eBook 01

MNP DIGITAL

Privacy, ethics, and the future of Artificial Intelligence (AI)

The data dilemma

This eBook series explores the big trends and concerns leaders have about protecting critical data amid upsurging artificial intelligence, machine learning, and cyber threats. It offers ideas for fortifying privacy and security while adding value.

Gold
Microsoft Partner

Microsoft

MNPdigital.ca

Organizational leaders speak out about digital privacy and security concerns

Is our organization appropriately protected from emerging threats?

Do we have the right protocols in place in the event of a cyber attack?

Are we prepared to respond effectively in the event of a data breach?

Are we in compliance with global data privacy regulations?

Have we addressed our customers' privacy and security concerns around artificial intelligence and machine learning?

As organizational leaders adopt technology innovations to deliver next-generation products and services, they have growing concerns about protecting security and privacy in an increasingly machine-learning driven world.

MNP Digital recently met with leaders of private businesses and public sector organizations across a variety of industries to understand their worries about cyber security and privacy.

During our conversations, three issues continually re-emerged.

The Data Dilemma focuses on these key issues. This series of eBooks captures the big trends and concerns and presents the views of our digital solutions experts regarding how to add value, protect privacy, and fortify security amid upsurging artificial intelligence, machine learning, and cyber threats.

eBook 1 – Privacy, Ethics, and the Future of AI

eBook 2 – Ideas to improve the effectiveness of your incident response plan

eBook 3 – Is encryption the best practice you've been missing?

The MNP Digital experts

Danny Timmins – National Cyber Security Leader
Adriana Gliga-Belavic – National Privacy Leader
Jason Lee – Partner and Leader of Applied Data Centre of Excellence
Chris Law – Partner and National Incident Management and Response and Offensive Security Leader
Eugene Ng – Partner and Leader of Security Operations and Technology Implementation Team

Featured Expert
Dr. Ann Cavoukian
Executive Director, Global Privacy & Security by Design Centre

eBook 1

Privacy, ethics, and the future of Artificial Intelligence (AI)

In this eBook:

- Why privacy, ethics, and the future of AI is important
- How might the future of privacy and platform ethics look in an algorithm-dominated world?
- Who is responsible for ensuring algorithms serve the needs of all users and stakeholders?
- What steps must developers and regulators take to ensure AI and Machine Learning (ML) platforms of tomorrow preserve trust and protect personal sovereignty?
- Some provinces are updating privacy regulations — what should we be thinking about?
- Key takeaways

Why privacy, ethics, and the future of AI is important

Artificial intelligence (AI) is rapidly becoming indispensable to organizations. But, contrary to its power and growing ubiquity, there is little regulation relating to its use. Organizations that use AI systems are typically self-policing.

Meanwhile, privacy is a dramatically growing concern for Canadians.

Canadians worry about privacy

- Only 45 percent believe that businesses respect their privacy rights.
- Almost 90 percent are at least somewhat concerned online information about them is being used in an attempt to steal their identity, including 48 percent who are extremely concerned about identity theft.
- The majority feel they have little or no control over how their personal information is being used by companies (61 percent), or by governments (65 percent).

2021 survey conducted for the Privacy Commissioner of Canada

MNP Digital is exploring the future of privacy and ethics in an algorithm-dominated world.

- Who should be responsible for ensuring algorithms serve the needs of all users and stakeholders?
- How can we train algorithms to protect privacy, and what groundwork is required for everyone to benefit from their immense potential?
- What steps should developers and regulators be taking to ensure the AI and ML platforms of tomorrow preserve trust and protect personal sovereignty?

Q: How might the future of privacy and platform ethics look in an algorithm-dominated world?

Leaders' concerns

- Compliance and privacy start to take a back seat when organizations try to be first to market. AI and ML are sometimes competitive differentiators so that can limit cooperation and collaboration with industry peers.
- From a resourcing point of view, the more tools and technology we use, the more resources we need to maintain and support them. These resources are in short supply.

The experts' take

When personal data is subject to privacy laws

When we talk about privacy laws and personal information, we are talking about personally identifiable data – information that is linked to an identifiable person such as name, address, social insurance number, etc.

Dr. Ann Cavoukian, Executive Director, Global Privacy & Security by Design Centre

The data perspective: Governance is key

As algorithmic systems are increasingly being used in decision-making processes in both the public and private sectors, there are concerns about their complexity and opacity to those who are impacted. But organizations in Canada are struggling with decisions about the privacy implications of AI because algorithmic systems generally do not fit into their existing governance, privacy, quality, and compliance frameworks. And, until recently, there has been no clear guidance advanced from government or industry.

This is likely to change when the federal government passes Bill C-27, Digital Charter Implementation Act, 2022. As well, Quebec's recent enactment of Bill 64: An Act to modernize legislative provisions as regards to the protection of personal information, addresses decision-making, and transparency issues.

So, with regulators and governments now focusing on governance matters and stronger privacy enforcement, will organizations need to establish data protection programs for AI and ML applications that are compliant with evolving regulations?

Recently, guidelines for responsible AI and ML frameworks have been established by several prominent organizations. These are reliable references from which to build your own. They include OECD AI Principles and Ethics Guidelines for Trustworthy AI from the European Commission.

OECD AI Principles

Value-based principles

- Inclusive growth, sustainable development and well-being
- Human-centered values and fairness
- Transparency and explainability
- Robustness, security and safety
- Accountability

Recommendations for policy makers

- Investing in AI research and development
- Fostering a digital ecosystem for AI
- Shaping an enabling policy environment for AI
- Building human capacity and preparing for labour market transformation
- International co-operation for trustworthy AI

Source: https://oecd.ai/en/ai-principles

Requirements of Trustworthy AI

Ethics Guidelines for Trustworthy AI :
Source: https://ai.bsa.org/wp-content/uploads/2019/09/AIHLEG_EthicsGuidelinesforTrustworthyAI-ENpdf.pdf - page 15

Transparency and accountability are essential to protect your organization and stakeholders. Data leaders need to define an encompassing framework that includes AI/ML bias, quality, privacy, compliance, security, and business rules.

Jason Lee, MNP Digital, Partner and Leader of Applied Data Centre of Excellence

The privacy perspective: Create an ethical foundation

Every decision about how to use personal data has ethical and privacy considerations. To maintain an ethical foundation when utilizing AI and ML requires the following:

- Clearly understanding how these technologies operate — what the technology is doing and what is being produced
- Transparency in how technology is used and how decisions are made
- Preserving data subjects' control over their personal information at all times
- Embedding the principles of privacy and data protection by design into all solutions

The implementation perspective: Supplement internal resources

Many organizations lack sufficient internal resources or knowledge to address ethical and privacy issues in the fast-moving world of algorithms. In these situations, talk with your industry's governing body about involving industry members in an initiative to explore these matters. Or look to academia and institutions that are operating innovation projects with industry partners.

Another option is to partner with experienced privacy professionals and firms that can provide guidance and lessons learned from other enterprises. The more you learn from those who are experiencing similar challenges, the more this intelligence can inform your organization's governance and decision making.

Q: Who is responsible for ensuring algorithms serve the needs of all users and stakeholders?

Leaders' concerns

- There's an efficiency question in terms of enabling the technology while also preserving competitiveness.
- There needs to be more ground level understanding of how decisions are made with data and who makes them.

The experts' take

The program implementation perspective: Integrity comes from the top, down

- Many organizations struggle to effectively leverage AI. The right foundation is key to ensure algorithms achieve organizational goals while also meeting the needs of stakeholders,. These are the essential elements of this foundation: Determine the specific problems you want to solve
- Define the desired outcomes
- Establish performance metrics
- Embrace transparency
- Embed ethics in the development process
- Continually measure metrics and share the value that is delivered to the organization, your customers and other stakeholders
- Address issues and concerns as they arise and aim for continuous improvements

Integrity should cascade from the top down to ensure rigour and accountability when implementing and changing algorithmic systems. Integrity must begin from the top and continue throughout an organization. Consider how to organize teams so they can ensure these systems are accurate and trustworthy as they progress and mature.

The regulatory perspective: The CEO is always accountable

Between January 2020 and 2021, European Union data protection authorities levied fines of US$1.2 billion for breaches of the General Data Protection Regulation (GDPR). A recent ruling by the Court of Justice of the European Union gives consumer groups the right to file representative actions against organizations that may be responsible for infringement of the laws protecting personal data.

Data protection laws and enforcement are getting tougher across the world. Data privacy breaches are costing companies millions of dollars in fines and class action lawsuits.

Regulators are saying: the CEO is accountable, and leaders of enterprises must establish "algorithmic accountability" right from the top to ensure technology meets the needs of stakeholders and does not use data in harmful ways.

A caution for CEOs about the personal information your organization uses

Bill 64 became law last September, bringing Quebec's private sector privacy legislation more in line with Europe's General Data Protection Regulation. British Columbia and Alberta have also updated their privacy laws for the private sector, and other provinces are likely to follow suit.

Quebec's law enables individuals to assert greater control over their personal information and imposes more obligations on organizations processing this personal information. For example, enterprises must obtain consent before communicating personal information to a third party or using this information for any purpose other than the primary purpose for which it was collected.

Bill 64 also requires that organizations designate an individual to be responsible for ensuring compliance with privacy legislation. For private businesses, this person is, by default, the CEO.

The legislation also increases fines for noncompliance with privacy legislation — up to $25 million. This is a significant incentive for CEOs to ensure strict data privacy within their enterprises.

Q: What steps must developers and regulators take to ensure that AI and ML platforms of tomorrow will preserve trust and protect personal sovereignty?

Leaders' concerns

- Cloud and other repositories are collecting huge swaths of data. When AI and ML look at those data repositories, there's a lot going on in terms of ethics and privacy.
- For decision making to achieve better outcomes, organizations are collecting more information than we typically did with manual processes. And there's an appetite to use that data for unconsented secondary purposes to gain insight or provide value to the organization and customers. What should we do about these racing trains?

The experts' take

The solution architect perspective: Collaboration and transparency build trust

To trust decisions made by machines and software, stakeholders need to understand how AI and ML systems work and what they produce.

This requires approaching AI and ML in a transparent, multi-disciplinary way with collaboration throughout an organization to ensure that the best interests of stakeholders are carefully considered. Development teams should be cross-functional, involving data science, engineering, sales, policy, communications, legal, and privacy and security.

Transparency is equally important. Since algorithms are complex, organizations must be open as to what data is being used, how it is used, and for what purposes.

To identify implementation issues early on and ensure the best results, the following tenets are important to keep in mind:

- Aim to design and deploy AI and ML so they fairly affect customers and other stakeholders, while always retaining trust; build compliance and security into the process
- Develop a complete roadmap that includes strategy, data, technology, people, and governance
- Understand applicable policies, principles, standards, and industry best practices and how they map to your models
- Consider AI and ML workflow as a sequential series of steps from data preparation to modeling, simulation, testing, and deployment
- Carefully analyze AI and ML use cases for impact, not just for compliance with legislation, but also from the perspective of ethics and responsibility
- Clearly define metrics
- Conduct robust testing and validation of delivery to ensure accuracy and optimal performance

> Integration is essential to interweave privacy into your operation. Don't have a Chief Privacy Officer over there, and your encryption team over here, and security over there. Consolidate people from all over your organization as a team.
>
> Dr. Ann Cavoukian, Executive Director, Global Privacy & Security by Design Centre

The regulatory perspective: Privacy by Design is the gold standard

As data becomes more important in the global economy and the use of personal data more prevalent, countries are adopting data sovereignty measures to protect citizens' data. Data security and privacy are now essential rights and regulators worldwide are taking measures to ensure that organizations comply with data privacy regulations.

This is what regulators look for:

- Built-in accountability that clearly demonstrates how operations are run
- A clear view regarding the technologies used and how they are overseen
- A documented system demonstrating efforts to follow appropriate regulations
- Mature processes to monitor and report on privacy risks over time
- Clear procedures to receive and respond to privacy complaints

Have you integrated Privacy by Design into your operations?

Too many organizations implement privacy processes as an afterthought, which can result in inefficiencies and barriers to building value.

Privacy by Design is a more productive approach, proactively embedding privacy assurance into systems, operations, and practices.

The seven foundational principles of Privacy by Design enable organizations to comply with relevant privacy legislation, build stakeholder trust and create competitive advantage.

Source: https://www.researchgate.net/figure/Seven-fundamental-principles-of-privacy-by-design-35_fig2_339790418

Enhancing privacy and security will enhance your business interests – it will strengthen operations, promote data utility and attract new opportunities.

Dr. Ann Cavoukian – Executive Director, Global Privacy & Security by Design Centre
Creator of Privacy by Design, Three-term Information and Privacy Commissioner of Ontario

Q: Some provinces are introducing privacy regulations: What should we be thinking about?

Leaders' concerns

- Quebec has introduced sweeping new privacy legislation — what's in store for the rest of the country and how should we prepare?

The experts' take

The regulatory perspective: Big changes to privacy legislation across the country

There is a proliferation of legislation governing data worldwide. Given that most come with punitive enforcement, it is important for private and public sector organizations to stay abreast of what is happening in this changing environment. Here are some of the recent changes in this country.

Federal Government

In June, the federal government tabled *Bill C-27, Digital Charter Implementation Act, 2022*, updating the private sector privacy law regime that protects citizens' personal information and regulates privacy practices of organizations. This will implement the *Consumer Privacy Protection Act (CPPA)* to replace the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, which has been in force since 2001. Here are the highlights.

- **Enforcement:** A new Personal Information and Data Protection Tribunal can impose penalties for noncompliance representing the greater of three percent of an organization's global gross revenues or $10 million. There are also higher fines in the case of penal proceedings: the greater of three percent of an organization's global gross revenues or $25 million.
- **Rights:** There is a new private right of action for individuals, new provisions for codes of practice and certification programs, and new individual rights — the right to be informed of automated decision-making, the right to disposal, and the right to mobility.
- **Accountability:** There is a new definition of control — an obligation for organizations to establish a privacy management program, and greater clarity about the role and responsibilities of service providers.
- **Consent:** There is clarification regarding valid consent.

Quebec

The province passed Bill 64 last year and when it came into effect in September 2022, Quebec had a fundamentally new GDPR-inspired law with massive penalties for noncompliance of up to eight percent of annual worldwide turnover for repeat offenders.

While the bill is an omnibus legislative package, the most significant amendments reform the Private Sector Act, which regulates the collection, use and disclosure of personal information by private organizations. Among the key provisions are the following:

- Major penalties of up to eight percent of annual worldwide turnover for repeat noncompliance offenders
- New cyber incident reporting obligations, including a requirement to notify individuals if a confidentiality incident poses a "risk of serious injury," as well as to take reasonable measures to reduce the risk or injury and to prevent new incidents
- New transparency and consent standards requiring that consent be clear, free, informed, and provided for specific purposes

Ontario

- The province released a white paper, Modernizing Privacy in Ontario, in June 2021. The proposals suggest implementing rights, enforcement, and penalties similar to the strict requirements of the GDPR — and stricter than those proposed in the federal Consumer Privacy Protection Act (CPPA). To date, no announcements have been made regarding the next phase of this privacy regime.

Other provinces

- Other provinces are likely to follow the federal government and Quebec in updating privacy and data protection statutes.

The privacy perspective: It is all about personal control

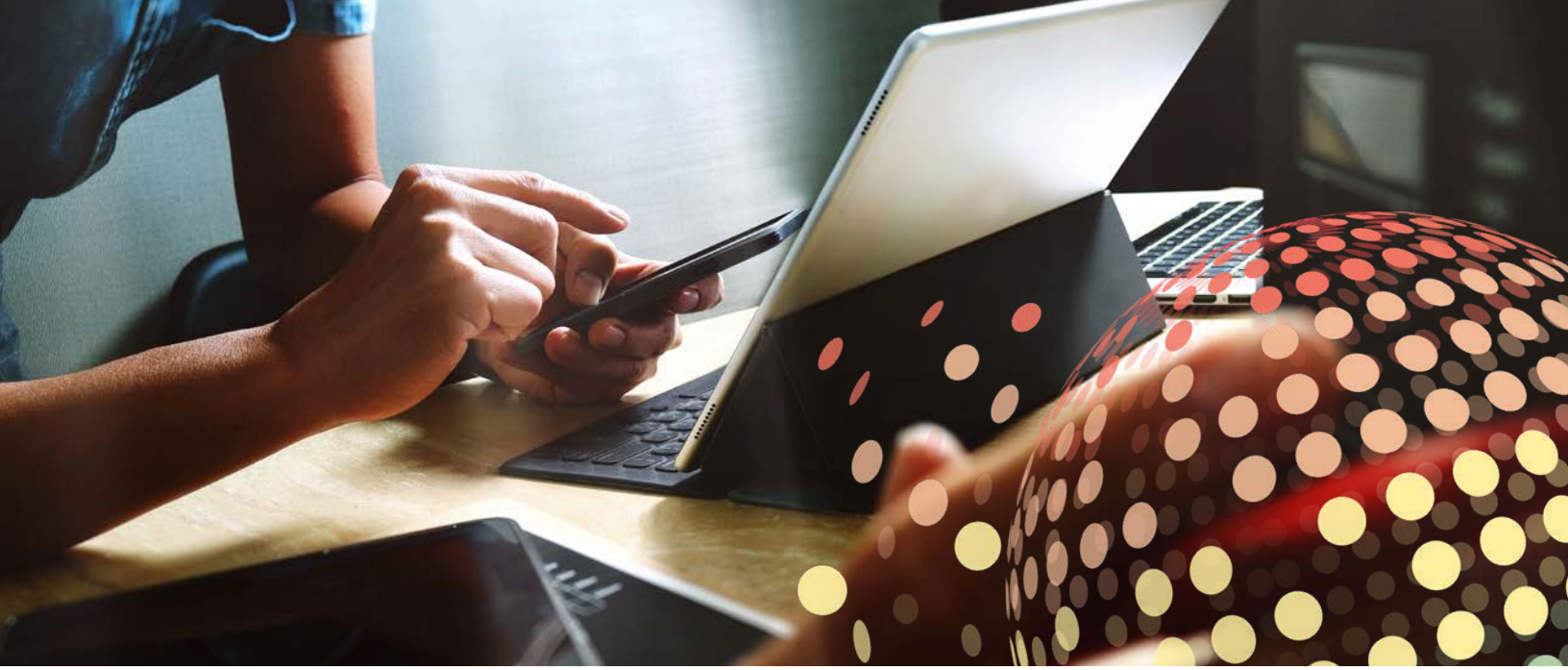
While it is important to understand the regulations that apply to your organization, it is equally important to approach privacy more broadly. Privacy is about individuals having control over the use and disclosure of their personal information, so consider the following.

- Do your customers — your data subjects — have control over their personal information?
- Are they aware of the ways in which your organization is using their personal data?
- Have they consented to this?
- If there are secondary uses for this data, have you obtained their additional consent for these uses?

These are the issues that regulations are addressing. Privacy and security are expected to be baked into all systems and processes.

> There's recognition that users should not be expected to navigate complex privacy settings. So, regulators are moving toward putting the onus on providers to be transparent regarding how their privacy protocols work.
>
> Adriana Gliga-Belavic – MNP Digital, Partner and National Privacy Leader

Enabling personal control of data, obtaining consent, protecting sensitive data while preserving data utility for AI and ML — these precautions enable organizations to comply with regulations, and also to realize all the advantages of digital transformation.



Key takeaways regarding privacy, ethics, and the future of AI

Data privacy policy is essential. Having a data privacy policy is not only a protective measure, it also reinforces the reputation of your organization as being trustworthy. Since most people are very concerned about government and business data overcollection, establishing policies that commit to data privacy enhances the value of your brand.

Lead with transparency. Inform stakeholders about the measures you are taking to protect their personal information. When people know what you are doing and see an organization making a real effort to communicate this, you build trust.

Always obtain consent for secondary use of data. As data is used for more purposes, the secondary use of personal information is becoming more common. Increasingly, privacy regulations are addressing these uses. But it is equally important to be proactive. Even where notification regarding the use of personal information is not required by law, it is unfailingly good policy to seek the consent of individuals when using their personal information for any secondary purpose.

Continually reinforce security maturity. As cyber and other security threats increase in volume, complexity and severity, organizations must aim to continuously improve security maturity — your security position relative to your risk environment.

> While it's not possible to prevent cyber breaches, when you are prepared with an appropriate security maturity level, such as security by design or Privacy by Design, in the event of a breach you are able to provide stakeholders with reassurance — clear information regarding what happened, how you dealt with it, and the other steps that you're taking. This way, you gain their trust.
>
> Danny Timmins – MNP Digital, Partner and National Cyber Security Leader

MNP DIGITAL

Transform data privacy and security into a competitive advantage

Is your organization exploring issues or next steps related to privacy, ethics, or artificial intelligence?

As you aim to capitalize on new technologies and innovations to add value and deliver results, we would be pleased to discuss your challenges, your expectations and how to transform your data, privacy, and security into a competitive advantage.

Contact our advisors for a free consultation or visit us at MNPdigital.ca to get started.

Adriana Gliga-Belavic
National Privacy Leader
adriana.gliga-belavic@mnp.ca
647.480.8489

Danny Timmins
National Cyber Security Leader
danny.timmins@mnp.ca
905.247.3290

Gold
Microsoft Partner
Microsoft