Privacy-Proof Your AI Technology

Leverage your privacy program to enable your AI projects.

INFO~TECH
RESEARCH GROUP

Your Presenter

Aaron Shum
Vice President - Research
Security & Privacy

Privacy-Proof Your AI Technology

Agenda

AI Primer

Data Privacy Primer

Challenges

Solutions

Questions

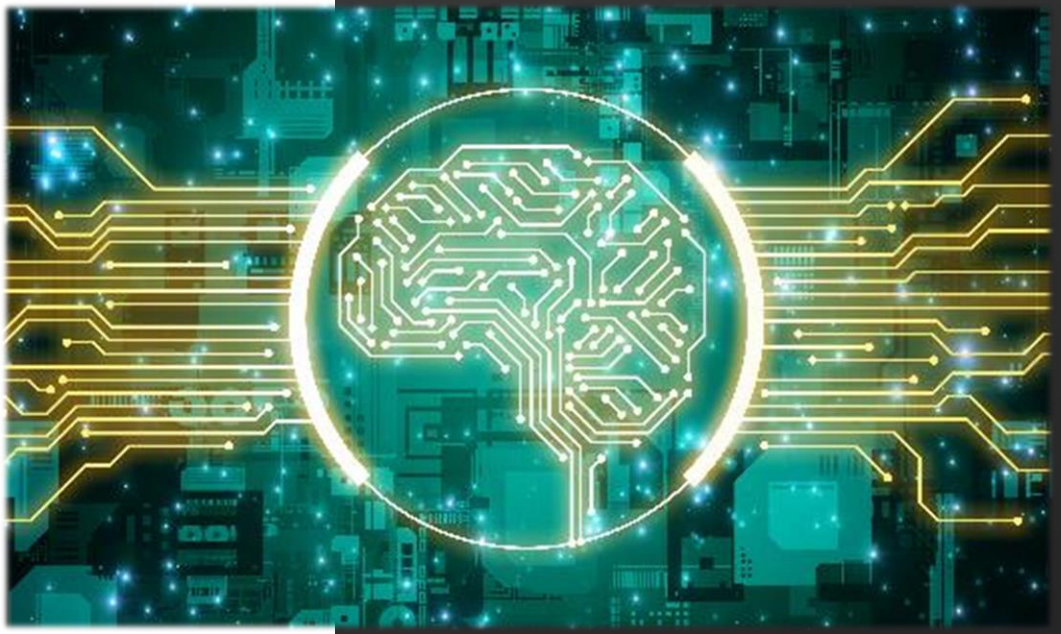
Let’s start with AI Technology...

Advantages and applications of AI

Artificial Intelligence is no longer limited to sci-fi and big tech

- AI:
  - Enable machines to perform the **activities of humans**;
  - Enable machines to **think and reason as humans do**;
  - Enable machines to **think and work without relying on human reasoning**.
- One of the sub-sets of AI has become increasingly leveraged by larger organizations looking to build intelligent systems and capabilities from data; this is widely known as machine learning.

Three out of **four** C-suite executives believe that if they don't scale Artificial Intelligence (AI) in the next five years, they risk going out of business entirely.[1]



[1]Accenture: AI Built to Scale, 2019

Applying *General Artificial Intelligence*

There are many ways in which we can break down Artificial Intelligence, including the following four commonly known subsets.

Machine Learning

The use of algorithms and data to assist computers in learning tasks or performing functions, without necessitating specific programming parameters. There are many types of ML currently used, including:

- Supervised Learning
- Unsupervised Learning
- Reinforced Learning

Computer Vision

A discipline within AI that bridges the gap between computers and the external visual environment. The purpose of computer vision is to move beyond simply translating a group of pixels into a corresponding image, but to incorporate classification and segmentation of images. Social media companies' use of computer vision has been rampant in past years through facial recognition features.

Natural Language Processing (NLP)

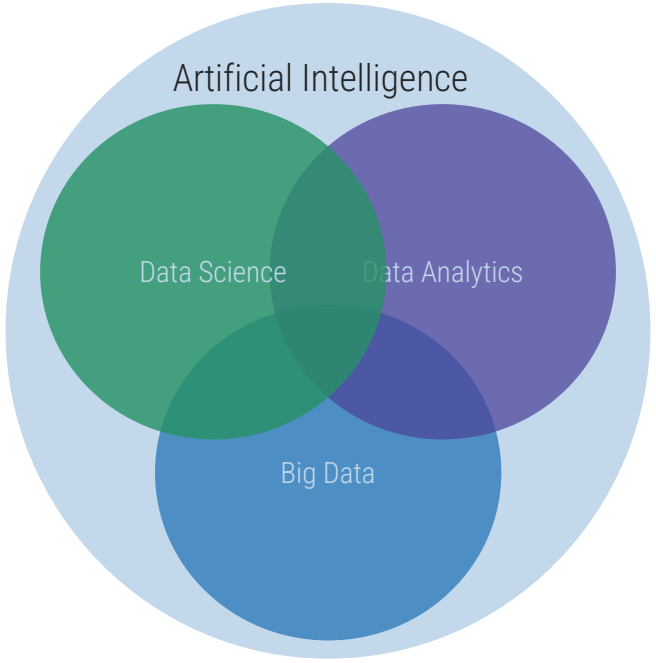
A subset of AI that involves the machine interpretation and replication of human language. NLP focuses on the study and analysis of linguistics as well as other principles of Artificial Intelligence to create an effective method of communication between humans and machines or computers.

Robotic Process Automation (RPA)

The focus of RPA is to drive business efficiency through automation of low-skilled, tedious operational tasks. The result is two-fold; business leaders can shift focus to high-effort, high-skills tasks, while simultaneously reducing the number of human errors that occur as a part of a supply chain. Organizations can leverage RPA as a part of **Intelligent Automation (IA),** which includes the automation of multiple steps within a value chain.

Data (R)evolution

Data's role in organizational operations has continued to shift from simple analytics to complex predictive learning techniques.



Business Intelligence	Involves a set of strategies based in technology that enable in-depth yet broad-reaching analysis and assessment of current and historical business information/data to help business and IT leaders make effective, informed, strategic decisions.
Data Science	The study of data and the related actions of cleansing, preparing, and analyzing. The objective of data science is to derive a set of insights from large sources of data (unstructured and structured).[1]
Big Data	High-volumes of data (unstructured and structured) unable to be stored centrally in one location. Often leveraged with the intent of providing insights and strategic guidance for future business processes.
Data Analytics	The science of assessing data in order to derive a conclusion or come to an analytical solution. Data analytics often draws on algorithmic processes in order to provide guidance regarding correlations that exist within the data set(s).
Artificial Intelligence	The Oxford English dictionary defines Artificial Intelligence as, "The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages."

Source: [1]SimpliLearn

Operational augmentation through data

AI drives business value through analysis and insight

- AI focuses on driving improvements in **efficiencies** within operational processes that already **exist** in the business context.
- The proliferation of **Artificial Intelligence** is built on the collection and analysis of mass amounts of data and the ability to synthesize this data to create learning models.
- "Good" or effective AI requires data inputs that are **reliable, valid,** and of **high volume** to derive accurate and representative models.
- As a result, there exists a strong link between **AI** and **data science** and **data analytics**. However, this does not mean that the two fields are mutually exclusive.
- It is imperative that organizations looking to leverage AI within the context of their operations have a strong **understanding** of the data environment.
- This requires IT and business leaders to take a step back and reexamine the current environment from the perspective of **"what do we have, where is it located, and how can we use it?"** before leaping too far down the AI rabbit hole.

"It is a capital mistake to theorize before one has data. Insensibly, one begins to twist the facts to suit theories, instead of theories to suit facts."

– Sherlock Holmes

Industry use-cases for AI

AI is no longer limited to tech companies; businesses globally have introduced AI technologies into their daily operating models.

Financial Services

- Fraud detection
- Regulatory compliance
- Automated customer service offerings
- Financing and loans
- Internal audit

Healthcare

- Diagnostics
- Clinical trials
- Improvements in patient experience
- Robotic assistance in surgical procedures
- Disease management

Retail

- Sales and CRM applications
- Customer recommendations
- Manufacturing
- Logistics and delivery
- Payments and payment services

Manufacturing

- Assembly line integration
- Supply chain management
- Automated QA
- Predictive maintenance

Info-Tech Insight

Learn from the ones who came before you. After you've identified your organization's data posture, examine the different use-cases based on your relevant operating industry. Evaluate how industry leaders have successfully and/or unsuccessfully integrated privacy-proof AI technology. Draw on both the beneficial outcomes and techniques to prepare your organization and weed out irrelevant or high-risk use-cases.

Industry Case Study: Financial Services

JP Morgan Chase

JPMorgan Chase & Co.

INDUSTRY
Financial Services

SOURCE
Emerj, imaginovation

A major player in the financial services industry, JPMorgan Chase used a significant increase in its technology budget to take advantage of the unique ways that AI is leveraged in this industry:

- Contract Intelligence (COiN)
- Emerging Opportunities Engine (Predictive Analytics)
- Chatbots

Results

- Since introducing the Contract Intelligence (CoiN) chatbot in 2017, the business has been able to reduce manual review processes for commercial credit agreements.
- The success of the chatbot feature enabled reduction in service desk hours spent on responding to employee tech service requests.

↓ **360,000**

Hours per year spent on tasks such as interpreting commercial-loan agreements REDUCED through the COiN implementation. The COiN infrastructure leverages unsupervised machine learning, necessitating minimal human interaction throughout its lifecycle post-deployment.

↑ **7%**

Increase in the company's per annum technology budget (9% of projected revenue) devoted to covering the cost of new tech initiatives (from 33% - 40%).

Industry Case Study: Retail

INDUSTRY
Retail

SOURCE
EMERJ, MarketingMag

The North Face + IBM's Watson

Outdoor apparel brand The North Face integrated Expert Personal Shoppers (XPS) software, which leverages the well-known tech giant IBM's Watson for its eCommerce customer engagement capabilities. Watson's machine-learning **cognitive computing technology** has been used by retailers globally to help streamline the customer purchase experience.

Why? Online retailers face a large problem when it comes to the number of shopping carts that are left orphaned prior to purchase completion. The intention was that through an interactive UI and customized shopping experience, the rate of carts left unpaid for at the end of a shopper's journey would be vastly reduced.

The technology assisted customers in selecting the best jacket for their purposes, using a range of inputs including location, activity, and lifestyle preferences.

Results

Though the initial pilot program boasted click-through rates of 60% and sales conversions of 75%, the integration showed its infancy in errors such as the customer's final selected item not being available in the requisite size.

Source: Emerj: AI Sectors Overview

The above image shows the user interface leveraged by The North Face to streamline the customer experience through a set of qualifying questions that helped determine the ideal outerwear jacket.

Industry Case Study: Healthcare

INDUSTRY
Healthcare

SOURCE
The University of Vermont, Quartz

Vermont Conversation Lab

Machine learning and natural language processing were used in order to assess the conversation techniques used during both caregiver/doctor to patient conversations, as well as clinical consultations for palliative care patients.

Bob Gramling and a supporting team undertook the task of studying palliative care conversation patterns in efforts to better understand the impact of communication within the end-of-life patient journey. This included analyzing emotions conveyed in conversations, silence and moments of pause, and resulting reactions from patients. The intent of this study was to use AI to automatically detect the emotional connection that occurs between doctors and patients to better train medical professionals in the field of palliative care.

Results

The machine-learning project resulted in the collection of over 12,000 minutes of palliative care patient conversations, consisting of 1.2 million words from 231 patients. The NLP palliative care consultations project collected over 350 conversations from the Palliative Care Communication Research Institute.

$34 billion

Revenue opportunity for the healthcare AI market by 2025.

$8.6 billion

In projected revenue generated through the use of 22 healthcare AI tools by 2025.

- Medical Image Analysis
- Computational Drug Discovery
- Healthcare VDAs

The top three use-cases for healthcare AI.

Source: Tractica

Industry Case Study: Utilities

INDUSTRY
Public Sector

SOURCE
Intel

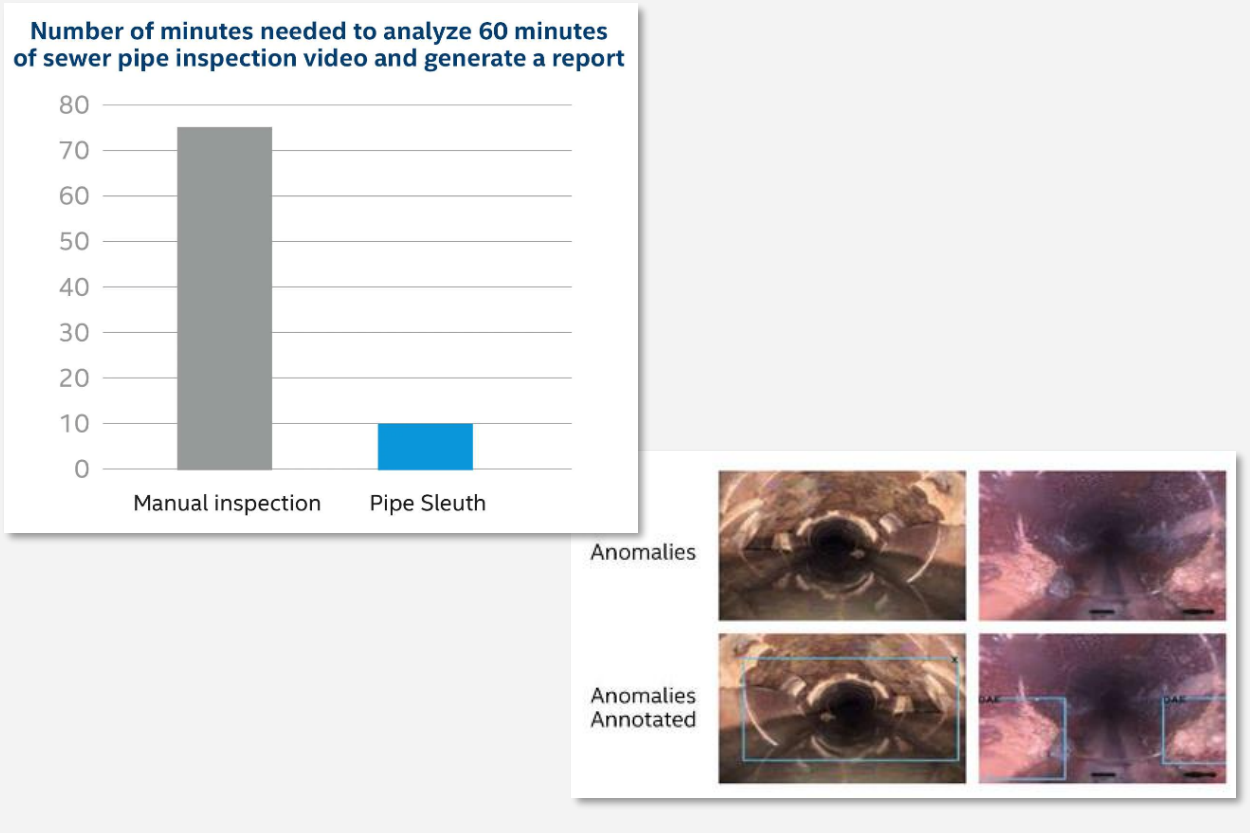
DC Water

With more than 1,800 miles of sewer pipes under Washington, D.C., 701,000 residents and nearly 20 million annual visitors, the aged utility system dating back to 1810 is a challenging infrastructure to support. The standard inspection process is onerous and cumbersome, where operators use video recording to produce inspection logs and summary reports, flagging anomalies or problems for quality control staff to pore through in real-time, leading to errors due to staff fatigue from this manual process.

To solve this problem, DC Water worked with Wipro and Intel to develop an AI-based solution to develop Pipe Sleuth, a Computer Vision solution comprising of a machine learning model trained from 26,600 annotated image sources. Pipe Sleuth compares new pipe inspection videos with established anomalies to replace the previously manual process.

Results

The Pipe Sleuth implementation helps detect 50 anomalies in the wastewater utility infrastructure, with a plan to support additional anomalies to further save time, increase accuracy from human errors, reduce up to 50% in scanning costs and ultimate contribute up to 350% ROI over a three-year period.



Questions / Discussions

What other innovative use of AI have you been considering?

What other areas of opportunity do you see with AI?

What other organizational benefits have you seen where AI played a key role?

About Data Privacy...

Privacy is all about personal data

When building a privacy program, focus on all personal data, whether it's publicly available or private. This includes defining how the data is processed, creating notices and capturing consent, and protecting the data itself. On the converse side, an effective privacy program also enables accessibility to information based on regulatory guidance and appropriate measures.

See examples of personal data in the below charts:

Traditional PII Personally Identifiable Information	**Personal Data** Any information relating to an identified or identifiable person	**Sensitive Personal Data** Special categories of personal data (some regulations, like CPRA, expand their scope to include these)
Full name (if not common)	First, middle (if applicable), last name	Biometrics data: retina scans, voice signatures, or facial geometry
Home address	IP address	Health information: patient identification number or health records
Date of birth	Email address or other online identifier	Political opinions
Social security number	Social media post	Trade union membership
Banking information	Location data	Sexual orientation
Passport number	Photograph	Religious or philosophical beliefs
Etc.	Etc.	Ethnic origin

The current state of privacy frameworks

A perspective on the proliferation of privacy law

Federal/National Privacy Regulation

GDPR

Cross-border data transfer safety, and data privacy rights of EU citizens

CCPA / CPRA

Consumer rights and consent to personal data use

PIPEDA

Privacy rights document for private sector organizations

Industry Privacy Regulation

HIPAA

National standard for privacy governance of health-specific documentation

GLBA

Federal law for financial institutions pertaining to customer data privacy

FERPA

Enforces data privacy and consent of students and their parents

Information Security Privacy Framework

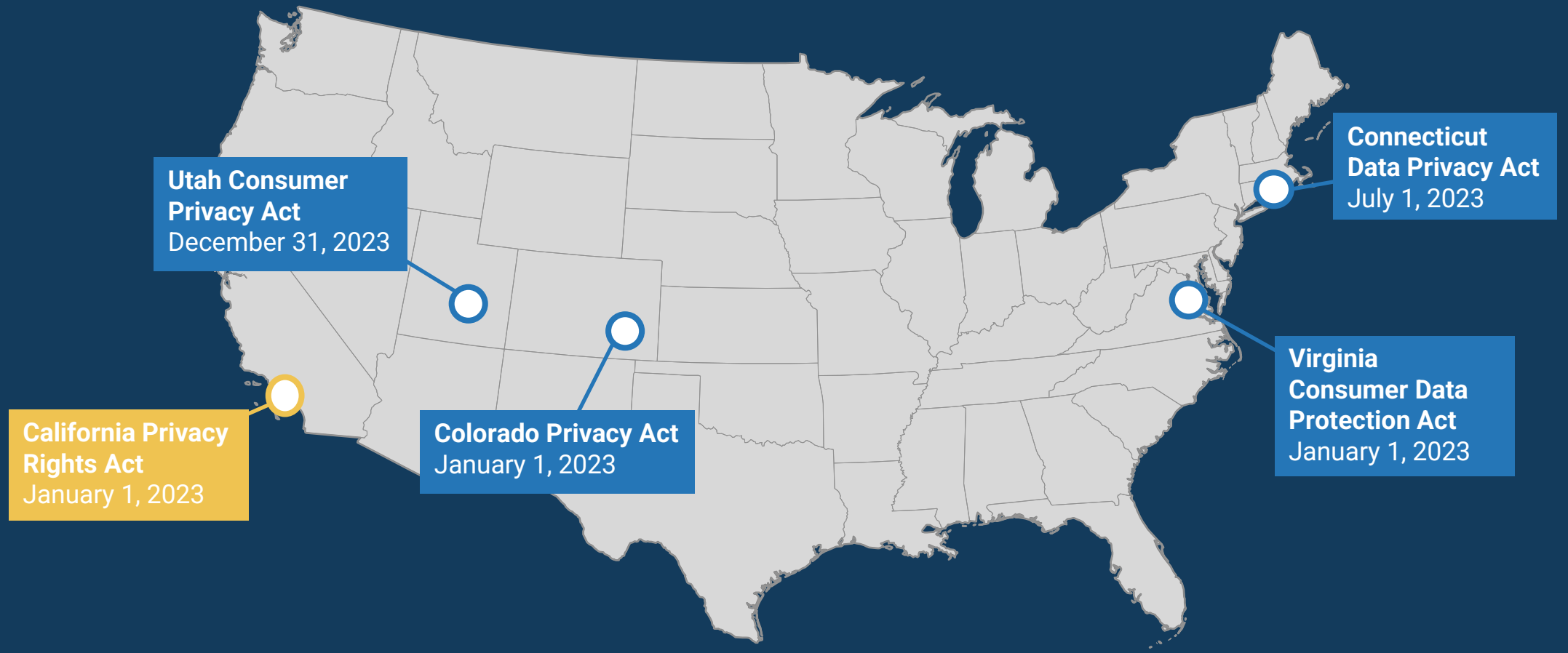
NIST Privacy Framework

Privacy framework mapped across five functional areas that encourages proactive privacy planning

ISO/IEC 27701

Operational controls mapped against GDPR articles for organization's specific compliance requirements

The US privacy landscape is changing



The US privacy landscape is changing

Federal Data Privacy Legislation

American Data Privacy and Protection Act

is coming…

What is CPRA and what does it mean?

The California Privacy Right Act (CPRA) is a state-wide privacy regulation passed in 2020 to supplant the California Consumer Privacy Act (CCPA). The CPRA takes effect on January 1, 2023, with a lookback period from January 1, 2022.

The CPRA introduces new concepts to data privacy in California. Concepts that draw the regulation closer to EU's GDPR, expand consumer rights, and close potential loopholes in the previous version of CCPA.

of companies that were required to comply with CCPA were unprepared in 2022.

What's new in CPRA

Business Scope

- **Buying,** selling, **or sharing** of **>100,000 consumers** or households *(addition of buy and share, increase from 50,000 to 100,000)*
- **Businesses, contractors, service providers,** and **third parties**

Data Governance

- **Data minimization, data retention,** and **purpose limitation** are now required for all businesses
- **Privacy risk assessments and cybersecurity audits** are now required

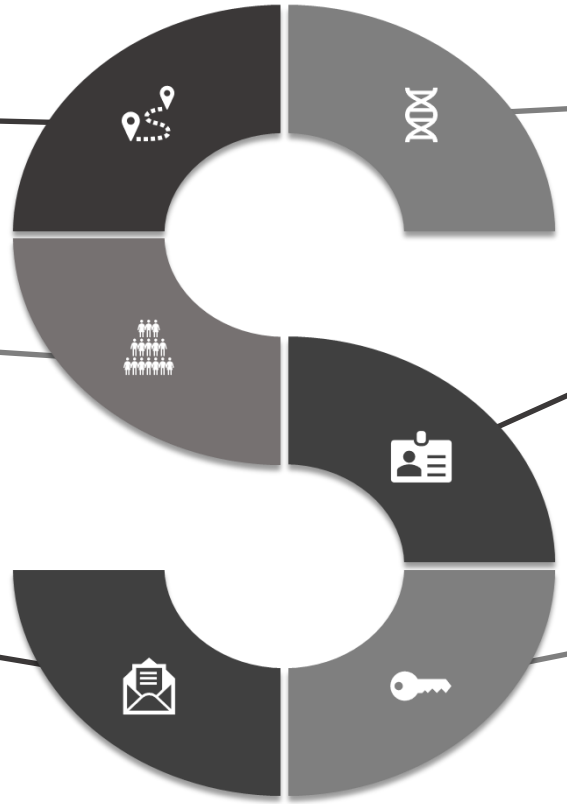
Consumer Rights

- **Additional** consumer rights
- **Correct** their Personal Information (PI)
- Limit the use of their **sensitive PI**, opt-out of the "selling" and "sharing" of their PI
- Access to information about **automated decision making**

Enforcement

- Automatic **$7,500 fine** per violation involving **children's data**
- Consumers can now file complaint with a **dedicated enforcement agency (CPPA)**

Sensitive personal information – NEW



Geolocation

A consumer's precise geolocation.

Genetics

A consumer's genetic data.

Diversity, Equity, Inclusion

A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.

Identifications

A consumer's social security, driver's license, state identification card, or passport number.

Communication Mode

The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

Authentication

A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

Question: which of these concern use of AI?

Business Scope

- ❑ **Buying,** selling, **or sharing** of **>100,000 consumers** or households *(addition of buy and share, increase from 50,000 to 100,000)*
- ❑ **Businesses, contractors, service providers,** and **third parties**

Data Governance

- ❑ **Data minimization, data retention,** and **purpose limitation** are now required for all businesses
- ❑ **Privacy risk assessments and cybersecurity audits** are now required

Consumer Rights

- ❑ **Additional** consumer rights
- ❑ **Correct** their Personal Information (PI)
- ❑ Limit the use of their **sensitive PI**, opt-out of the "selling" and "sharing" of their PI
- ❑ Access to information about **automated decision making**

Enforcement

- ❑ Automatic **$7,500 fine** per violation involving **children's data**
- ❑ Consumers can now file complaint with a **dedicated enforcement agency (CPPA)**

Question: which of these concern use of AI?

Business Scope

- ❑ **Buying,** selling, **or sharing** of **>100,000 consumers** or households *(addition of buy and share, increase from 50,000 to 100,000)*
- ✓ **Businesses, contractors, service providers,** and **third parties**

Data Governance

- ✓ **Data minimization, data retention,** and **purpose limitation** are now required for all businesses
- ✓ **Privacy risk assessments and cybersecurity audits** are now required

Consumer Rights

- ❑ **Additional** consumer rights
- ✓ **Correct** their Personal Information (PI)
- ✓ Limit the use of their **sensitive PI**, opt-out of the "selling" and "sharing" of their PI
- ✓ Access to information about **automated decision making**

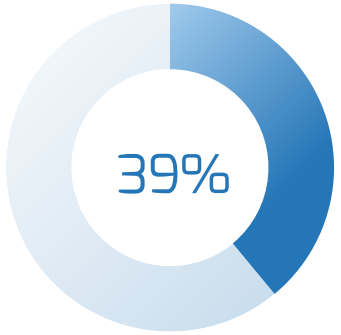
Enforcement

- ✓ Automatic **$7,500 fine** per violation involving **children's data**
- ❑ Consumers can now file complaint with a **dedicated enforcement agency (CPPA)**

Data privacy as a barrier to AI

The AI Integration vs. Data Privacy Regulation Debate

- ✓ Profiling
- ✓ Automating
- ✓ Minimizing
- ✓ Defined Period of Retention
- ✓ Transparency
- ✓ Right to Explanation
- ✓ Purpose or Intent
- ✓ Consent

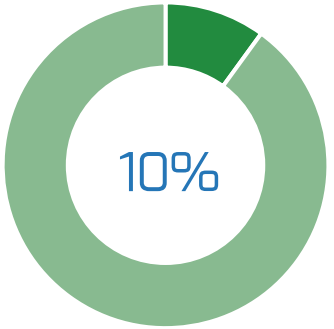


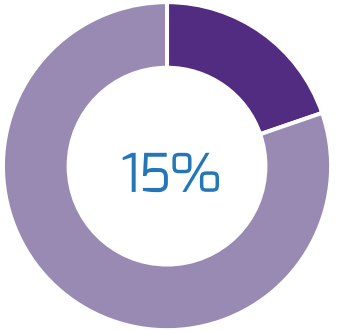
Of business leaders cite consumer concerns about privacy and use of data as a primary trust issue with respect to AI in a business context.

Source: Statista, Trust Barriers related AI / Data Privacy, 2019

Of cybersecurity professionals surveyed cited elevated cybersecurity risks as a key obstacle to AI implementation.

Source: SANS Institute/Cylance, Security Gets Smart with AI, 2019





Of the same surveyed professionals plan to use AI as a key enabler in regulatory compliance efforts.

Source: SANS Institute/Cylance, Security Gets Smart with AI, 2019

Data Privacy versus Artificial Intelligence

AI vs. HIPAA

- HIPAA's regulations under "notices and consent" state that "Individuals must provide written authorization for use and disclosure of any PHI that is not for treatment, payment, or healthcare operations (or other reasons listed in HIPAA)."
- HIPAA only applies to a subset of healthcare providers and, as a result, significant amounts of health-related information and data is being collected and leveraged through AI without explicit consent.
- Organizations that process personal health information **not technically considered PHI** (i.e. fitness applications, genetic testing companies) and leveraging AI applications must take appropriate precautions to adequately protect data.

AI vs. EU GDPR

- Article 22(1) of the GDPR under "Automated Decision Making" states that **"The data subject shall have the right not to be subject to a decision based solely on automated processing,** including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."
- As a result, organizations leveraging AI technology must be able to validate and explain the process by which automated decisions are made to the respective data subjects.
- Article 6 of the GDPR outlines the requisite **six Lawful Bases for processing;** this must be defined for AI processes that leverage personal data.

AI vs. CPRA

- The CPRA restricts personal information collected by businesses to that which is "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected." **This limits aggregation of personal data to be used in building AI models.**
- The CPRA allows businesses to collect personal information only for "specific, explicit, and legitimate disclosed purposes" that are disclosed in advance to consumers.
- Consumers now have the right to access information about how companies use **automated decision-making** technology. The CPRA allows consumers the **right to opt-out** of any automated decision-making processes.

Google Search:

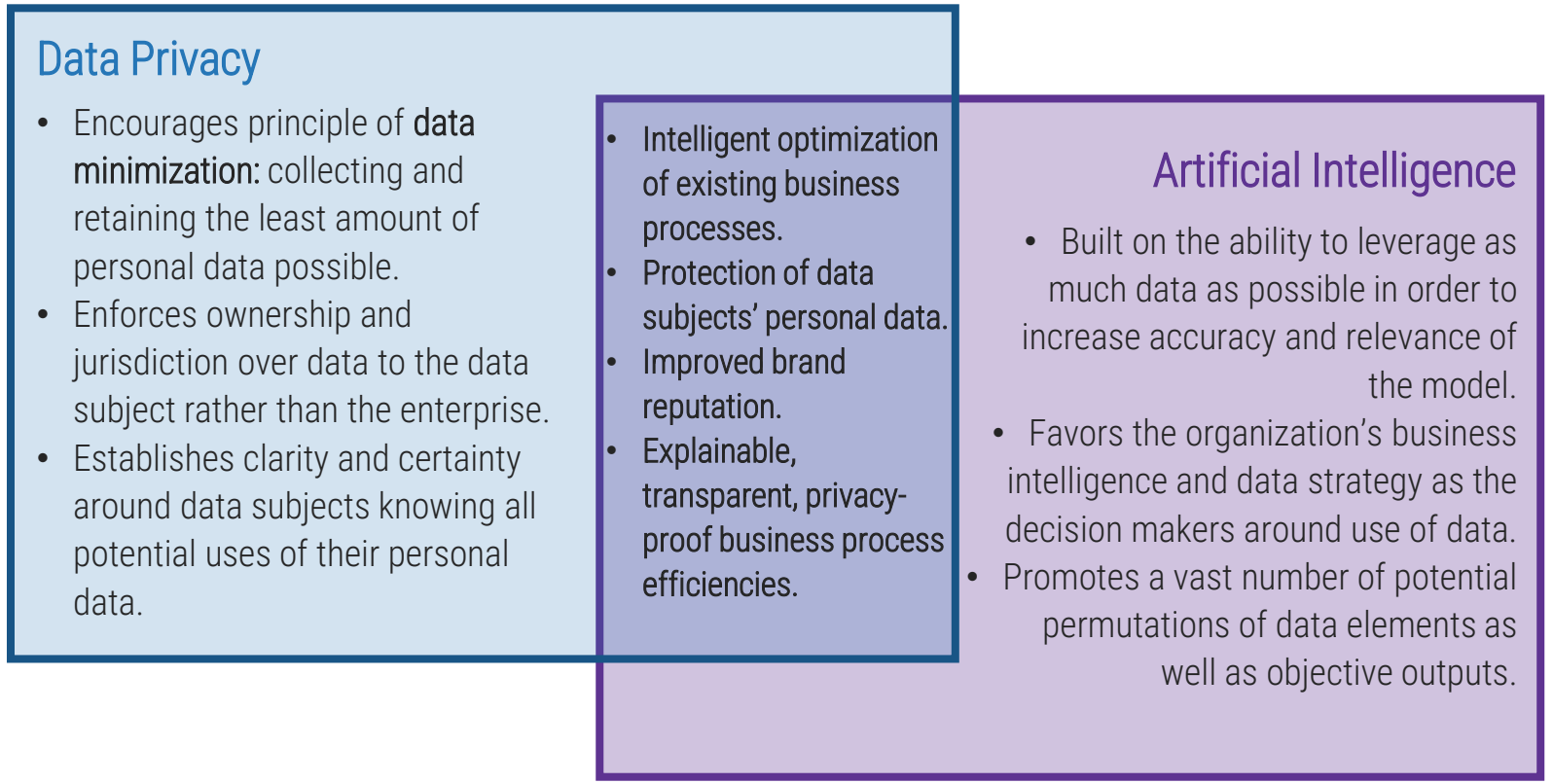
“Artificial Intelligence and Data Privacy”

Analyst Perspective

Effective data governance and data privacy strategy leads to well-designed AI implementation.

The AI versus data privacy debate

An increase in the commoditization of data has resulted in heavy scrutiny around the use of personal data as a part of developing Artificial Intelligence technologies.



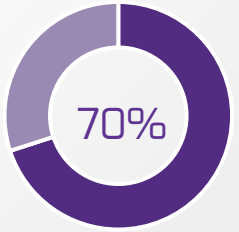
"As artificial intelligence evolves, it magnifies the ability to use personal information in ways that can intrude on privacy interests by raising analysis of personal information to new levels of power and speed."

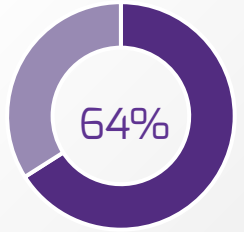
Source: Brookings – Protecting privacy in an AI-driven world

Your challenge

- Develop a set of relevant use-cases for AI implementation based on the industry and nature of the organization's business
- Eliminate inefficiencies by streamlining less-skilled tasks through use of AI
- **Retain trust of workforce through ethical AI implementation**
- Create or revise the current data governance structure within the context of the business
- Align the data-privacy requirements of the organization with the scope of the external regulatory environment
- Ensure that data privacy becomes a standard pre-planning process involved in all technology implementation projects

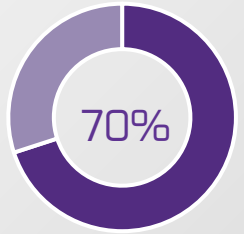
Of surveyed US workers have a positive outlook on the integration of AI technologies in their workplace





Of this surveyed group believes AI will make them more efficient in their specific job functions.

Of these employees trust their employers' ethical use of AI



Source: Cision on Genesys Survey

"As artificial intelligence evolves, it magnifies the ability to use personal information in ways that can intrude on privacy interests by raising analysis of personal information to new levels of power and speed."
Cameron Kerry

Explainable AI (XAI)

"The 'black box' problem that plagues AI — our inability to peek inside exotic neural networks and understand how they work — represents one of the most urgent moral and business imperatives of our time."

Sheldon Fernandez, CEO/Founder of DarwinAI

- XAI solutions should aim to:
  - Maintain objectivity in the chosen approach to evaluation
  - Inspect actions taken by AI technologies to arrive at decision output
  - Maintain accuracy in prediction models for future reference
  - Promote traceability in how models come to decisions
  - Apply discretion in level of explainability in models depending on the volume and sensitivity of data processed and magnitude of the output decision

Source: GIGAOM, A Deep Dive Into XAI

Making AI explainable for data privacy

With the right framework, data privacy and AI can peacefully coexist

"The future of AI lies in enabling people to collaborate with machines to solve complex problems. Like any efficient collaboration, this requires good communication, trust, and understanding."

Freddy Lecue, Explainable AI Research Lead – Accenture Labs

ICO Framework: explaining decisions made with AI

The ICO and the Alan Turing Institute's release provides organizations with a set of steps to better understand the effects and privacy implications of AI-assisted services or products.

1. The Basics of Explaining AI
   - *Legal framework*
   - *Benefits/risks*
   - *Principles*
2. Explaining AI in Practice (Tasks)
   - *Data collection/prioritization best practices*
   - *Build the system*
   - *Prepare to deploy*
   - *Present the explanation*
3. What Explaining AI Means for the Organization
   - *Roles and functions for explaining AI*
   - *Policies, procedures, documentation*

Source: ICO – Explaining Decisions Made with AI

Case Study: Nvidia leads by example with privacy-first AI

INDUSTRY
Technology (Healthcare)

SOURCE
Nvidia, EWeek

Nvidia

Leading player within the AI solution space, Nvidia's Clara Federated Learning provides a long-awaited solution to a privacy-centric integration of AI within the healthcare industry.

The solution safeguards patient data privacy by ensuring that all data remains within the respective health-care provider's database, as opposed to moving it externally to cloud storage. A federated learning server is leveraged in order to share data, completed via a secure link. This framework enables a distributed model to learn and safely share client data without risk of sensitive client data being exposed and adheres to regulatory standards.

Clara is run on the NVIDIA EGX intelligent edge computing platform. It is currently in development with healthcare giants such as the American College of Radiology, UCLA Health, Massachusetts General Hospital, as well as King's College London, Owkin in the UK, and the National Health Service (NHS).

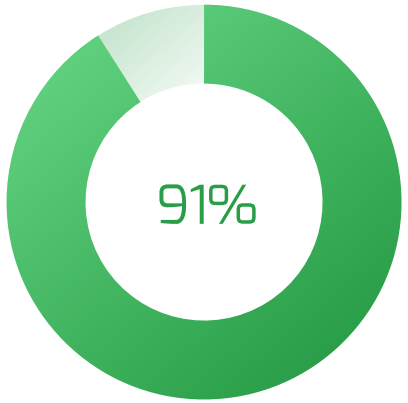
Nvidia provides solutions across its product offerings, including AI-augmented medical imaging, pathology, and radiology solutions.

Personal health information, data privacy, and AI

- Global proliferation in data privacy regulations may be recent, but the realm of personal health information is most often governed by its own set of regulatory laws. Some countries with national data governance regulations include health information and data within special categories of personal data.
  - HIPAA – Health Insurance Portability and Accountability Act (1996, United States)
  - PHIPA - Personal Health Information Protection Act (2004, Canada)
  - GDPR – General Data Protection Regulation (2018, European Union)
  - CPRA – California Privacy and Rights Act (2023, California)
- This does not prohibit the injection of AI within the healthcare industry, but it calls for significant care in the integration of specific technologies due to the highly sensitive nature of the data being assessed.

Integration: How business and IT leaders see AI within the context of their operations

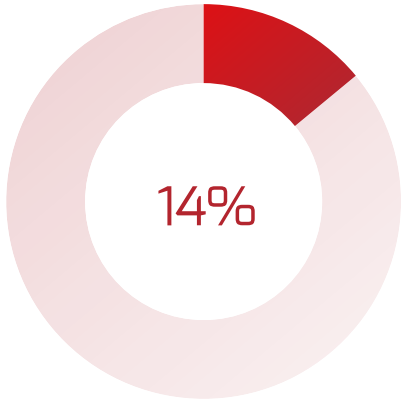
The rapid proliferation of AI is met with trepidation as organizations carefully examine the challenges associated with implementation.



Of over 700 surveyed C-suite executives, **believe that AI will enable them to outpace their competitors** in coming years.

Source: Forbes Insights

Of this same group of executives believe their data is ready and available organization-wide.



Source: Forbes Insights

Data Strategy drives AI readiness.

Only 12% of executives state their organization currently has, and is executing, a company-wide data strategy. Challenges to data strategy development only delay the ability to scope down and adapt AI technology to fit the needs of the organization.

Info-Tech Insight

Data first, AI second. Effective AI implementation is built on a simplified and consistent approach to managing company data.

Data governance as an enabler of AI

Integrity, quality, and **security** of data are key outputs of data governance programs, as well as pre-requisites for effective AI.

Data Governance in Action

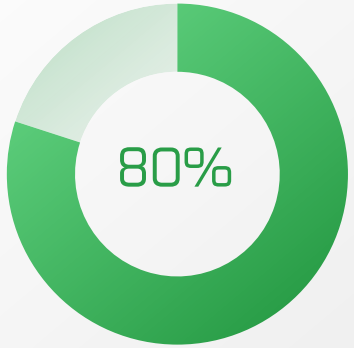
Canada has recently established the Canadian Data Governance Standardization Collaborative governed by the Standards Council of Canada. The purpose of which is multi-pronged:

a) Examines the foundational elements of data governance (privacy, cybersecurity, ethics, etc.)

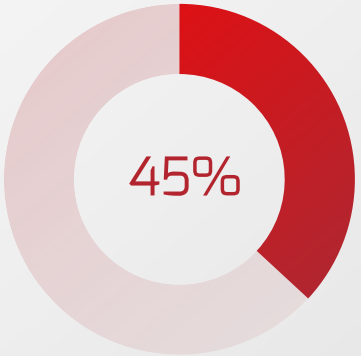
b) Lays out standards for data quality and data collection best-practices

c) Examines infrastructure of IT systems to support data access and sharing

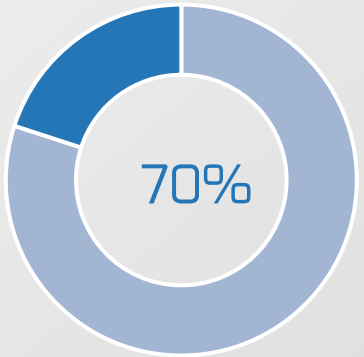
d) Builds data analytics in an effort to promote effective and ethical AI solutions



Of surveyed C-suite executives believe that 40% or less of their enterprise data is available for sharing



Of these same execs promote the need for a “comprehensive, enterprise-wide” approach to data strategy and data governance

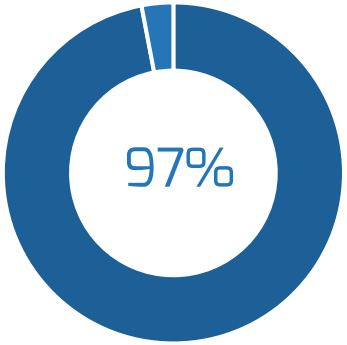


Consider data governance to be a significant work-in-progress, while **48%** say data management is properly scaled for AI adoption.

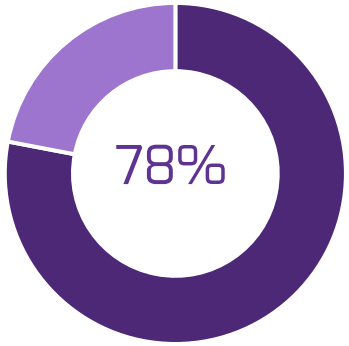
Source: Global Government Forum

Build a successful relationship between data privacy and AI

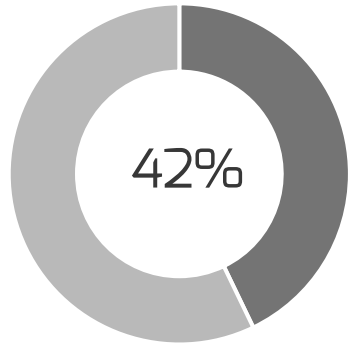
Common wisdom does not favor data privacy and AI coexisting, while a data privacy program strategy is integral in ethical and transparent AI.



Of organizations are looking to increase budget allocations to data privacy initiatives.



Of these same organizations believe that "the value of data encourages organizations to seek compliance" – this means increasing spend in areas of data privacy strategy.



Aim to develop a "clear, consistent set of data privacy standards across their organizations" in preparation for privacy law compliance.

Source: FTI Consulting

Info-Tech Insight

Privacy-first frameworks are not just for compliance; they span the spectrum of your operating environment and home in on areas where personal data exists within the organization – a foundational necessity for ethical AI implementation. A privacy framework gives you the insight and awareness to take AI and right-size it based on the current operating environment, regulatory implications, and intended future state.

Identify the business data inputs for a privacy-proof integration

"Garbage in, garbage out" dictates that high-quality data breeds effective AI integration

Data Governance

\+

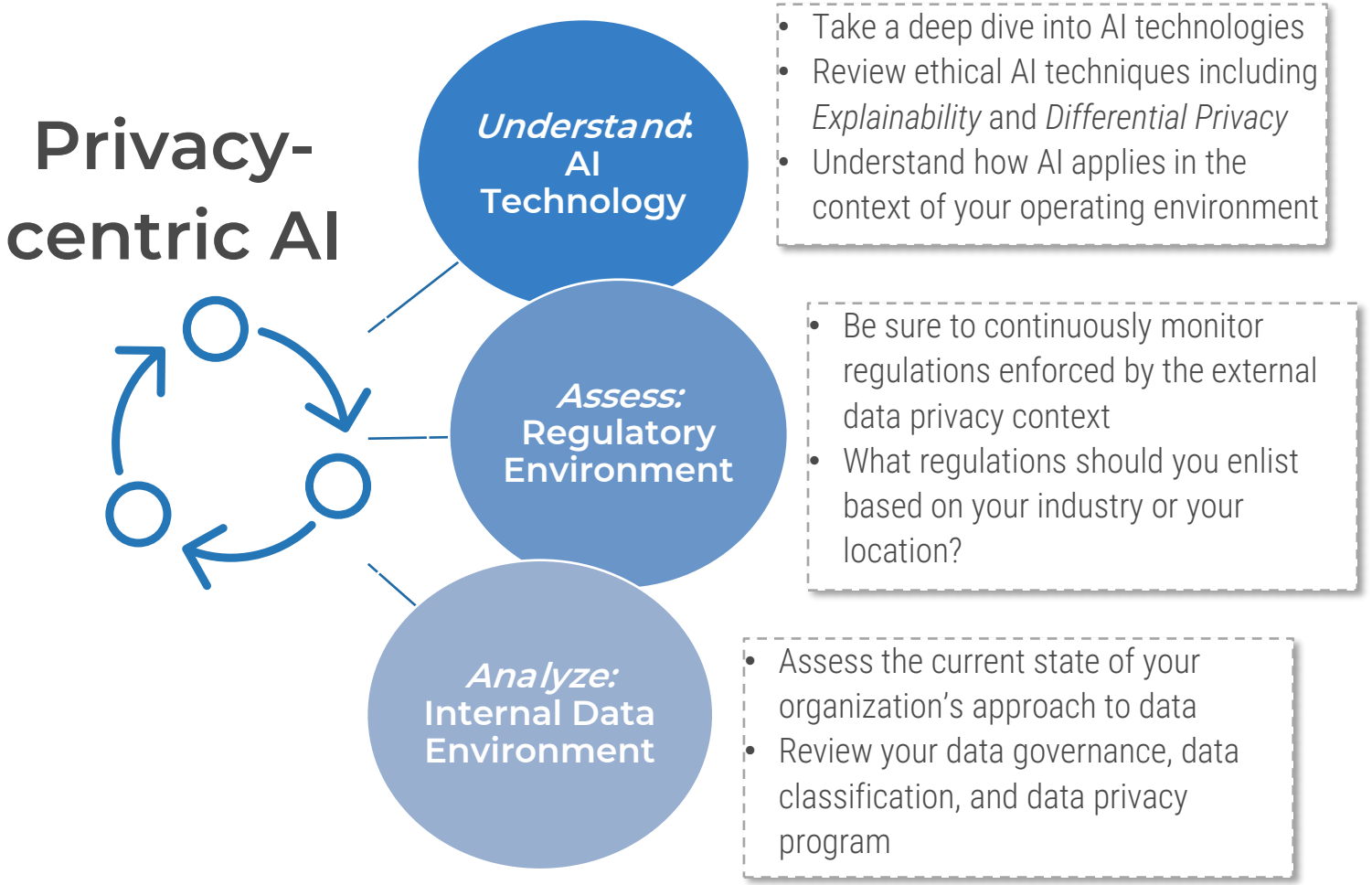
Data Privacy

=

Privacy-Proof AI

Info-Tech's approach

Take a privacy-first approach to AI evaluation and implementation.



- Take a deep dive into AI technologies
- Review ethical AI techniques including *Explainability* and *Differential Privacy*
- Understand how AI applies in the context of your operating environment

- Be sure to continuously monitor regulations enforced by the external data privacy context
- What regulations should you enlist based on your industry or your location?

- Assess the current state of your organization's approach to data
- Review your data governance, data classification, and data privacy program

IT The Info-Tech difference:

1. Understand AI from a data privacy lens
   - Get a grasp on how AI technology can elevate operations
   - Assess how the proliferation of data privacy regulations will impact your organization
   - Identify both your AI technology and data privacy program drivers

2. Identify the business posture
   - Delve into the applications of various types of AI across industries
   - Assess use-cases that apply to the context of your organization
   - Review your current data governance approach

Connect the pieces of your data privacy foundation

Review Info-Tech's research in the following domains to finalize your organization's data posture.

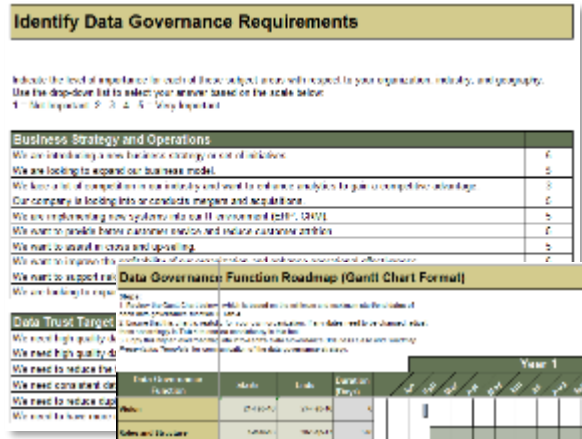
1. Data Governance

- Build a collaborative data governance plan
- Develop the data governance implementation roadmap
- Drive the data governance program

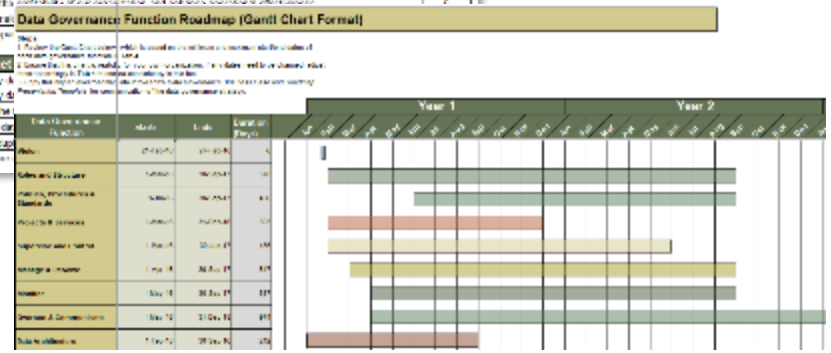
2. Data Privacy

- Collect privacy requirements
- Conduct a privacy gap analysis
- Build the privacy roadmap
- Implement and operationalize

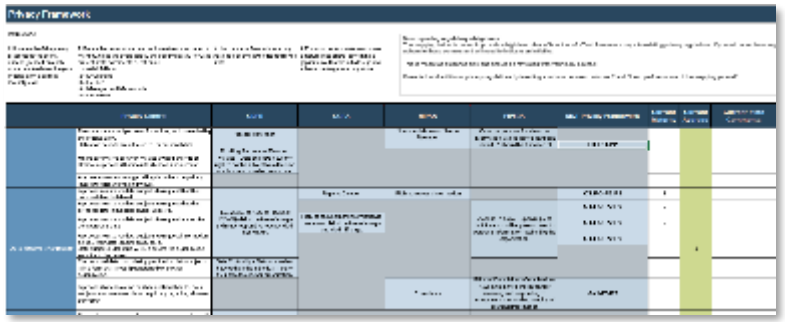
Data Governance Requirements Gathering tool



Data Governance Initiative Planning and Roadmap tool



Privacy Framework tool

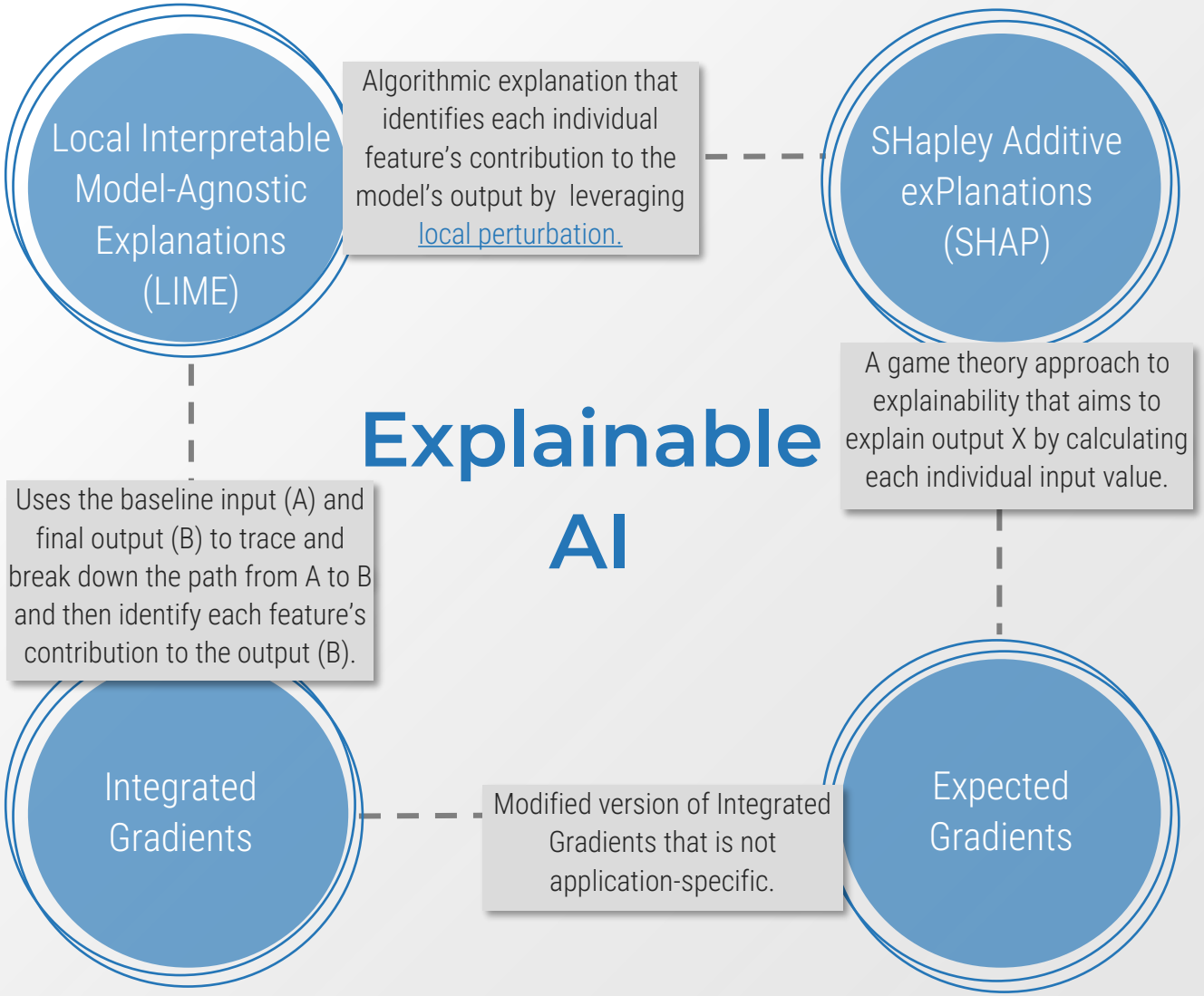


Explainability's role in privacy-proofing AI

Explainable AI aims to eliminate the opaque "black box" that has become an accepted feature of AI.

Accuracy vs. Predictability

In general, the more accurate a machine-learning model's output is, the more predictable it is. To improve level of accuracy, a larger data set is needed. While this is beneficial for larger neural networks facilitating complex decision-making tasks, it does not lend itself well to application in a heavily regulated environment and opens the organization in question up to transparency concerns.



Source: Dark AI And The Promise Of Explainability, Medium

Integrate XAI to comply

Federal and state-level data privacy and protection regulations, including the GDPR and CPRA, call for organizations to provide transparency around how automated decision-making solutions arrive at their outputs.

The CPRA added a new definition of "profiling," giving consumers opt-out rights with respect to businesses' use of "automated decision-making technology,"

vs.

"If AI is required to be explainable, then we are explicitly limiting the science to merely human-level performance. [...] This massively shortchanges the technology and shackles an otherwise powerful technology."

– Byron Reese

AI Platforms with Explainability

DarwinAI – "AI building AI" tech company that leverages proprietary Generative Synthesis platform to demystify deep learning neural networks.

Diveplane – Provides automated AI-powered business solutions across finance, healthcare, supply chain, real estate, and defense.

KYNDI – AI platform for government, financial services, and life sciences that aims to improve productivity of skilled workers.

simMachines – Focuses on AI solution delivery in the areas of fraud prevention, marketing, identity management, media, finance, and retail.

Digite – Provides AI solutions for project management across industries.

Stratyfy – Financial services solutions that mitigate bias through machine-learning techniques.

fiddler labs – Provides solutions that understand, analyze, validate, and monitor AI predictions, behavior, compliance, and performance.

Maaind – Neurotech company whose solutions promote cognitive improvements.

Tachyum – Universal processor for data center, AI, and HPC workloads.

Understanding differential privacy

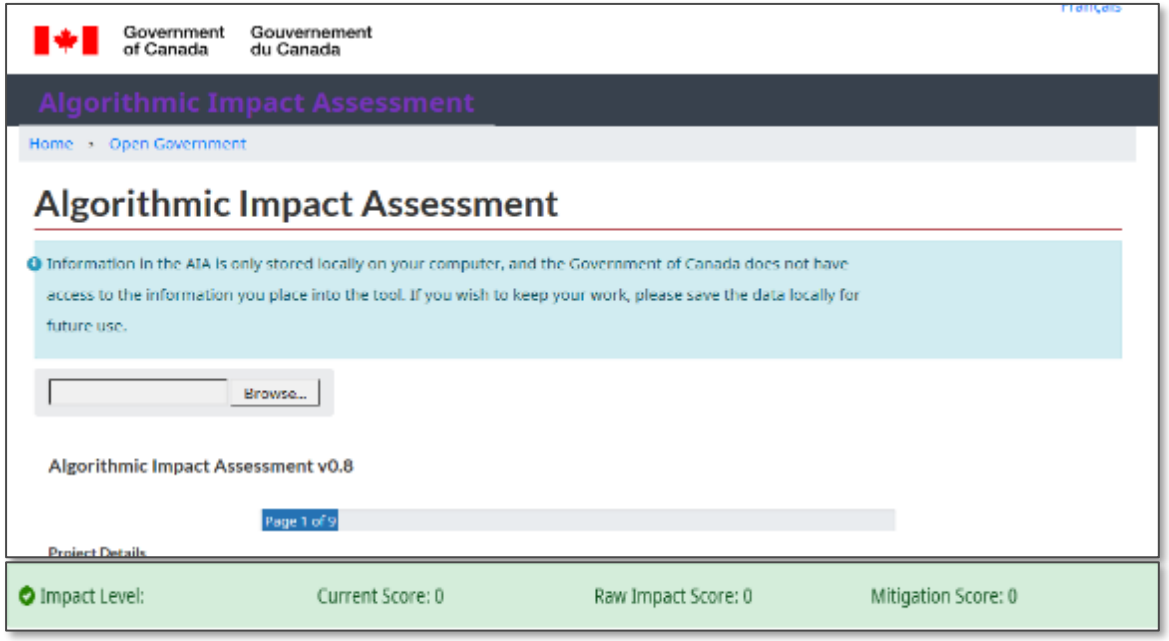
Differential privacy plays a crucial role in ensuring AI technology does not cross ethical boundaries when it comes to data processing.

> "Differential privacy makes it possible for tech companies to collect and share aggregate information about user habits, while maintaining the privacy of individual users."
>
> The Conversation

[1] Source: Differential Privacy: A Primer for a Non-Technical audience

Algorithmic Impact Assessment (AIA)

Perform an Algorithmic Impact Assessment (AIA) to validate the accountability of deployed AI technology's algorithmic decision.



Source: Government of Canada AIA

Info-Tech Insight

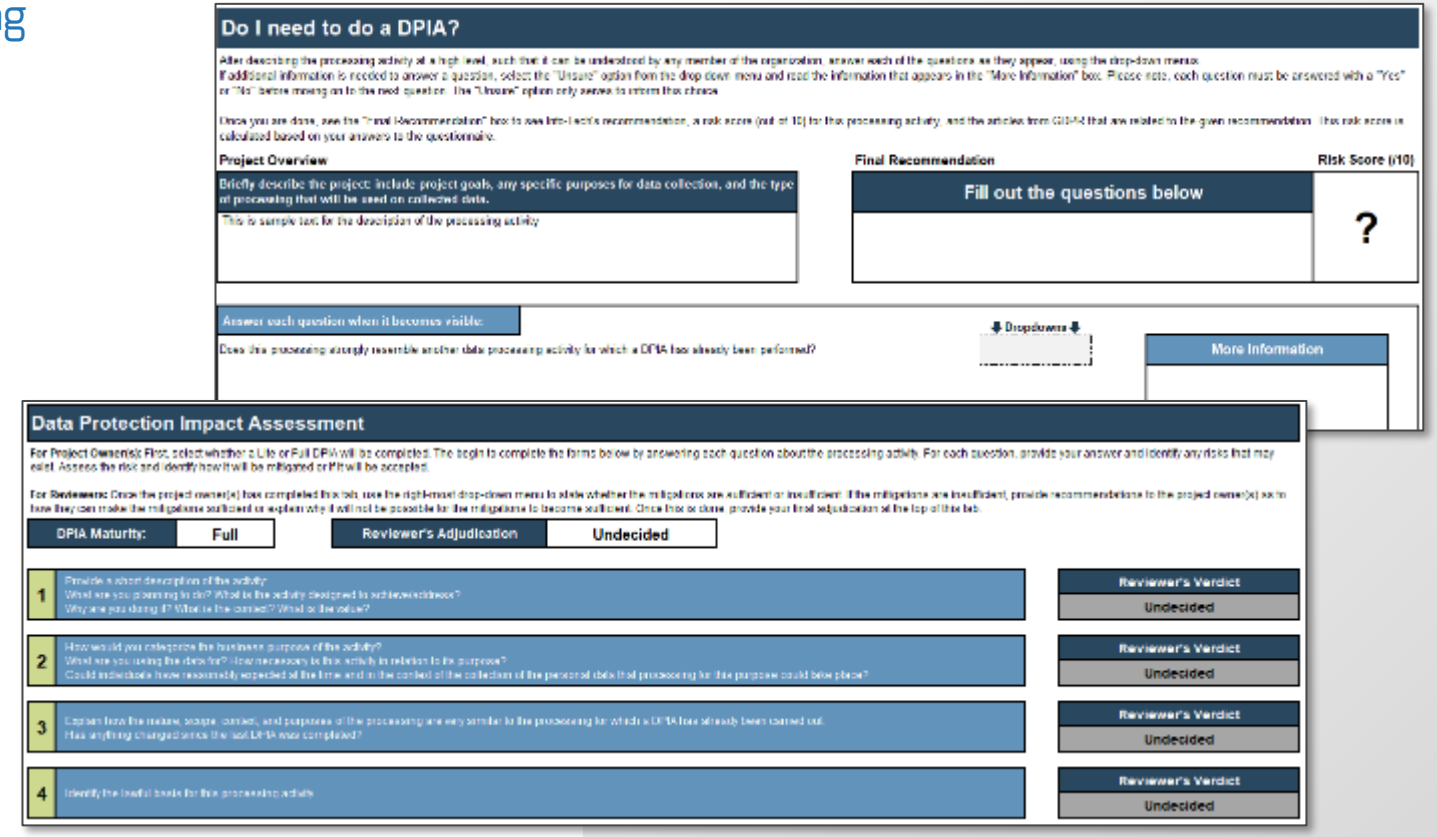
Define the objective. AIAs are powerful tools in establishing transparency in areas that were previously opaque. It helps to define what objective your organization aims to achieve in conducting an AIA, for which data subject group, and across which systems.

Data Protection / Privacy Impact Assessment (DPIA / PIA)

Understand the importance of the Data Protection Impact Assessment tool in validating high-risk data processing activities.

- A **Data Protection Impact Assessment (DPIA)** is used to assess how much private data will be affected by planned processing activities.
- The GDPR and CPRA require that a DPIA be performed.
- A DPIA ensures that data-processing activities are both compliant with data protection regulations and that data processors are cognizant of the risks surrounding the processing of personal data.
- Info-Tech's DPIA tool can be completed in a *lite* or *full* version based on the nature of the process.
- Involve the process owner (*Project Owner*) as well as a third-party stakeholder (*Project Reviewer*) throughout the assessment for oversight and validation of results.

A Threshold Assessment determines whether or not a DPIA is necessary.



A DPIA validates whether or not the processing activity is valid based on a set of qualifying questions and criteria.

Key Insights

Take a privacy-first approach.

Data privacy first, AI second. Your organization's internal and external environment impact not only the integration of AI-based technology, but also govern the approach to data privacy. By understanding your data privacy environment, you lay the foundation for a streamlined AI implementation.

Assess the changing landscape.

AI is rapidly evolving and continuously changing. So, too, is the external privacy environment as we shift toward an increasingly aware data privacy culture. Be aware of the changing AI and privacy landscape, which takes into account both the **external, industry implications,** and **data privacy regulations**, as well as the **internal drivers from a tech and privacy perspective.**

Look before you leap.

Know where you are before you dive head-first into the AI pond. **Establish your privacy posture, including data governance and a privacy program strategy,** as these will both heavily dictate the success and potential shortcomings of any future AI technology implementation projects. Look to fellow industry players to glean examples of effective, privacy-proof AI integration.

Be precise.

Narrow down the potential ways AI can improve existing operations in your environment in order to drive efficiencies.

Govern your data.

Know your data and governance environment before you act. Scope what potential data will be impacted and ensure that the appropriate mitigating controls are in place.

"When it comes to technology and policy, policy will always lag and form a gap. AI is a dramatic example of this. Ethics is the bridge that can be used to navigate this gap and ensure that trust of these technologies is possible."

– Kabir Barday, CEO OneTrust

Determine your data posture for AI

Govern your data

With a strong framework around where data exists within the business, who handles it, and for what processes and purposes, you move from a "present-day" perspective of data's role in AI to a "future outcome" outlook. The business and IT are well-positioned to know the parameters around the data sets involved or pulled on, including potential privacy implications.

Inject privacy and data protection

Privacy-proof AI breeds ethical AI implementation. Beyond staying on top of industry-specific and jurisdictional regulations, continue to apply Privacy by Design and/or Data Protection by Design principles when assessing AI technologies. Aim for transparency and explainability in the implementation outline.

Assess industry use-cases

With an understanding of the different AI technologies used within your industry, including their frameworks and outputs, you can build the use-case that best applies to the current operating context and future strategic objective of your organization. Identify opportunities for innovation as well as straightforward process improvements that drive efficiencies.

Thank You!

Questions?

Contact:

- aaronshum@gmail.com
- https://www.infotech.com/profiles/aaron-shum
- https://www.linkedin.com/in/aaronshum/

Aaron Shum
Vice President, Research
Security & Privacy


INFO~TECH
RESEARCH GROUP