automated detection of unusual data exfiltration
- Access controls weren't aligned with least-privilege principles

The Real Problem

This is the threat that keeps CISOs awake at night: the insider with legitimate credentials.

Your firewalls don't help. Your encryption doesn't help. Your penetration testing doesn't help. Someone on your team, with the access they need to do their job, decides to do something they shouldn't.

The only defense is governance: limiting access to what's truly necessary, monitoring for anomalies, and building a culture where privacy is everyone's responsibility.

The Cost

Category	Estimated Cost
Class action settlement	$200 million
Cyber improvements	$100+ million
Identity theft protection for members	$50 million
Regulatory compliance	$5 million
Total Estimated Impact	**$350-400 million**

The Lesson

Even well-funded institutions collapse without proper access governance. PIA-driven controls prevent catastrophic insider threats.

If you haven't assessed: Who has access to what? Do they need that access? How would you detect if someone was exfiltrating data?—you have a gap.

PART 3: WHERE ORGANIZATIONS FAIL

Chapter 9: No Legal Authority — The Silent Killer

The Scenario

You're a government agency launching a new digital service. You've built the technology. You've tested it. You're ready to collect citizen data and deliver value.

But here's the question nobody asked: **Do you have the legal authority to collect this data for this purpose?**

The Real Problem

Under the Privacy Act, PIPEDA, FIPPA, and virtually every Canadian privacy law, you must have clear legal authority for collecting personal information. This isn't optional. It's foundational.

Yet organizations routinely skip this step:

- Assuming authority exists because "we've always done it this way"

- Launching programs before legal analysis is complete
- Collecting data first and figuring out authority later
- Assuming consent covers gaps in statutory authority

Why It Matters

Without legal authority:

- Every piece of data you collect is potentially unlawful
- Individuals have grounds for complaints
- Regulators can order you to stop processing
- Your entire program can be shut down

The Solution

A proper PIA starts with this question. Before you design data flows, before you build systems, before you launch services: What is our legal authority? Under which statute? For which purposes?

If you can't answer that clearly, you're not ready to proceed.

Chapter 10: Over-Collection — The Data You Didn't Need

The Scenario

Your intake form asks for: full name, address, date of birth, social insurance number, phone number, email, emergency contact, employer information, income range, and demographic details.

But your service only requires: name and email.

The Real Problem

Data minimization isn't just a principle—it's a requirement.

Every piece of personal information you collect is liability. It's data you have to protect, retain appropriately, and potentially disclose in a breach. The more you collect, the more you're exposed.

Common over-collection patterns:

- Forms that "might be useful later"
- Legacy fields nobody removed

- "Nice to have" data for analytics
- Vendor requirements that exceed your needs

Why It Matters

- More data = larger breach impact
- More data = higher regulatory scrutiny
- More data = more individual complaints
- More data = more retention complexity

The Solution

A PIA forces the question: For each data element, what is the purpose? Is it necessary? Can we achieve the same outcome with less?

If you're collecting social insurance numbers for a newsletter signup, something has gone wrong.

Chapter 11: The Vendor You Never Assessed

The Scenario

You're using a cloud service to process client data. The vendor seemed reputable. They signed a contract. You assume they're handling data appropriately.

But you never actually verified:

- Where they store the data
- Who at the vendor has access
- What their security controls are
- Whether they use subprocessors
- What happens if they have a breach

The Real Problem

Even if you outsource the processing, you can't outsource the liability.

Under Canadian privacy law, you remain responsible for the personal information you share with third parties. If your vendor has a breach, you're the one notifying individuals and explaining to regulators.

Common Vendor Gaps

- No Data Processing Agreement (DPA) in place
- No Vendor Risk Assessment conducted
- No verification of claimed security certifications
- No understanding of subprocessor relationships
- No breach notification requirements in contract

The Solution

Third-Party Privacy Assessments (TPPAs) evaluate vendor privacy practices before you share data. They verify that vendors meet your standards, not just their own claims.

If you're sharing personal information with any external party—cloud providers, consultants, software vendors, service providers—you need documented evidence that they can be trusted.

Chapter 12: Retention Without Limits

The Scenario

Your organization has files from 2008. Client records from programs that ended a decade ago. Employee data from people who left years back. And nobody can explain why any of it is still there.

"We might need it someday."

The Real Problem

Data you don't need is data you shouldn't have.

Every piece of personal information you retain beyond its useful life is:

- Liability in a breach
- Subject to access requests
- Consuming storage and security resources
- Creating confusion about what's current

Organizations routinely fail at retention because:

- No defined retention schedules
- No automated deletion processes
- Fear of deleting something "important"
- Lack of clarity on when retention periods start/end

Why It Matters

When you have a breach, the first question is: What was exposed? If your answer includes "data from programs that ended 15 years ago that we kept for no clear reason," you have a problem.

When you receive an access request, you have to search everything. If that includes decades of unorganized legacy data, the cost of compliance explodes.

The Solution

A PIA addresses retention: How long do we keep this data? Why? What triggers deletion? How do we ensure it actually gets deleted?

If you don't have documented retention schedules tied to legal requirements and business purposes, you're keeping data you shouldn't have.

Chapter 13: The PIA You Never Did

The Scenario

Your organization has launched 15 new digital initiatives in the past three years. New systems, new integrations, new data collection, new vendors.

How many Privacy Impact Assessments have you completed?

For many organizations, the answer is zero.

The Real Problem

PIAs aren't bureaucratic overhead. They're the mechanism for identifying problems before they become incidents.

Organizations skip PIAs because:

- They think it's "just paperwork"
- They don't have internal capacity
- They're moving too fast to stop and assess
- They don't realize when one is required
- They assume security assessments cover privacy

What You're Missing

When you skip a PIA, you don't know:

- Whether you have legal authority for your data processing
- Whether you're collecting more data than necessary
- Whether your retention practices create liability
- Whether your vendors meet privacy standards
- Whether your security controls adequately protect privacy
- Whether individuals are properly informed about your practices

The Solution

PIAs should be standard practice for any new or significantly modified program involving personal information. They don't have to take months. With the right approach and expertise, a focused PIA can be completed in weeks.

The alternative—finding out about gaps after a breach—is significantly more expensive.

PART 4: THE PRIVACY MATURITY FRAMEWORK

Chapter 14: The 5 Levels of Privacy Maturity

Not all organizations are at the same place in their privacy journey. Understanding where you are helps you understand what you need.

Level 1: Reactive

Characteristics:

- No formal privacy program
- Privacy addressed only when issues arise
- No dedicated privacy resources
- Policies are outdated or nonexistent
- PIAs are not conducted

Risk Level: Critical

Typical Cost of Incident: Existential—could threaten organization viability

---

Level 2: Developing

Characteristics:

- Basic privacy policies exist
- Some awareness of privacy requirements
- Ad hoc approach to assessments
- Limited resources for privacy
- Compliance is inconsistent

Risk Level: High

Typical Cost of Incident: $500K - $5M depending on severity

Level 3: Defined

Characteristics:

- Formal privacy program established
- Designated privacy officer
- PIAs conducted for major initiatives
- Policies are current and communicated
- Training is provided but not comprehensive

Risk Level: Medium

Typical Cost of Incident: $100K - $500K, manageable with preparation

---

Level 4: Managed

Characteristics:

- Privacy embedded in project lifecycles
- Automated workflows for assessments
- Continuous monitoring and improvement
- Strong vendor management
- Regular audits and updates

Risk Level: Low

Typical Cost of Incident: Under $100K, contained quickly

Level 5: Optimized

Characteristics:

- Privacy by design is standard practice
- Predictive risk management
- Industry-leading practices
- Privacy as competitive advantage
- Continuous innovation in privacy protection

Risk Level: Minimal

Typical Cost of Incident: Rare, quickly contained, minimal impact

---

Chapter 15: Where Do You Stand? (Self-Assessment)

Answer honestly. Nobody is watching.

Legal Authority

- [ ] We have documented legal authority for all data collection
- [ ] We're not sure about some programs
- [ ] We've never formally assessed this

Privacy Impact Assessments

- [ ] We conduct PIAs for all new initiatives
- [ ] We do PIAs sometimes
- [ ] We rarely or never conduct PIAs

Data Minimization

- [ ] We only collect data we can justify
- [ ] We probably collect more than necessary
- [ ] We've never audited our collection practices

Retention Practices

- [ ] We have defined schedules and automated deletion
- [ ] We have schedules but inconsistent enforcement
- [ ] We keep most data indefinitely

Vendor Management

- [ ] We assess all vendors handling personal data
- [ ] We assess major vendors only
- [ ] We rely on vendor assurances without verification

Breach Preparedness

- [ ] We have tested incident response plans
- [ ] We have plans but haven't tested them
- [ ] We don't have documented plans

Training

- [ ] All staff receive regular privacy training
- [ ] Some staff are trained
- [ ] Training is minimal or nonexistent

Scoring:

- Mostly first options: Level 4-5
- Mix of first and second: Level 3
- Mostly second options: Level 2
- Mostly third options: Level 1

PART 5: WHAT TO DO NEXT

Chapter 16: The Path Forward

If you found yourself in these chapters—if the case studies sounded familiar, if the gaps resonate with your organization—you have two choices:

Choice 1: Hope it doesn't happen to you.

The organizations in this guide thought the same thing. They were busy. They had other priorities. They assumed their existing controls were sufficient.

Until they weren't.

Choice 2: Close the gaps before regulators or attackers find them.

Privacy compliance isn't about perfection. It's about having the governance, the assessments, and the controls that demonstrate you take privacy seriously.

When a breach happens—and eventually, something will happen—the question isn't whether you were perfect. The question is: Did you do reasonable things to protect personal information? Can you prove it?

Organizations with documented PIAs, defined policies, trained staff, and monitored controls can answer: Yes.

Organizations without them face a much harder conversation.

About Mosaic Effect

Mosaic Effect Inc. is a Canadian privacy consultancy specializing in the design, execution, and automation of Privacy Impact Assessments.

Our Clients Include:

- ServiceOntario
- Treasury Board of Canada Secretariat
- Canadian Housing and Mortgage Corporation (CMHC)
- Farm Credit Canada
- Ontario Health
- Ministry of Public & Business Service Delivery

Our Founder:

Sukhpreet Singh has 10+ years of experience leading PIAs, data governance frameworks, and privacy compliance across federal and provincial ministries. He holds a Master of Public Administration & Law, maintains Secret Security Clearance, and has personally led 80+ Privacy Impact Assessments for complex government programs.

What We Do:

- Privacy Impact Assessments (Full, Conceptual, Delta, Third-Party)
- Privacy Management Program Development
- Breach Response and Preparedness
- Privacy Training
- Policy Development
- Vendor Risk Assessments

Our Approach:

We don't just check boxes. We build privacy governance that's practical, defensible, and aligned with how your organization actually operates.

Book Your Discovery Call

If you found gaps in this guide that match your organization, let's talk about closing them.

This is a Solutions Call, Not a Sales Call.

We're going to:

- Understand your specific situation
- Identify which gaps pose the highest risk
- Explain how we'd approach solving them
- Give you honest assessment of timeline and investment

We're not going to:

- Pressure you into anything
- Promise unrealistic timelines
- Pretend we can solve everything overnight

Before You Book:

This call makes sense if:

- You identified multiple gaps in this guide
- You have budget for professional privacy services
- You're ready to take action, not just explore

If you're just curious, that's fine—but this guide should give you most of what you need to assess your situation. The call is for organizations ready to move.

Book Here: [calendly.com/mosaiceffectinc/30min]
