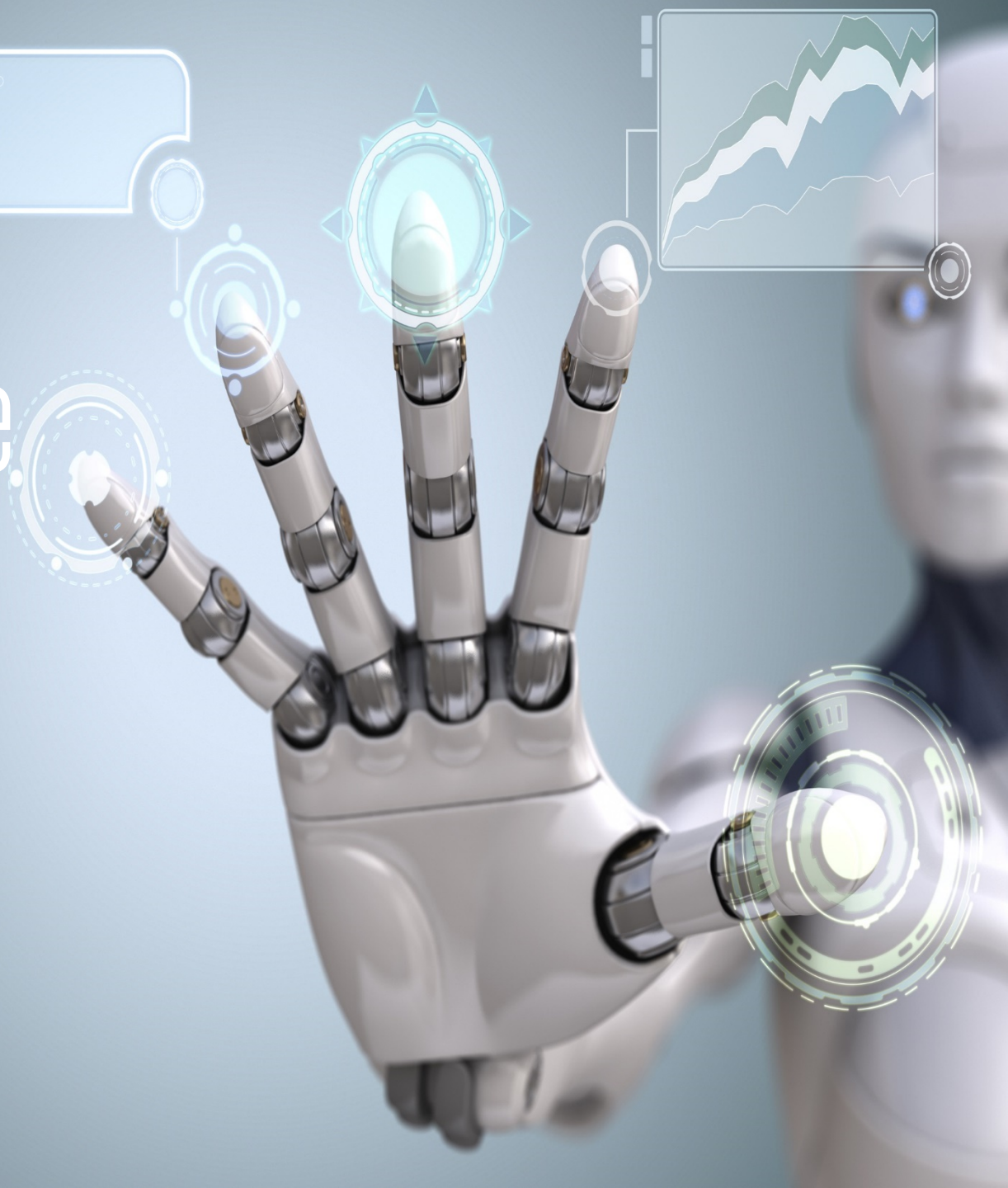
KPMG

Éthique de la Mégadonnée et de l'intelligence Artificielle

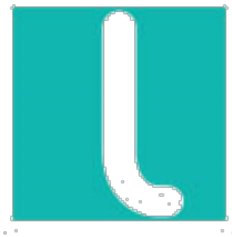
Dominic Jaar

Associé, KPMG Canada




KPMG


CanLII




lexum

Charte Québécoise

Toute personne a droit à la sauvegarde de sa **dignité**, de son **honneur** et de sa **réputation**.

Art. 4 *Charte des droits et libertés de la personne* (CDLP)

Toute personne a droit au **respect de sa vie privée**.

Art. 5 CDLP

Code Civil du Québec

Le mineur peut, compte tenu de son âge et de son discernement, contracter seul pour satisfaire ses besoins ordinaires et usuels.

Art. 157 Code Civil du Québec (CcQ)

Hors les cas où il peut agir seul, le mineur est représenté par son tuteur pour l'exercice de ses droits civils.

Art. 158 al. 1 (CcQ)

LADOPPRP

Les renseignements personnels sont confidentiels

sauf dans les cas suivants:

1° la **personne concernée** par ces renseignements **consent** à leur divulgation;

si cette personne est mineure, le consentement peut également être donné par le **titulaire de l'autorité parentale**…

Art. 53, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LADOPPRP)

Sécurité

25. La personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les **mesures de sécurité propres à en assurer la confidentialité**, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder.

Loi concernant le cadre juridique des technologies de l'information, RLRQ c C-1.1

Impartition

26. Quiconque confie un document technologique à un prestataire de services pour qu'il en assure la garde est, au préalable, tenu d'**informer le prestataire quant à la protection** que requiert le document en ce qui a trait à la confidentialité de l'information et quant aux personnes qui sont habilitées à en prendre connaissance.

Le prestataire de services est tenu, durant la période où il a la garde du document, de voir à ce que les **moyens technologiques convenus** soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Il doit de même assurer le respect de toute autre obligation prévue par la loi relativement à la conservation du document.

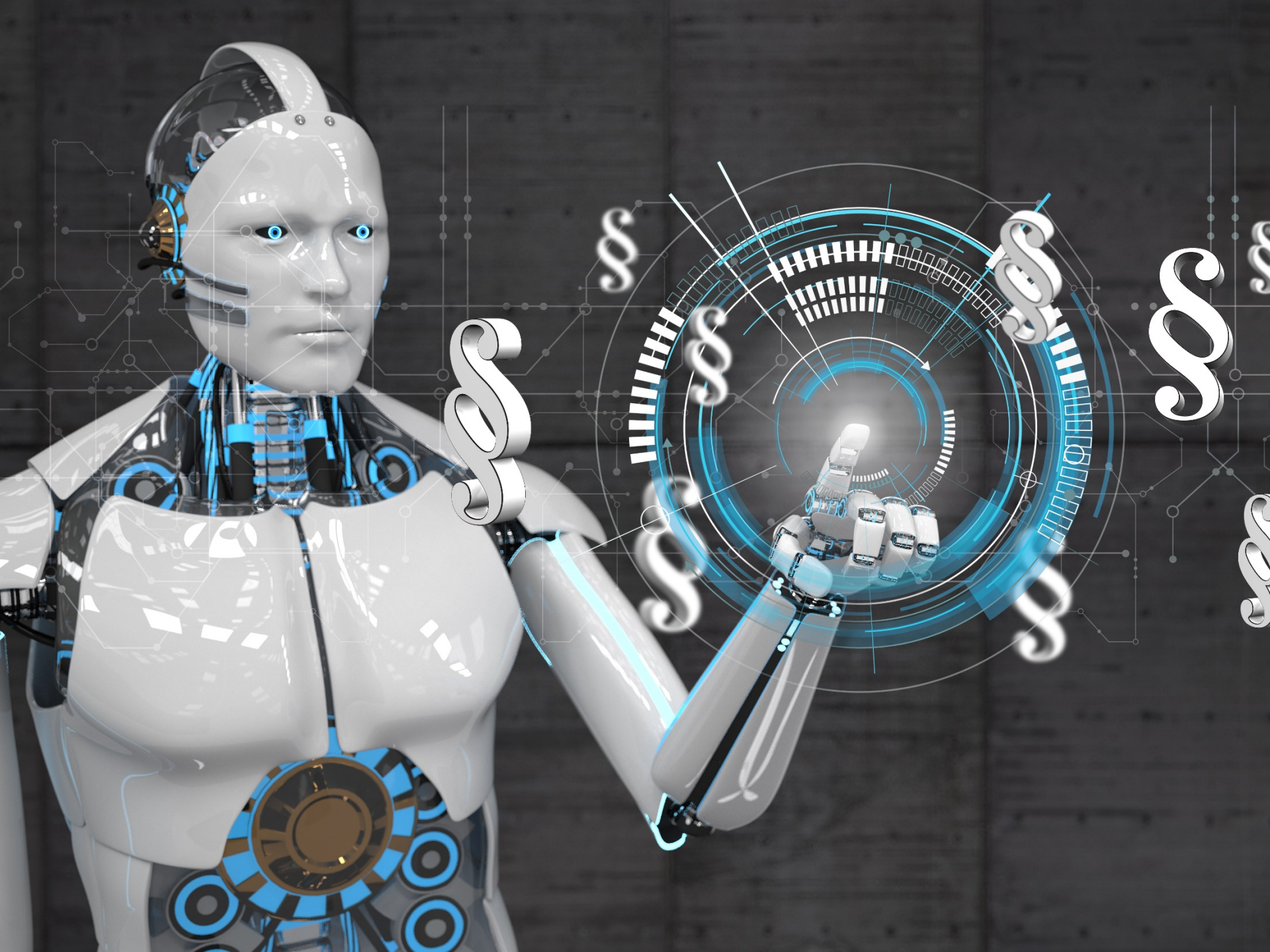
Loi concernant le cadre juridique des technologies de l'information, RLRQ c C-1.1

Communication

34. Lorsque la loi déclare confidentiels des renseignements que comporte un document, leur confidentialité doit être **protégée par un moyen approprié au mode de transmission**, y compris sur des réseaux de communication.

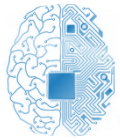
La documentation expliquant le **mode de transmission convenu**, incluant les moyens pris pour assurer la confidentialité du document transmis, doit être disponible pour production en preuve, le cas échéant.

Loi concernant le cadre juridique des technologies de l'information, RLRQ c C-1.1



Technologies et Techniques d'IA

Informatique neuromorphique



Systèmes Autonomes

Cyber Sécurité cognitive

Apprentissage Machine

Robot personnel

Apprentissage Profond

TECHNOLOGY READINESS

- Maintenant
- 1-2 ans
- 2-4 ans
- > 4 Ans

ARTIFICIAL INTELLIGENCE - Shaping a Future New Zealand (AI Forum New Zealand Report) V 1.2 March 2018

Chirurgie autonome

Réseaux neuronaux

Robotique infonuagique de nouvelle génération

Reconnaissance de motifs

Jeu contrôlé par la pensée

Traitement du language naturel

Traduction universelle en temps réel

Agents converationnels (Chabots)

Compagnons virtuels

Analyse d'émotion en temps réel

Décision individuelle automatisée, y compris le profilage

Article 22

La personne concernée a le **droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé**, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

RGPD - Réglement (UE) 2016/679, Parlement Européen

Standards Éthiques

- CIO Strategy Council on AI and Ethics- “Keeping Ethics in Artificial Intelligence”

https://open.canada.ca/en/blog/using-artificial-intelligence-government-means-balancing-innovation-ethical-and-responsible

https://www.itworldcanada.com/article/keeping-ethics-in-artificial-intelligence/408090

- IEEE on AI and Ethics- “The IEEE Global Initiatives on Ethics of Autonomous and Intelligent Systems”

https://standards.ieee.org/industry-connections/ec/autonomous-systems.html

- ISO on AI- “Framework for Artificial Intelligence Systems Using Machine Learning”

https://www.iso.org/standard/74438.html

- IAPP- “Building Ethics into Privacy Frameworks for Big Data and AI”

https://iapp.org/media/pdf/resource_center/BUILDING-ETHICS-INTO-PRIVACY-FRAMEWORKS-FOR-BIG-DATA-AND-AI-UN-Global-Pulse-IAPP.pdf

Déclaration de Montréal pour un développement responsable de l'intelligence artificielle

(3 Novembre 2017)

https://www.declarationmontreal-iaresponsable.com/la-declaration

Principes

- Bien-être
- Autonomie
- Justice
- Vie privée
- Connaissance
- Démocratie
- Responsabilité

DÉCLARATION SUR L'ÉTHIQUE ET LA PROTECTION DES DONNÉES DANS LE SECTEUR DE L'INTELLIGENCE ARTIFICIELLE

40e Conférence internationale des commissaires à la protection des données et de la vie privée

(23 Octobre 2018)

https://icdppc.org/wp-content/uploads/2018/10/20181023_ICDPPC-Declaration-AI_Adopted-FR.pdf

Loyauté

1. Les technologies d'intelligence artificielle et d'apprentissage automatique doivent être **conçues**, **développées** et **utilisées** dans le **respect des droits fondamentaux** de l'homme et conformément au principe de loyauté, en particulier en procédant ainsi :

a. En tenant compte des **attentes raisonnables** des individus, en s'assurant à cette fin que l'utilisation des systèmes d'intelligence artificielle reste fidèle aux objectifs d'origine et que l'**utilisation des données est compatible avec l'objectif premier de leur collecte** ;

b. En tenant compte non seulement de l'impact de l'utilisation de l'intelligence artificielle sur l'individu, mais aussi de son **impact collectif** sur les groupes et la société dans son ensemble ;

c. En s'assurant que les systèmes d'intelligence artificielle sont développés de façon à faciliter l'épanouissement de l'individu, sans l'entraver ni le mettre en danger, reconnaissant ainsi le besoin de **définir et** de **délimiter certaines utilisations**.

Attention, Vigilance et Responsabilité

2. Il est nécessaire de continuer à faire preuve d'**attention** et de **vigilance**, ainsi que de **transparence**, en ce qui concerne les effets et les conséquences des systèmes d'intelligence artificielle, en particulier en procédant ainsi :

a. En encourageant toutes les parties prenantes pertinentes à appliquer le principe de transparence au niveau des individus, des autorités de contrôle et d'autres tiers le cas échéant, y compris grâce à la réalisation d'**audits**, de suivi permanent et d'**évaluation de l'impact** des systèmes d'intelligence artificielle, ainsi que par un **examen périodique des mécanismes de surveillance** ;

b. En encourageant la **responsabilité collective et conjointe**, impliquant l'ensemble des acteurs et des parties prenantes, par exemple pour le développement de normes collaboratives et le partage des bonnes pratiques ;

c. En investissant dans une meilleure **sensibilisation**, l'**éducation**, la **recherche** et la **formation** afin de garantir un niveau satisfaisant d'information et de compréhension dans le domaine de l'intelligence artificielle et de ses effets potentiels sur la société ; et

d. En mettant en place, pour tous les acteurs concernés, des **processus de gouvernance** dont on peut apporter la preuve, par exemple en s'appuyant sur des **tiers dignes de confiance** ou en créant des **comités d'éthique indépendants**.

Transparence et Intelligibilité

3. Il convient d'améliorer la transparence et l'intelligibilité des systèmes d'intelligence artificielle, l'objectif étant de permettre une mise en œuvre efficace, en particulier en procédant ainsi :

a. En investissant dans la recherche scientifique publique et privée portant sur l'intelligence artificielle explicable ;

b. En promouvant la transparence, l'intelligibilité et l'accessibilité, par exemple en développant des modes de communication innovants, en tenant compte des différents niveaux de transparence et d'information requis en fonction de chaque audience concernée ;

c. En rendant les pratiques des organisations plus transparentes, en particulier en mettant l'accent sur la transparence des algorithmes et la vérifiabilité des systèmes, tout en garantissant le sérieux des informations fournies ; et

d. En **garantissant la liberté des individus de maîtriser les informations les concernant**, en particulier en s'assurant qu'ils sont toujours informés de façon appropriée lorsqu'ils interagissent directement avec un système d'intelligence artificielle ou qu'ils fournissent des données à caractère personnel qui seront traitées par de tels systèmes ;

e. En fournissant des informations adéquates sur les objectifs et les effets de l'intelligence artificielle, afin de vérifier que cette dernière s'aligne toujours sur les attentes des individus et que ces derniers peuvent exercer un contrôle global sur ces systèmes.

Éthique Intégrée

4. Dans le cadre d'une approche globale basée sur l'« **Ethics by design** » (éthique intégrée), les systèmes d'intelligence artificielle doivent être **conçus et développés de manière responsable**, en appliquant **les principes de protection de la vie privée par défaut et protection intégrée de la vie privée**, en particulier en procédant ainsi :

a. En mettant en œuvre des mesures et procédures technico-organisationnelles, en fonction du type de système développé, pour s'assurer du respect de la vie privée des personnes concernées et de leurs données à caractère personnel, aussi bien au moment de déterminer les méthodes de traitement des données que lors du traitement lui-même ;

b. En **évaluant** et en décrivant les **impacts attendus** sur les individus et la société, au début d'un projet reposant sur l'intelligence artificielle et au cours des développements pertinents durant tout son cycle de vie ; et

c. En identifiant les besoins spécifiques en vue d'une utilisation éthique et loyale des systèmes, et pour respecter les droits de l'homme, dans le cadre du développement et de l'exploitation de tout système d'intelligence artificielle.

Autonomisation

5. Il convient de donner davantage de pouvoirs à chaque personne et d'encourager l'exercice des droits individuels, tout en créant des opportunités de participation publique, en particulier en procédant ainsi :

a. En respectant les droits en matière de vie privée et de protection des données, y compris, le cas échéant, le **droit à l'information**, le droit **d'accès**, le droit **de s'opposer au traitement** des données et le droit **à l'effacement**, ainsi qu'en promouvant ces droits grâce aux campagnes d'éducation et de sensibilisation ;

b. En respectant les **droits connexes**, y compris la **liberté d'expression** et **d'information** ainsi que la **non-discrimination** ;

c. En reconnaissant que le **droit d'opposition** ou **de recours** s'applique aux technologies qui ont une influence sur les opinions ou le développement personnels et en garantissant, le cas échéant, le droit de chaque individu de ne pas faire l'objet d'une décision du simple fait d'un traitement automatique, si cette décision a un impact significatif sur le plan personnel et, si ce n'est pas le cas, en garantissant le droit de chaque individu de contester une telle décision;

d. En utilisant les capacités des systèmes d'intelligence artificielle à doter chaque individu de **pouvoirs égaux** et à **améliorer la participation publique**, via des interfaces adaptables et des outils accessibles, par exemple.

Préjugés ou Discrimination

6. Il convient de **réduire et** d'**atténuer** les préjugés ou les discriminations illicites pouvant résulter de l'utilisation de données présentes dans les systèmes d'intelligence artificielle, y compris en procédant ainsi :

a. En assurant le respect des instruments juridiques internationaux en matière de droits de l'Homme et de non-discrimination ;

b. En investissant dans la recherche portant sur les moyens techniques d'identifier, de traiter et de limiter les préjugés ;

c. En prenant des mesures raisonnables pour s'assurer que les données et les informations à caractère personnel utilisées dans les prises de décision automatiques sont exactes, actuelles et aussi exhaustives que possible ; et

d. En rédigeant des conseils et des principes spécifiques destinés au traitement des préjugés et de la discrimination, et en sensibilisant davantage les individus et les parties prenantes.

Zones Interdites de la Donnée

Le Commissariat Fédéral estime que ces pratiques ne sont pas conformes à la loi fédérale sur la protection des renseignements personnels dans le secteur privé (LPRPDE - *PIPEDA*).

- **Collecte**, **utilisation** ou **communication** qui autrement est **illégale**
- **Profilage** ou catégorisation donnant lieu à un traitement injuste, contraire à l'éthique ou discriminatoire en vertu de la législation sur les droits de la personne
- Collecte, utilisation ou communication à des fins qui causent ou sont susceptibles de causer un préjudice probable et grave à des individus
- Publication de renseignements personnels dans le but de réclamer un paiement aux individus pour retirer ces renseignements
- Obligation de communiquer le mot de passe des comptes de médias sociaux aux fins de la sélection des employés
- **Surveillance exercée par une organisation au moyen des fonctions audio ou vidéo de l'appareil de l'individu lui-même**

In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military-industrial complex. The potential for the disastrous rise of misplaced power exists and will persist.

We must never let the weight of this combination endanger our liberties or democratic processes. We should take nothing for granted. Only an alert and knowledgeable citizenry can compel the proper meshing of the huge industrial and military machinery of defense with our peaceful methods and goals, so that security and liberty may prosper together.

- President Dwight Eisenhower
Farewell Address to the nation
January 17, 1961


Privacy


OFF AIR
"I don't want to live in a society that does these sort of things"
HD
Edward
International Students For Liberty Conferenc...
OFF AIR

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
FOR AN ORDER REQUIRING THE
PRODUCTION OF TANGIBLE THINGS
FROM VERIZON BUSINESS NETWORK SERVICES,

Docket Number: BR

13-80

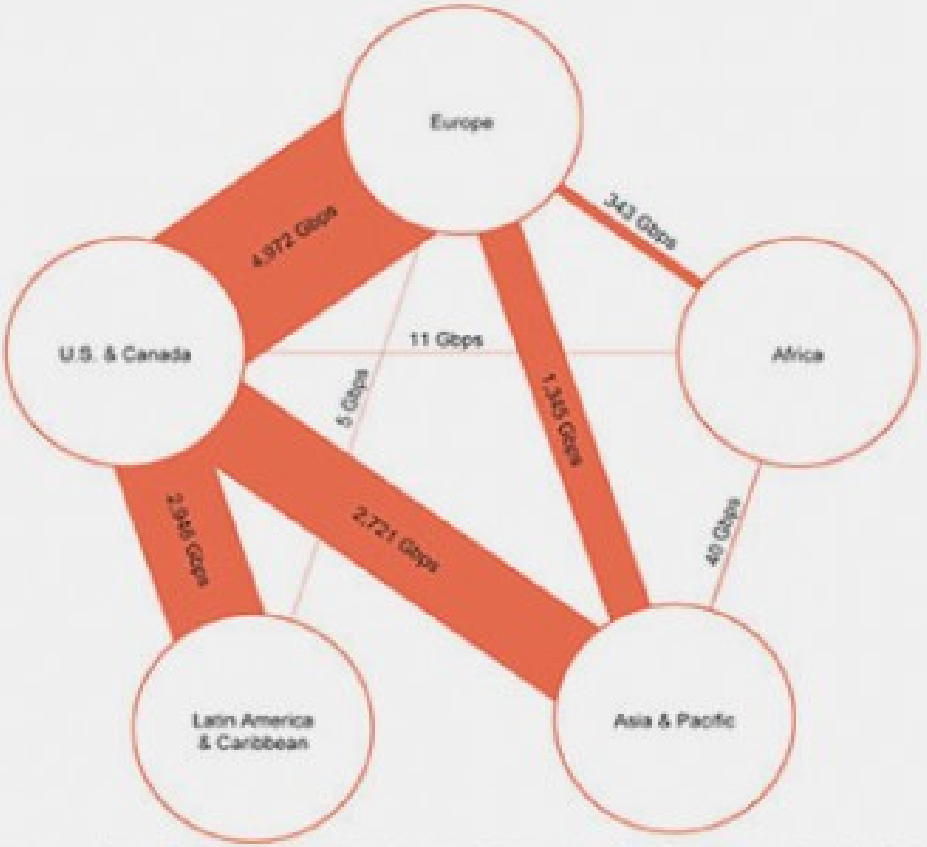
IT IS FURTHER ORDERED that **no person shall disclose to any other person** that the FBI or NSA has sought or obtained tangible things under this Order, other than to: (a) those persons to whom disclosure is necessary to comply with such Order; (b) an attorney to obtain legal advice or assistance with respect to the production of things in response to the Order; or (c) other persons as permitted by the Director of the FBI or the Director's designee. A person to whom disclosure is made pursuant to (a), (b), or (c) shall be subject to the nondisclosure requirements applicable to a person to whom an Order is directed in the same manner as such person. Anyone who discloses to a person described in (a), (b), or (c) that the FBI or NSA has sought or obtained tangible things pursuant to this Order shall notify such person of the nondisclosure requirements of this Order. At the request of the Director of the FBI or the designee of the Director, any person making or intending to make a disclosure under (a) or (c) above shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.


PRISM

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.

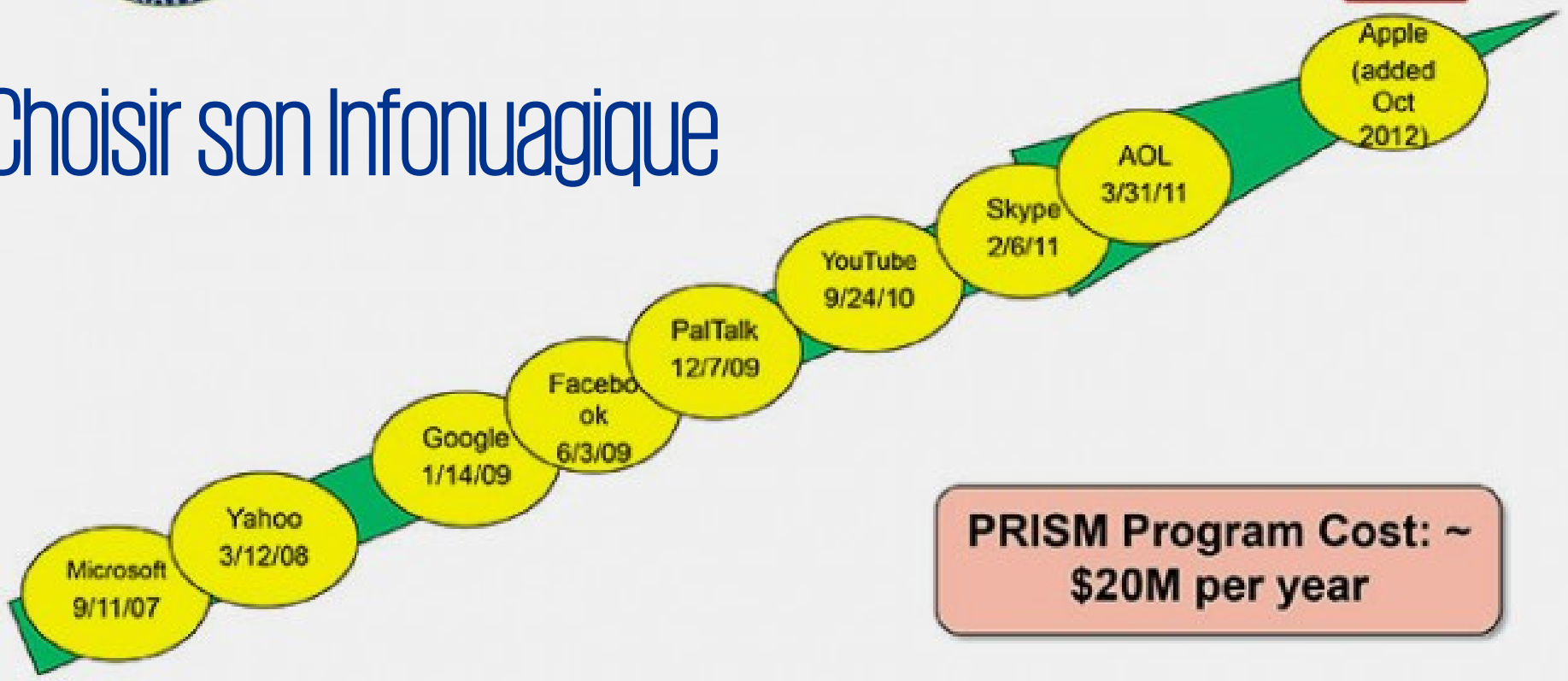


International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

Choisir son Infonuagique

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



(TS//SI//NF) PRISM Collection Details

Current Providers

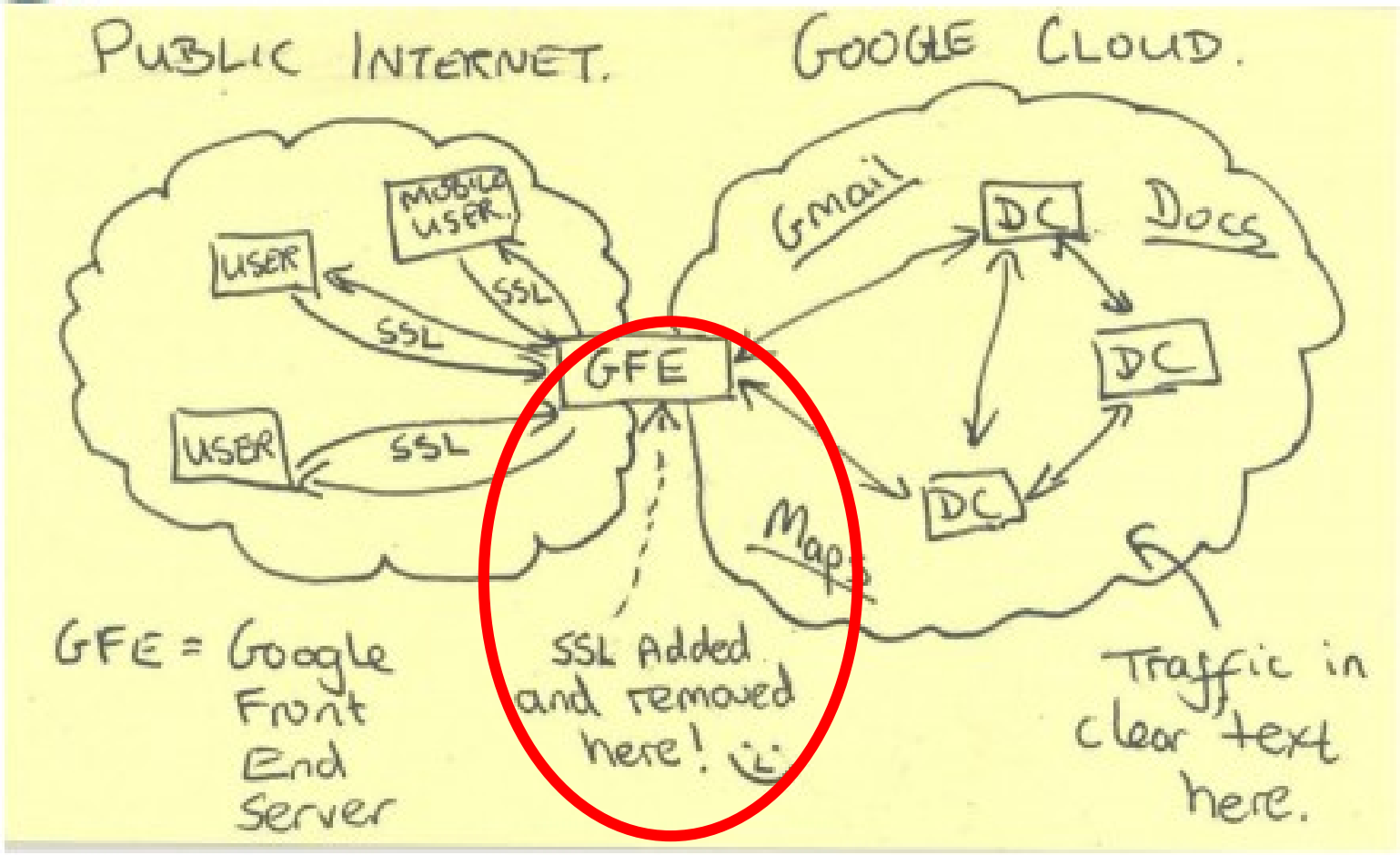
- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

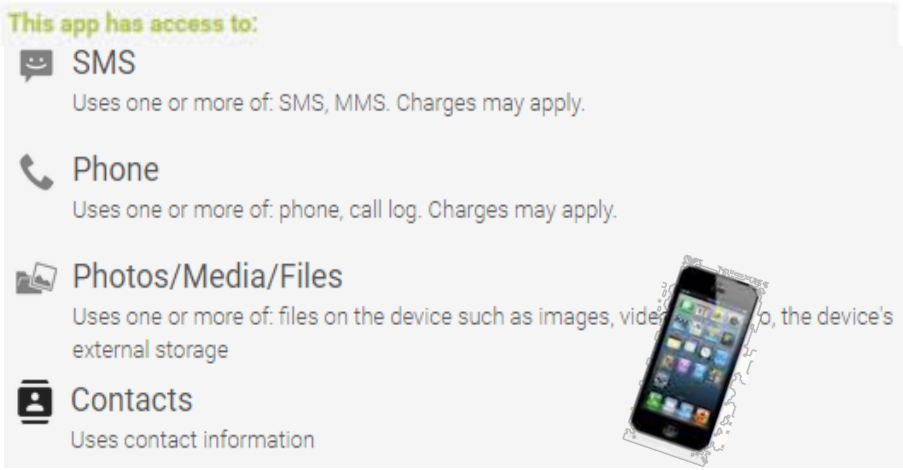
Current Efforts - Google



…You can tag individuals… Let's say you work at a major German corporation and I want access to that network, I can track your username on a website on a form somewhere, I can track your real name, I can track associations with your friends and I can build what's called a fingerprint, which is network activity unique to you, which means anywhere you go in the world, anywhere you try to sort of hide your online presence, your identity.”

Données personnelles vs professionnelles…

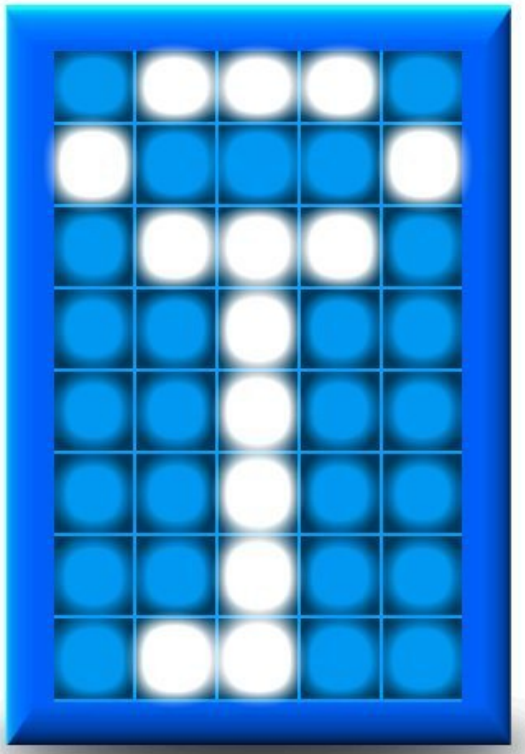
- Permissions des applications
- « Avoir accès à…. »



Êtes-vous dans les nuages?

- Traitement des données
  - Métadonnées
  - Dictée et reconnaissance vocale
  - Image et reconnaissance faciale
  - Vidéo et reconnaissance morphologique et motrice
  - Géolocalisation
  - Biométrie (empreinte digitale, vocale, ADN…)
- Usage des données
- Conservation des données
- Localisations des serveurs applicatifs
- Stockage en nuage par défaut…

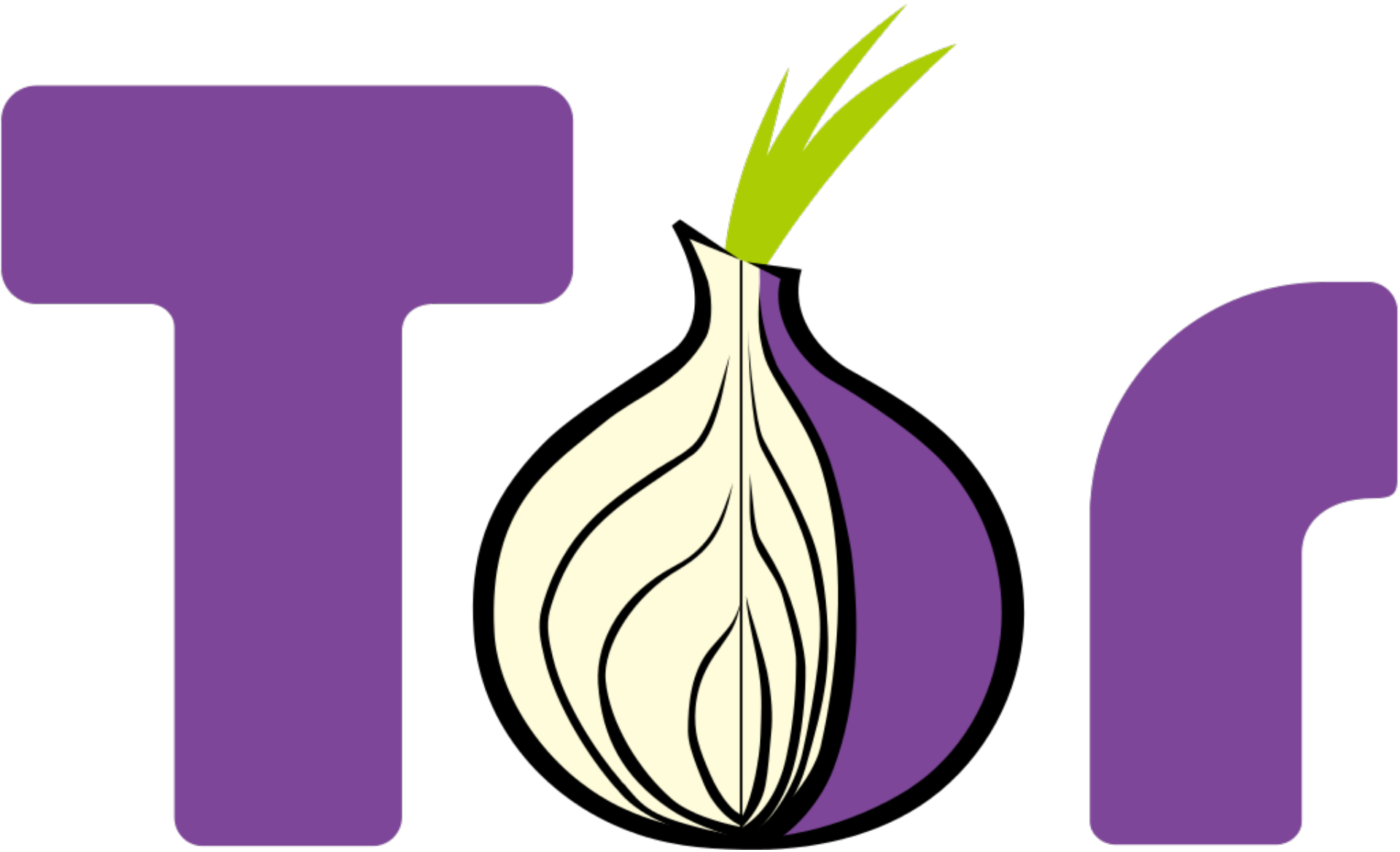

IMPossible



OpenPGP Alliance

Off-the-Record Messaging

HTTPS Everywhere



Stinks (U)

[redacted]

CT SIGDEV

[redacted]

JUN 2012


ACLU
AMERICAN CIVIL LIBERTIES UNION


ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD


epic.org
ELECTRONIC PRIVACY
INFORMATION CENTER

KPMG

Annexes

AI/ML Risk Management Framework

AI/ML Risk Management Framework Elements and Components

Risk Strategy & Appetite	Algorithmic Risk	Risk Governance	Risk Assessment & Measurement	Risk Management & Monitoring	Risk Reporting & Insights	Privacy & Security	Data & Technology	Risk Culture
Linkage to Corporate Strategy	Transparency & Accountability of Algorithms	Board Oversight & Committee	Risk Definition & Taxonomy	Risk Mitigation, Response & Action Plans	Risk Reporting	Ethical Treatment of Personal Data	Data Quality & Governance	Knowledge & Understanding
Risk Strategy	Algorithmic Oversight and Responsibility	Company Risk Operating Structure	Risk Identification	Testing, Validation & Management's Assurance	Business/ Operational Requirements	Respect for Privacy	Risk Analytics	Belief & Commitment
Risk Appetite & Tolerance	Model Validation	Risk Guidance	Assessment & Prioritization	Monitoring	Board & Senior Management Requirements	Data Protection & Personal Control	Technology Enablement	Competencies & Context
	Program & AI/ML Monitoring	Roles & Responsibilities	Quantitative Methods & Modeling	Risk in Projects/ Initiatives	External Requirements	Security Risks		Action & Determination
	AI/ML Applications Authentication	Decision Support	Risk Aggregation, Correlation & Concentration			Ethical Design & Data Symmetry Documentation		
	Change Management		Scenario Analysis & Stress Testing					
			Capital & Performance Management					

AI Framework Element Descriptions

FRAMEWORK ELEMENT	DESCRIPTION
Risk Strategy & Appetite	Alignment/Conscious decision to use risk management to enable the achievement of business plans, goals and strategic objectives. It includes a risk appetite statement supported by risk tolerances, limits and associated protocols to control risk levels throughout the organization.
Risk Assessment & Measurement	The activities in place that allow an organization to identify, assess and quantify known and emerging risks. The risk assessment and measurement processes allow organizations to consider the extent to which potential events may have an impact on achievement of objectives. It encompasses qualitative and quantitative approaches, processes, tools and systems that organizations develop and implement to identify, assess, and measure risks.
Risk Management & Monitoring	Management's response to manage, mitigate, or accept risk. Risk management efforts create value through the use of risk and control information to improve business performance across the enterprise. Management designs activities to assure stakeholders that risk management activities and controls are effective in managing risks that could have an impact on achievement of objectives (i.e. Integrated Assurance). For example, due diligence or proof of compliance through rigorous documentation, risk assessments, testing & monitoring.

AI Framework Element Descriptions

FRAMEWORK ELEMENT	DESCRIPTION
Algorithmic Risk	Common risks of AI/ML algorithms relate to governance; programs and AI monitoring; authentication of AI applications and change management. Common challenges associated with AI algorithms are difficulty to interpret, level of model maturity and monitoring of dynamic models.
Risk Governance	A structure through which an organization directs, manages and reports its risk management activities. It encompasses clearly defined roles and responsibilities, decision rights, the risk governance operating model, and reporting lines. For AI / ML, it is a data governance and accountability structure informed by transparent practices.
Risk Reporting & Insights	Reporting of risk and related information (e.g. mitigation activities) provide insight into the strengths and weaknesses of risk management activity. Disclosure of risk management information to key stakeholders also supports the decision making processes. Effective risk reporting enhances the transparency of risks that could have an impact on achievement of objectives in a timely manner.

AI Framework Element Descriptions

FRAMEWORK ELEMENT	DESCRIPTION
Data & Technology	Management of risk data that can be translated into meaningful risk information for stakeholders. It includes the development and deployment of risk management tools, software, databases, technology architecture, and systems that support risk management activities.
Privacy & Security	Management of privacy and security through design principles such as ethical design and data symmetry. Important privacy principles include data protection and personal control as well as the ethical treatment of personal data.
Risk Culture	Values and behaviors present throughout an organization that shape risk decisions. Risk culture influences the decisions of management and employees, even if they are not consciously weighing risks and benefits. A strong risk culture helps to encourage strategic decisions that are in the long-term best interest of the organization, its shareholders and employees.

DOMINIC JAAR

514.212.9348
djaar@kpmg.ca
@dominicjaar