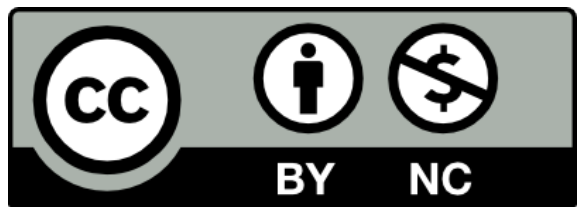
Business 4720 - Class 23

Legal Issues in Business Analytics

Joerg Evermann

Faculty of Business Administration
Memorial University of Newfoundland
jevermann@mun.ca



MEMORIAL UNIVERSITY

This Class

What You Will Learn:

- Torts
- Contracts
- Copyright
- Web-sites
- Privacy legislation (PIPEDA)
- Artifical intelligence and data act (AIDA, Bill C-27)
- European Union AI Act

MEMORIAL UNIVERSITY

Torts

Review of Concepts

- Civil wrong, other than breach of contract
- Vicarious liability for employees
- Compensatory and punitive damages, injunctions

MEMORIAL UNIVERSITY

Intentional Torts

”Invasion of Privacy”

- Trespass (e.g. to collect image or other sensor data)
- Breach of confidence (e.g. unauthorized use of confidential information)
- Intrusion on seclusion (e.g. employees inappropriately using data access)
- Public disclosure of private facts

Defenses

- Consent
- Assumption of risk
- Contributory negligence

MEMORIAL UNIVERSITY

Negligence

Examples

- Data loss or breach
- Physical or economic loss due to advice based on analytics models

Duty of Care

- Reasonably foreseeable
- Affordable precautions
- Proximity of loss (incl. careless statements)
- Product liability (incl. data/information products)

Defenses

- Asumption of risk
- Contributory negligence

Contracts

General Concepts

- Contract creation and acceptance of offers
- UECA and provincial electronic commerce acts
  - Specifies communication (sending, receiving) of offers and acceptance
- Consideration, privity, and assignment
- Terms, misrepresentation (negligence, fraud)
- Compensation or rescission (how?), and obstacles
- Exclusion, limitation, and waiver clauses

MEMORIAL UNIVERSITY

Contracts

Examples In Business Analytics

- Purchase or sale of data
- Collection or creation of data
- Licensing of data
- Data processing and manipulation (e.g. data cleaning, anonymization, etc)
- Provide or access/use analytics services

Specify

- What is being purchased (e.g. copyright (assignment), licence, or analytics service)?
- What is the required quality and how is it measured?

MEMORIAL UNIVERSITY

Licences

Permission to Use or Do Something

- Exclusive, sole, or non-exclusive (ordinary)
- Revocable or irrevocable
- Transferrable or non-transferrable
- Sublicenseable or not sublicenseable
- Limited or unlimited (in time or geography)
- Permitted uses (granted rights)
- Requirements for use
- Warranties, explicit or implied
- Indemnification

MEMORIAL UNIVERSITY

Copyrights

What is copyrightable?

- Non-trivial, original work
- Requiring *skill and judgment*
- Data as compilation of facts?
- Copyrightable by transformation, curation, collection

What are the copyrights?

- Reproduction (copying), making available, adaptation, translation, etc.
- Is data ingestion into a prediction model reproduction, adaptation, or translation? (”temporary reproduction”)

MEMORIAL UNIVERSITY

Websites

Using Web Data

- Terms of use
- Automatic access (”bots”, ”crawlers”)

Robots files

- Specify user agent (”User-agent”)
  - ”Googlebot”, ”Bingbot”, ”Googlebot-Image”, . . .
- Specify prohibited files or folders (all others allowed)
- Specify allowed files or folders (all others prohibited)
- Specify crawl frequency (”Crawl-delay”)
- Specify no search indexing (”Noindex”)

MEMORIAL UNIVERSITY

Example Robots File

```
# robots.txt file for YouTube
# Created in the distant future (the year 2000) after
# the robotic uprising of the mid 90's which wiped
# out all humans.

User-agent: Mediapartners-Google*
Disallow:

User-agent: *
Disallow: /api/
Disallow: /comment
Disallow: /feeds/videos.xml

Disallow: /watch_popup
Disallow: /watch_queue_ajax
Disallow: /youtubei/
```

Source: `youtube.com/robots.txt`

MEMORIAL UNIVERSITY

Hands-On Exercise

Identify the robots.txt file of your university web site.

- Are there portions of the site a crawler bot is not permitted? Why might this be?
- Are there different directives for different crawlers?
- Are there limits on crawl frequency?

MEMORIAL UNIVERSITY

Privacy Legislation

- Personal Information Protection and Electronic Documents Act (PIPEDA) (federal)
- Applies to commercial activity in all Canadian provinces
- Except for activity solely within provinces that have ”substantially similar” legislation (BC, ON)
- Does not apply to federal government, covered by Privacy Act and Access to Information Acts
- Does not apply to provincial government (e.g. Newfoundland Access to Information and Protection of Privacy Act (ATIPPA))
- Office of the Privacy Commissioner of Canada (OPC)
  - Investigate complaints
  - Report with recommendation but no enforcement powers
  - Federal Court

MEMORIAL UNIVERSITY

Personal Information

- Name, age, weight, height
- Medical information, e.g. medical records
- Financial information, e.g. income, purchases, ...
- Race and ethnicity, marital status and religion
- Biometrics, such as DNA and fingerprints
- Address and communication info (email, phone #, ...)
- Eduction, such as transcripts and grades
- Employment information and employment records
- Opinions and comments

PIPEDA

Fair Information Principles

1. Be accountable
2. Identify the purpose
3. Obtain valid, informed consent
4. Limit collection
5. Limit use, disclosure and retention
6. Be accurate
7. Use appropriate safeguards
8. Be open
9. Give individuals access
10. Challenging compliance

MEMORIAL UNIVERSITY

PIPEDA

- Mandatory breach reporting
- Complaint process through the OPC
- Authority to audit

Sources and Further Information

- Privacy Guide for Businesses (OPC)
- PIPEDA fair information principles (OPC)

MEMORIAL UNIVERSITY

PIPEDA – 1. Accountability

Requirements

- Comply with all 10 principles
- Appoint person responsible for compliance (privacy officer)
- Define reporting mechanisms to/from this person or office
- Protect all personal information, incl. that transferred to 3rd parties and agents
- Develop and implement policies and procedures for compliance

Source: PIPEDA Fair Information Principle 1 – Accountability (OPC)

MEMORIAL UNIVERSITY

Hands-On Exercise

Identify the privacy policy of your bank or communications provider or other large organization you regularly deal with.

- Who is the responsible person?
- Who do they report to?
- How can you contact them?

MEMORIAL UNIVERSITY

PIPEDA – 1. Accountability (Building Blocks)

- **Information inventory**, incl. sensitivity evaluation
- **Policies** for
  - Collection, use and disclosure (incl. consent & notification)
  - Access to and correction of information
  - Retention and disposal
  - Administrative, physical and technological security controls and access privileges
  - Challenging compliance
- **Risk and threat assessment** for all operations (esp. involving 3rd parties outside Canada)
- **Privacy training and education** for all employees
- **Breach and incident management** protocols
- **Manage external service providers** with access to data (e.g. contractual provisions, training and education, audits)
- **External communication** procedures (notification, access/contact means, etc.)

Source: Getting accountability right with a privacy management program (OPC)

MEMORIAL UNIVERSITY

PIPEDA – 1. Accountability (Ongoing Assessment and Revision)

- Oversight plan for monitoring privacy management effectiveness and compliance
- Periodically review and revise plan
- Monitor ongoing processes:
  - Are controls effective?
  - Do controls reflect latest OPC or industry guideslines?
  - Are new services being offered that involve increased collection, use, or disclosure?
  - Is training being delivered and effective?
  - Are policies known and followed?
- Document compliance for audits and investigations

Source: Getting accountability right with a privacy management program (OPC)

MEMORIAL UNIVERSITY

PIPEDA – Cross-Border Personal Data Processing

- The transferring organization remains accountable
- Contractually ensure generally equivalent protection
- Take all reasonable steps to protect data
  - Contractual terms
  - External party staff training
  - External party security measures
  - Audits and inspection
- Be aware of legal requirements of the jurisdiction in which the third party processor operates, e.g.
  - Financial information disclosure requirements
  - National security access to information

Source: Guidelines for processing personal data across borders (OPC)

MEMORIAL UNIVERSITY

PIPEDA – 2. Identifying Purpose

- Ensure information is required for purpose
- Explain purpose when collecting information
- Maintain records for purpose and received consents
- Ensure purpose is reasonably and appropriately limited

Source: PIPDA Fair Information Principle 2 – Identifying purposes (OPC)

MEMORIAL UNIVERSITY

PIPEDA – 3. Consent

- Consent must be meaningful and valid
- Consent can be required only if necessary to fulfill a legitimate purpose
- Form of consent must take into account the sensitivity of information
- Individuals may withdraw consent at any time

Source: PIPDA Fair Information Principle 3 – Consent (OPC)

MEMORIAL UNIVERSITY

PIPEDA – 3. Consent (Guidelines)

- Make privacy information clearly available: *what* information is collected, *who* is it shared with, *for what* purpose, and what are the *potential risks or harms*?
- Provide a clear choice
- Ensure the consent process is user friendly
- Allow individuals to withdraw consent
- Re-obtain consent when making significant changes to privacy practices
- Retain records to demonstrate compliance

Source: Optaining meaningful consent infographic (OPC)

Source: Guidelines for obtaining meaningful consent (OPC)

MEMORIAL UNIVERSITY

PIPEDA – 3. Consent (Interpretation)

- Consent is necessary, but not sufficient
- Purpose of collection must be ”reasonable”
  - Information collection must serve real business interest
  - Loss of privacy must be proportional to benefits gained

”No-Go Zones”

- Collection, use or disclosure that would be illegal
- Profiling or categorization that leads to unfair, unethical, or discriminatory treatment
- Collection, use or disclosure that is likely to cause significant harm
- Publishing information with intent to charge for removal
- Requiring social media passwords for employee screening
- Surveillance through an individual’s own device

Source: Guidance on inappropriate data practices: Interpretation and application of subsection 5(3) (OPC)

MEMORIAL UNIVERSITY

PIPEDA – 3. Consent (Example Decisions)

- Number of gym visits: Collection may be benign but disclosure to work team members may not be, requiring explicit consent
- Viewing of health-related websites is sensitive information.
- Email address may be sensitive if it indicates social connection.
- Palm-vein scanning is not sensitive if the scan is not retained and immediately transformed.
- Disclosure of sensitive financial information requires explicit consent, while disclosure of customer contact for financial marketing may only require opt-out consent.
- Purchasing habits are sensitive, require explicit consent
- Voice prints for computer authentication are not sensitive
- Non-users of social networking sites would not reasonably expect the use of their email addresses for creating links, requiring explicit consent.

Source: Interpretation Bulletin: Form of Consent (OPC)

MEMORIAL UNIVERSITY

PIPEDA – 3. Consent (Implied Consent)

- In initiating a complaint procedure, medical information may be be disclosed to the defendant in order to defend themselves through implied consent.
- GPS location data may be collected by implied consent for the purposes of improving productivity, or protecting and managing company assets, but not for employee evaluation.

Source: Interpretation Bulletin: Form of Consent (OPC)

MEMORIAL UNIVERSITY

PIPEDA – 3. Consent (Conditions for Opt-out Consent)

- Information is non-sensitive in nature and in context.
- Information sharing is limited and well-defined
- Organization's purposes are limited and well-defined and clearly stated at time of collection
- Opportunity for opt-out offered at the earliest opportunity
- Convenient procedure for opting out
- Opt-out takes effect immediately
- Opt-out must be communicated to related businesses, subsidiaries, etc.

Source: Interpretation Bulletin: Form of Consent (OPC)

MEMORIAL UNIVERSITY

Hands-On Exercise

Consider your bank or communications provider or other large organization you regularly deal with.

- What information have they collected and for what purpose?
- How have you provided meaningful consent? Did you have a clear choice?
- What is process for withdrawing or revoking consent?

MEMORIAL UNIVERSITY

PIPEDA – 4. Limiting Collection

- Information must fulfill a legitimate, identified purpose
- Collection must be fair and lawful
- Information collected should be identified in information management policies
- Collecting less information reduces risk or impact of loss or breach

Source: PIPEDA Fair Information Principle 4 – Limiting Collection (OPC)

MEMORIAL UNIVERSITY

PIPEDA – Video Data Collection

- Use less privacy-intensive alternatives, if possible (e.g. infrared cameras, LIDAR scanners, etc.)
- Establish business reason
- Develop policy on use of data
- Limit use and viewing range as far as possible; do not record audio unless necessary
- Inform public that surveillance is taking place
- Store data securely and destroy when no longer required
- Allow individuals to access their video data (but not that of others)
- Train and educate human camera operators and data processors (if any) on privacy obligations
- Periodically evaluate the need for video surveillance

Source: Guideliens for Overt Video Surveillance in the Private Sector (OPC)

MEMORIAL UNIVERSITY

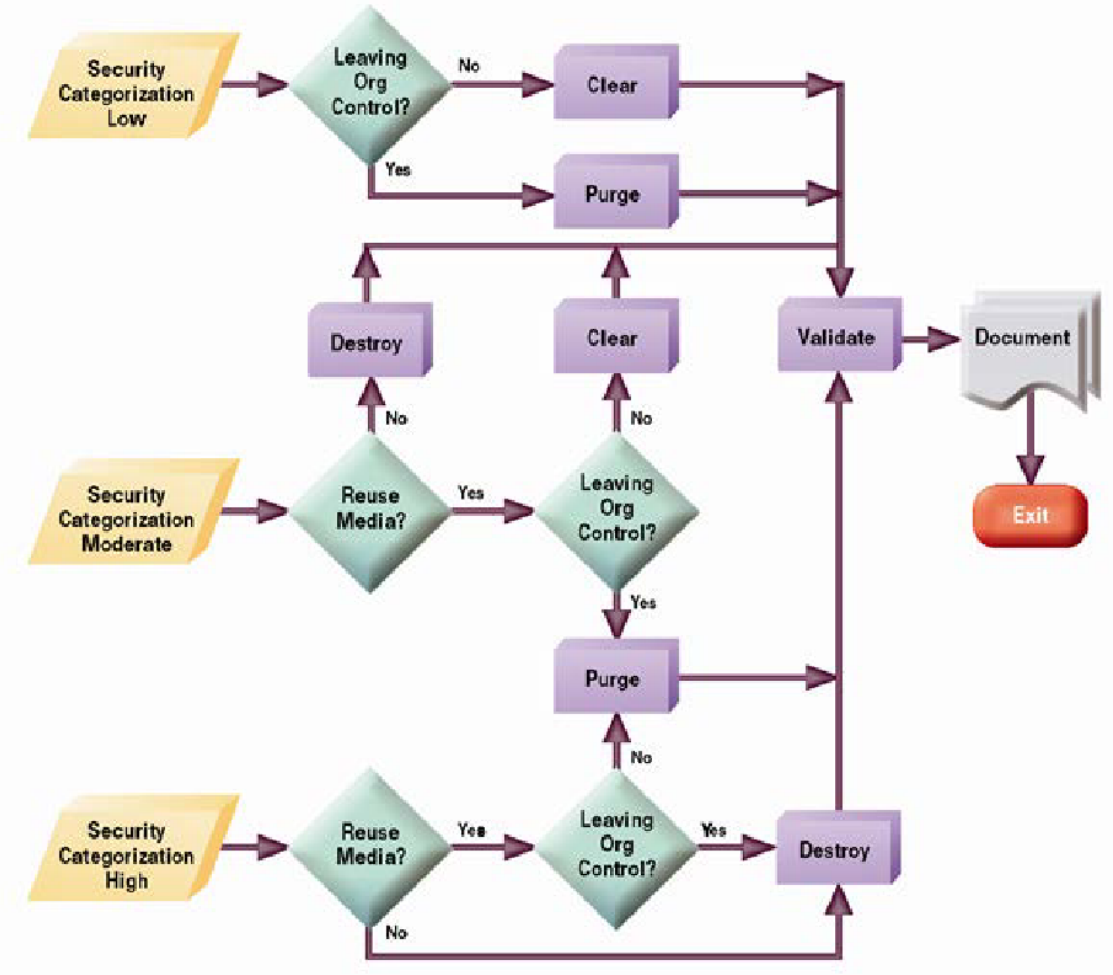
PIPEDA – 5. Limiting Use, Disclosure, and Retention

- Define appropriate retention period
- Limit employee access
- Monitor information access
- Define deletion/disposal processes for different media
  - Maintain security and access controls during disposal
  - Include back-ups and copies
  - Include copies at outsourcers and service providers
  - Verify and document deletion/disposal
  - Verify contractual compliance by third party disposal providers (if any)

Source: PIPEDA Fair Information Principle 5 – Limiting use, Disclosure, and Retention (OPC)

MEMORIAL UNIVERSITY

Guidelines for Media Sanitization



Source: NIST SP 800-88R1 — Guidelines for Media Sanitization, National Institute of Standards and Technology, US

MEMORIAL UNIVERSITY

PIPEDA – 6. Accuracy

- Ensure accuracy, completeness, and currency of information
- Record collection dates for all information
- Record and document measures for ensuring accuracy

Source: PIPEDA Fair Information Principle 6 – Accuracy (OPC)

MEMORIAL UNIVERSITY

PIPEDA – 6. Accuracy (Interpretation)

- Information must be as accurate as necessary for purpose
- Industry standards are not an appropriate reference for adequate accuracy
- Responsibility for accuracy rests with the organization, not the individual
- Information must be updated also to third parties

Source: Interpretation Bulletin: Accuracy (OPC)

MEMORIAL UNIVERSITY

PIPEDA – 7. Safeguards

- Develop and implement security policies
- Use physical, technological, and organizational measues to provide protection
- Anonymize unnecessary personal information
- Review safeguards
- Employee training and education

Source: PIPEDA Fair Information Principle 7 – Safeguards (OPC)

MEMORIAL UNIVERSITY

PIPEDA – 7. Safeguards (Interpretation)

- Safeguards must be commensurate with sensitivity
- Policies must be effectively applied
- Secure disposal policies must be implemented
- Medical and payroll information are highly sensitive
- Employee training and education is required
- Organizations must ensure that third parties have safeguards in place
- Data on portable devices must be encrypted
- Data in online storage must be encrypted
- Organizations must ensure technological safeguards remain current

Source: Interpretation Bulletin: Safeguards (OPC)

MEMORIAL UNIVERSITY

PIPEDA – 7. Safeguards ("Employee Snooping")

- Privacy culture
- Training and reminders
- Policies for granting and revoking access
- Ensure access is restricted to roles, geography, time, etc.
- Monitor access and detect anomalies and inappropriate access

Source: Ten tips for addressing employee snooping (OPC)

MEMORIAL UNIVERSITY

PIPEDA – 8. Openness

- Inform customers and employees about policies and procedures
- Ensure that policies are easily available and easy to understandable
- Specify (at minimum):
  - Accountable person
  - How to access and amend/update/delete personal information
  - How to complain about practices
  - Collected information and disclosure to others

Source: PIPEDA Fair Information Principle 8 – Openness (OPC)

MEMORIAL UNIVERSITY

Hands-On Exercise

Consider your bank or communications provider or other large organization you regularly deal with.

- What policies or procedures do they communicate?
- Where can you find them? Are they easy to find? Are they easy to understand?

MEMORIAL UNIVERSITY

PIPEDA – 9. Individual Access

- Advise individuals about their information held, how it was collected and used, and disclosures to third parties.
- Requests have to be in writing
- Verify requestor identify before disclosing to requestor
- Document requests for information and their processing, incl. the documents provided to the requestor
- Provide access at minimal or no cost, using easy process
- 30 day to provide requested information; 30 day extension in exceptional circumstances (e.g. legal consult, format shifting, etc.)
- Ensure retention is updated
- Inform individuals of their right to complain to OPC
- Ensure staff training

Source: PIPEDA Fair Information Principle 9 – Individual Access (OPC)

MEMORIAL UNIVERSITY

PIPEDA – 9. Access (Exemptions)

- Disclosure would reveal information about others
- Solicitor-client privilege
- Confidential commercial information
- Threaten security of others

Source: Responding to access to information requests under PIPEDA (OPC)

MEMORIAL UNIVERSITY

Hands-On Exercise

Consider your bank or communications provider or other large organization you regularly deal with.

- What is the process to access the information held about you? Who do you contact?
- Is access free or does it have an associated cost?
- What is the process to update your information? Who do you contact?

MEMORIAL UNIVERSITY

PIPEDA – 10. Challenging Compliance

- Simple complaint handling procedures
- Inform complainants about organization's procedures, and those of industry bodies, regulators, and OPC
- Record and acknowledge complaints
- Notify and record outcomes, decisions, and actions taken in response

Source: PIPEDA Fair Information Principle 10 – Challenging Compliance (OPC)

MEMORIAL UNIVERSITY

Hands-On Exercise

Consider your bank or communications provider or other large organization you regularly deal with.

- How do you initiate a complaint about lack of compliance?
- Who do you contact?

MEMORIAL UNIVERSITY

PIPEDA – Privacy Breach

- Report breaches of security safeguards that pose a real risk of significant harm to OPC
  - Examples: Financial loss, identity theft, credit record, loss of employement or business opportunities, damage to reputation or relationships, damage to or loss of property, bodily harm
  - Consider sensitivity of information
  - Consider probability of misuse
- Notify affected parties and third parties
- Maintain records of all breaches
- Responsibility to report for third party processor breaches

Source: What you need to know about mandatory reporting of breaches of security safeguards (OPC)

MEMORIAL UNIVERSITY

Other Data Protection and Privacy Laws

- European Union (GDPR)
- California (CCPA)
- US (COPPA, HIPAA)
- China (PIPL)
- Singapore (PDPA)
- South Africa (PoPIA)
- ...

MEMORIAL UNIVERSITY

Bill C-27

Digital Charter Implementation Act 2022

- Consumer Privacy Protection Act (update to PIPEDA)
- Personal Information and Data Protection Tribunal Act
- Artificial Intelligence and Data Act (AIDA)

Progress in House of Commons

- Minister for Innovation, Science and Economic Development
- First reading June 2022, second reading June 2023
- Standing Committee on Industry and Technology (in progress)

Sources and Further Information

- Parliament of Canada
- AIDA Companion Document (Government of Canada)

AIDA

- Prohibit reckless and malicious use of AI
- Ensure accountability of risks associated with AI systems
- Applicable to ”high-impact AI systems”
  - Severity of potential harm
  - Evidence of risks to health or safety, risk of adverse impact on human rights
  - Imbalances of economic and social circumstances, or age of impacted persons
  - Consider both intended and unintended consequences

> *”Artificial intelligence system means a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions.”*

Parliament of Canada

MEMORIAL UNIVERSITY

AIDA – High Impact Examples

Screening systems

- Systems that make decisions, recommendations, or predictions
- Impacting access to services (e.g. credit) or employment
- Potential of discriminatory outcomes and economic harm

Biometric systems

- Make predictions about people
- Identify person remotely
- Predict characteristics, psychology or behaviour
- Potential impact on mental health and autonomy

MEMORIAL UNIVERSITY

AIDA – High Impact Examples

Influence human behaviour at scale

- Content recommendation systems
- Influence behaviour, expression, and emotion
- Potential impact on psychological and physical health

Critical to health and safety

- AI applications integrated in health and safety functions
- Decisions or recommendations based on sensor data
- Example: Autonomous driving systems
- Example: Triage decisions in health care
- Potential to cause physical harm

MEMORIAL UNIVERSITY

AIDA – Harms

- Individual harms
- Collective harms
  - Historically marginalized communities
  - Human rights impacts
- Biased output
  - Differentiation directly or indirectly through variables that act as a proxy for prohibited grounds
  - Race, gender, but also income (proxy for race or gender)

> *"Biased output means content that is generated, or a decision, recommendation or prediction that is made, by an artificial intelligence system and that adversely differentiates, directly or indirectly and without justification, in relation to an individual on one or more of the prohibited grounds of discrimination set out in section 3 of the Canadian Human Rights Act . . . "*

Parliament of Canada

MEMORIAL UNIVERSITY

AIDA – Requirements

Human Oversight & Monitoring

- Exercise meaningful human oversight
- Includes interpretability appropriate to context
- Measurement and assessment of high-impact AI systems and their output

Transparency

- Publicly provide information on how high-impact AI is used
- Allow public to understand capabilities, limitations, and potential impacts

MEMORIAL UNIVERSITY

AIDA – Requirements

Fairness and Equity

- Demonstrate awareness of potential discriminatory outcomes
- Actions to mitigate discriminatory outcomes

Safety

- Proactively assess high-impact AI systems to identify potential harms
- Mitigate risk of harm

MEMORIAL UNIVERSITY

AIDA – Requirements

Accountability

- Implement governance mechanisms to ensure compliance with AIDA
- Documentation of policies, processes, and implemented measures

Validity & Robustness

- Perform consistently with intended objectives
- Stable and resilient in a variety of circumstances

MEMORIAL UNIVERSITY

AIDA – Examples Measures

System Design

- Perform initial risk assessment
- Assess and address potential biases in training data selection
- System design informed by required level of interpretability

System Development

- Document data and models
- Evaluate and validate, retrain as needed
- Build mechanisms for human oversight and monitoring
- Document appropriate use and limitations

MEMORIAL UNIVERSITY

AIDA – Examples Measures

Make System Available for Use

- Document how requirements for design and development are met
- Provide documentation to users regarding training data, limitations, and appropriate uses
- Continuous risk assessment

Managing Operations of a System

- Logging and monitoring of output
- Ensure adequate monitoring and human oversight
- Intervene as needed

MEMORIAL UNIVERSITY

AIDA

- Notification requirement in case of harm or potential material harm
- Specific requirements to be set through regulation by the Minister (expected within 2 years after royal assent)
- Minister would have power to audit, order cessation of use

Enforcement Mechanisms

- Administrative monetrary penalties
- Regulary offences
- Criminal offences

MEMORIAL UNIVERSITY

AIDA

New Criminal Offences:

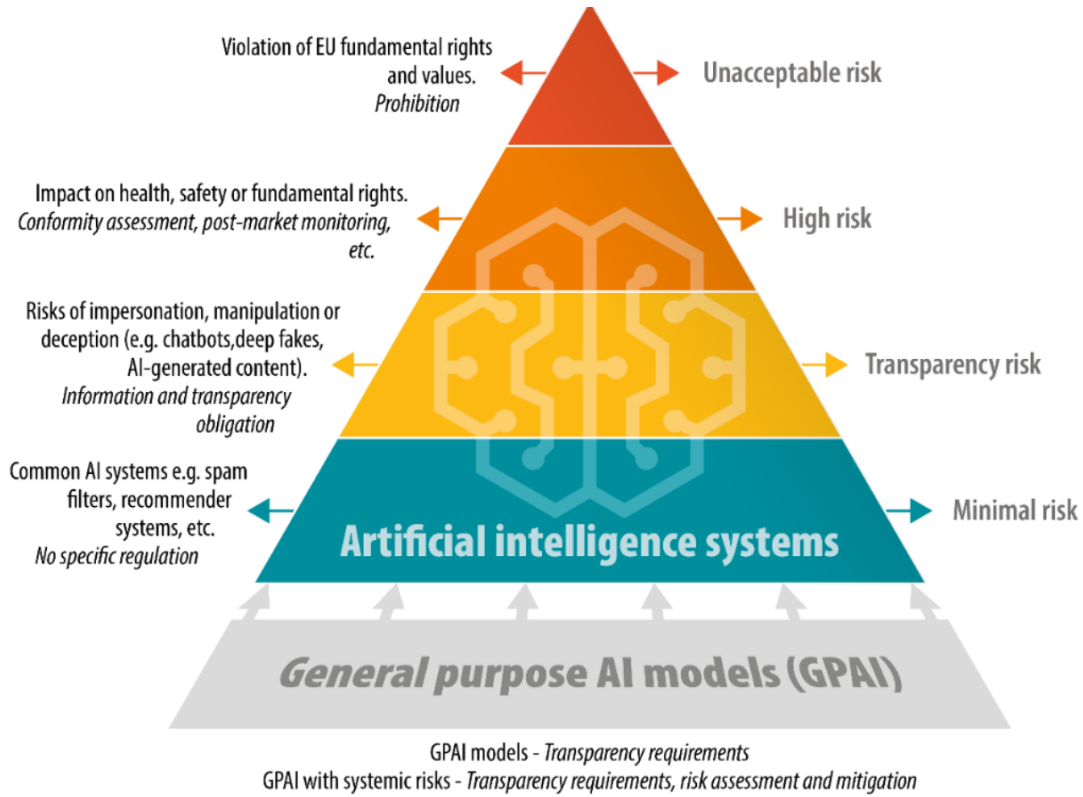
- Knowingly possessing or using unlawfully obtained personal information to design, develope, use or make available for use an AI system.
- Making an AI system available for use, knowing, or being reckless as to whether it is likely to cause serious harm . . . where its use actually causes such harm.
- Making an AI system available for use iwht the intent to defraud the public and to cause substantial economic loss to an individual, where its use actually causes that loss.

MEMORIAL UNIVERSITY

European Union AI Act

Source and Further Information

- EU AI Act (European Parliament)



Source: AI Act Briefing (EU Parliament)

MEMORIAL UNIVERSITY

European Union AI Act

Unacceptable Risk

- Prohibited
- Examples:
  - Cognitive behavioural manipulation
  - Classifying people based on behaviour, socio-economic status or personal characteristics (”social scoring”)
  - Untargeted scraping of internet for facial images
  - Emotion recognition in the workplace and educational institutions (except for medical or safety reasons)
  - Biometric categorisation to infer race, sexual orientation, political opinions, religous beliefs
  - Real-time remote biometric identification systems in public spaces, such as facial recognition

MEMORIAL UNIVERSITY

European Union AI Act

High Risk

- Asssessment before market introduction and throughout product lifecycle
- AI systems that are used in products are subject to EU product safety legislation (e.g. toys, aircraft, cars, medical devices, etc.)
- Profiling of natural persons
- Registration requirement for specific areas:
  - Operation of critical infrastructure
  - Education and vocational training
  - Employment, worker management and access to self-employment
  - Access to essential private and public services, & benefits
  - Law enforcement
  - Migration, asylum, and border control
  - Assistance in legal interpretation and application of the law

European Union AI Act

Transparency Risk

- Risk of impersonation, manipulation, or deception
- Chatbots, deep fakes, AI-generated content, . . .
- Information and transparency obligation
- E.g. watermarking output, disclosure of AI generated content

Minimal Risk

- Common AI systems
- No specific regulation

MEMORIAL UNIVERSITY