# What the Hack!? Who is Really Using Your Information

**Stephen Burns**
**Bennett Jones LLP**

**Association of Corporate Counsel**
**May 3, 2024**

# TODAY'S DISCUSSION

- ARTIFICIAL INTELLIGENCE – CHANGING THE GAME
- DATA DRIVEN RISKS:
  - CHANGING FACE OF PRIVACY
  - MANAGING CHANGE: TECHNOLOGY RISKS
  - INCREASING COMPLEXITY OF SECURITY
  - GOVERNANCE: PRACTICAL APPROACH REQUIRED

*Note: This presentation was prepared by Bennett Jones LLP to provide information on recent legal developments and topical issues in various areas of law as it relates to information technology, data and privacy issues. Due to the general nature of this presentation, it should not be relied upon as legal advice.*

# HISTORICALLY - BIG DATA

License to use Primary Data. Customer acknowledges that Seller and its Affiliates have an irrevocable, perpetual, royalty-free, non-exclusive transferable world-wide right to access, compile, analyze, distribute, disseminate and reproduce all Data collected or retrieved by Seller through a Device owned by a Customer and Subscribed for Services for research and development, marketing and/or commercial uses for the benefit of Seller PROVIDED THAT all Primary Data is stripped of information identifying:

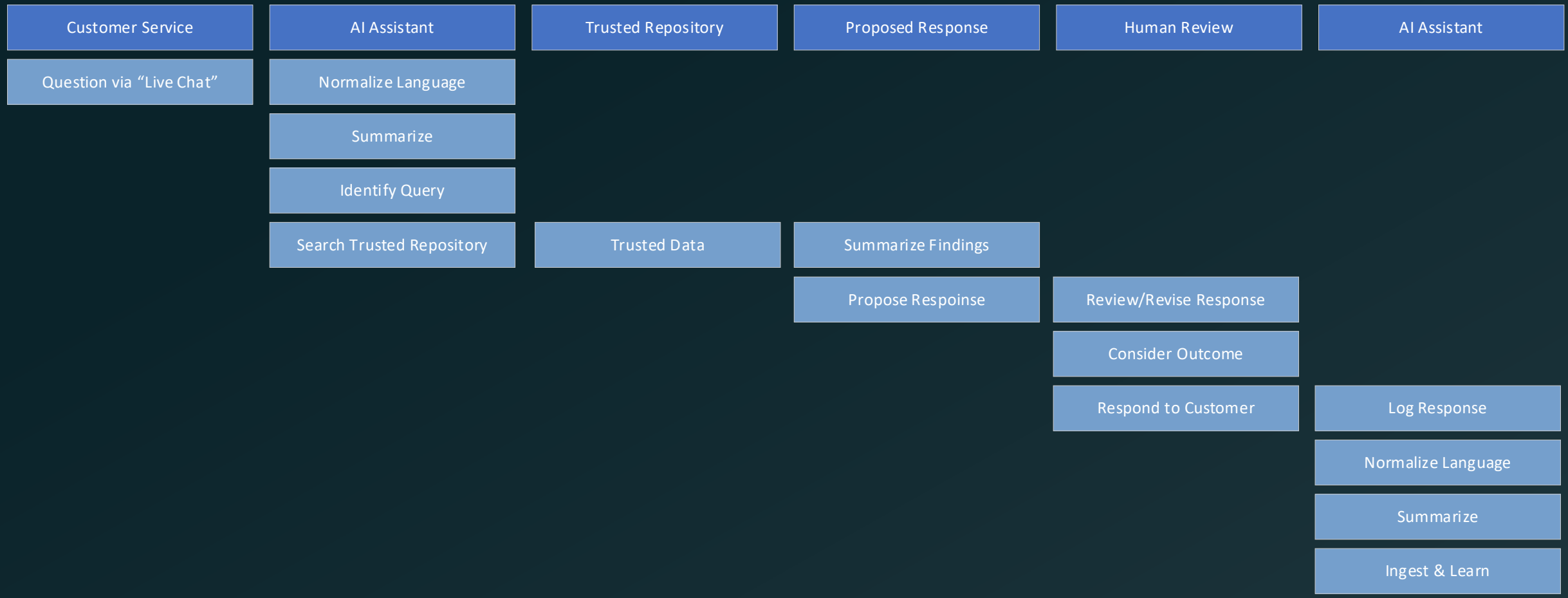
(a) Customer as the owner of such Data; and

(b) The location of the Device from which such Data was collected,

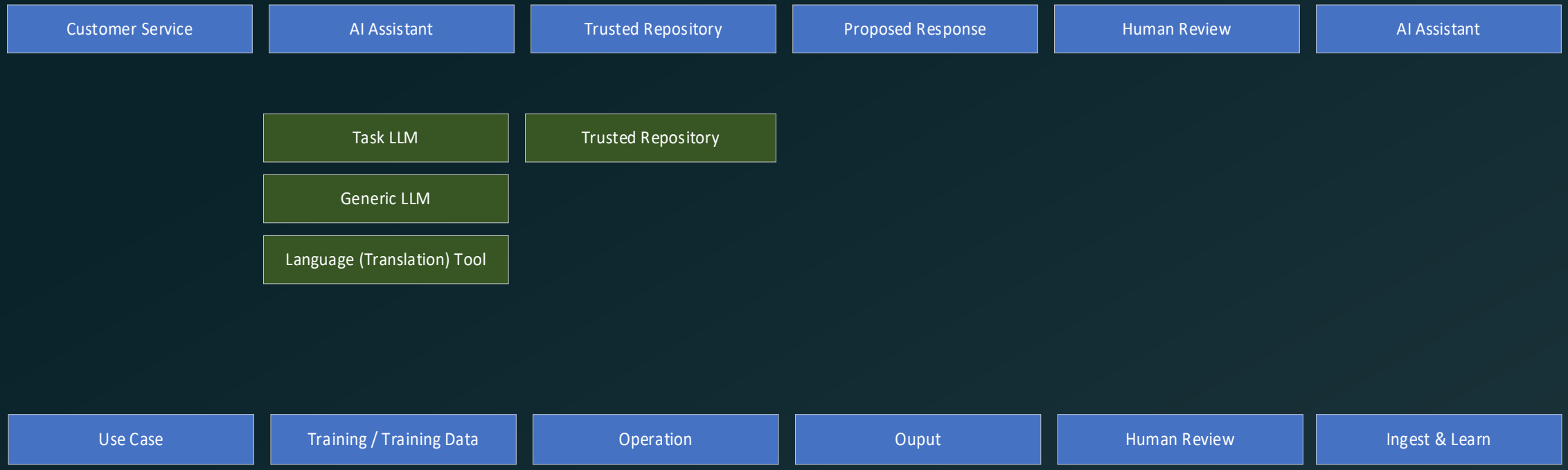
("Customer's Anonymous Data").

Customer agrees that Customer's Anonymous Data may be aggregated, compiled, integrated, modified, adapted and/or used by Seller for its own commercial benefit and use in conjunction with other data collected by Seller (including without limitation data from Third Parties) and Customer acknowledges and understands that Seller will have copyright, trademark and any other intellectual property rights resulting from any database, data files, tables, compilations, analyses, and results derived from Customer's Anonymous Data (whether on a standalone basis or when combined with other data) and any output, copies, reproductions, improvements, modifications, adaptations and translations resulting therefrom.

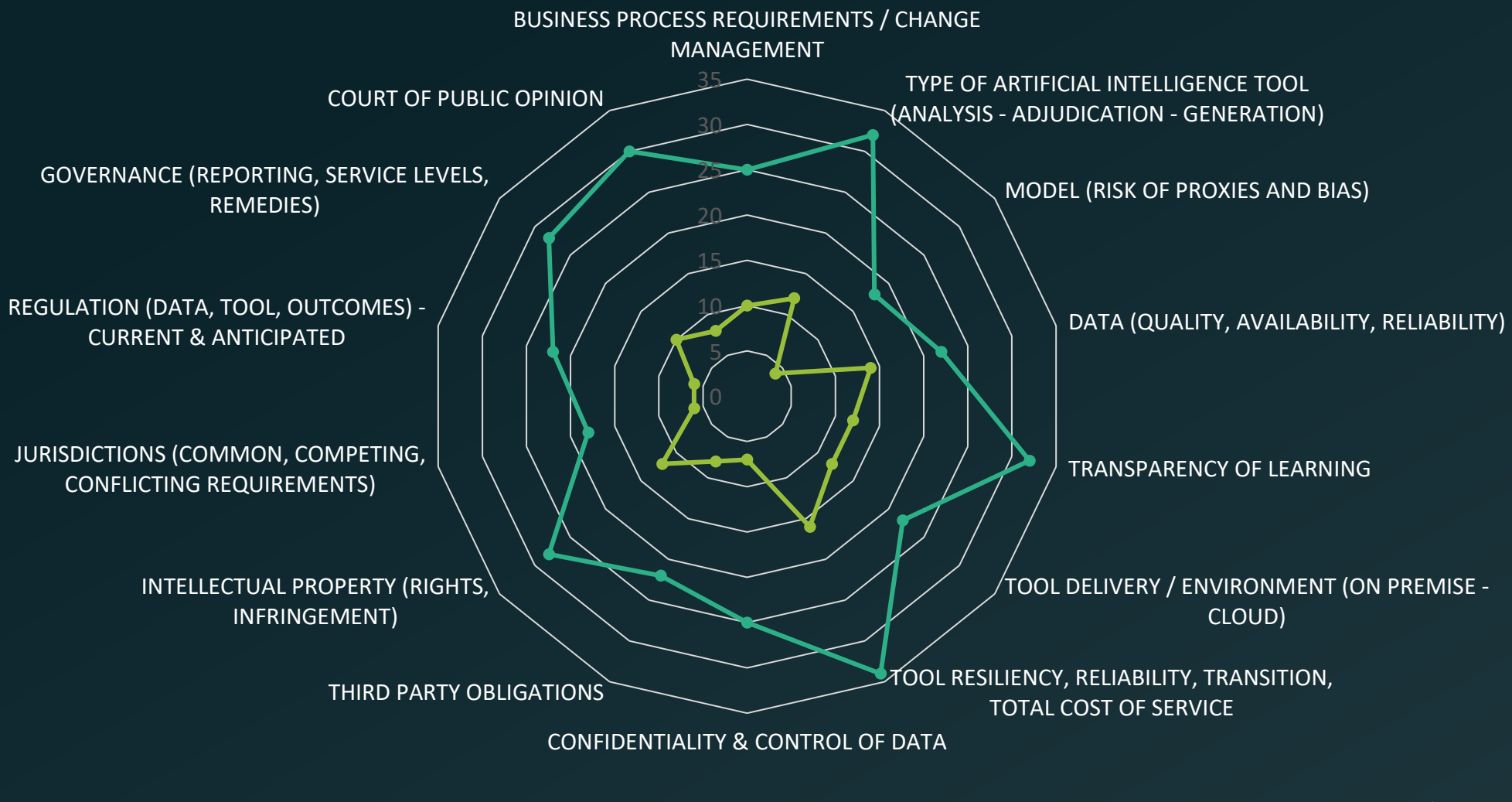
# THE AI ECOSYSTEM – AN EXAMPLE



# THE AI ECOSYSTEM – KEY POINTS

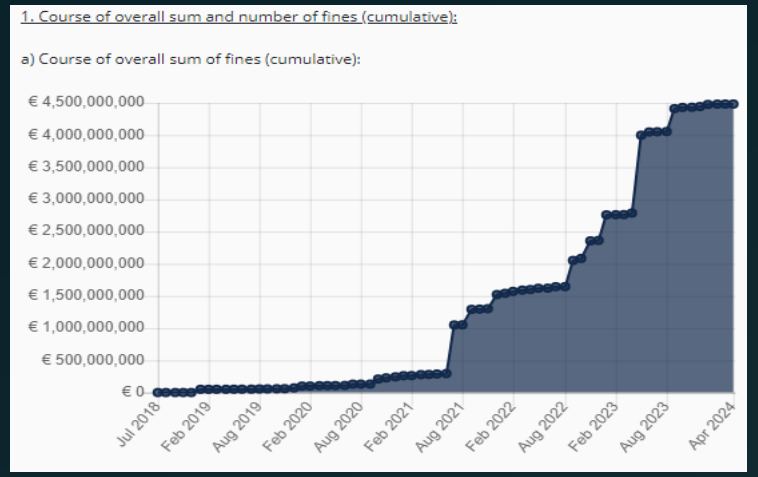


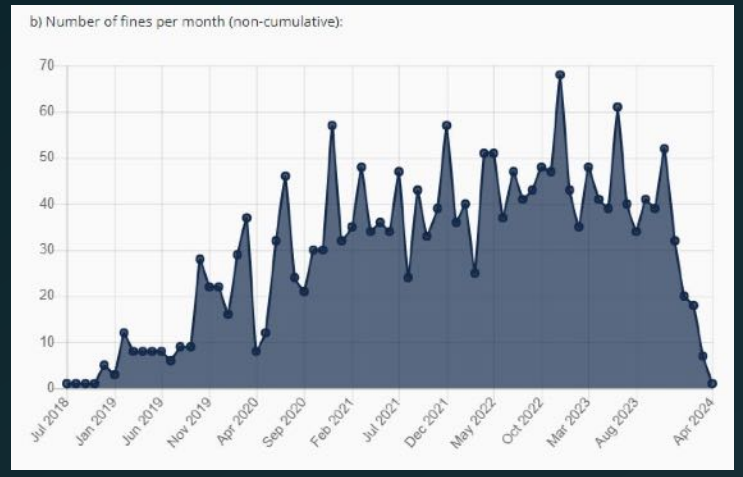
# UNDERSTANDING THE RISKS



# CHANGING FACE OF PRIVACY: LESSONS FROM GDPR

# LESSONS FROM GDPR: FINES




**Statistics: Highest individual fines (Top 10)**

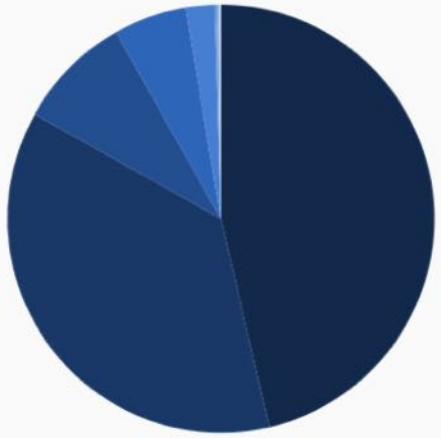
The following statistics shows the highest individual fines imposed to date per data controller (only top 10 fines).

| | Controller | Sector | Country | Fine [€] | Type of Violation | Date |
|---|---|---|---|---|---|---|
| 1 | **Meta Platforms Ireland Limited** | Media, Telecoms and Broadcasting | IRELAND | 1200000000 | Insufficient legal basis for data processing | 2023-05-12 |
| 2 | **Amazon Europe Core S.à.r.l.** | Industry and Commerce | LUXEMBOURG | 746000000 | Non-compliance with general data processing principles | 2021-07-16 |
| 3 | **Meta Platforms, Inc.** | Media, Telecoms and Broadcasting | IRELAND | 405000000 | Non-compliance with general data processing principles | 2022-09-05 |
| 4 | **Meta Platforms Ireland Limited** | Media, Telecoms and Broadcasting | IRELAND | 390000000 | Non-compliance with general data processing principles | 2023-01-04 |
| 5 | **TikTok Limited** | Media, Telecoms and Broadcasting | IRELAND | 345000000 | Non-compliance with general data processing principles | 2023-09-01 |
| 6 | **Meta Platforms Ireland Limited** | Media, Telecoms and Broadcasting | IRELAND | 265000000 | Insufficient technical and organisational measures to ensure information security | 2022-11-25 |
| 7 | **WhatsApp Ireland Ltd.** | Media, Telecoms and Broadcasting | IRELAND | 225000000 | Insufficient fulfilment of information obligations | 2021-09-02 |
| 8 | **Google LLC** | Media, Telecoms and Broadcasting | FRANCE | 90000000 | Insufficient legal basis for data processing | 2021-12-31 |
| 9 | **Facebook Ireland Ltd.** | Media, Telecoms and Broadcasting | FRANCE | 60000000 | Insufficient legal basis for data processing | 2021-12-31 |
| 10 | **Google Ireland Ltd.** | Media, Telecoms and Broadcasting | FRANCE | 60000000 | Insufficient legal basis for data processing | 2021-12-31 |

https://www.enforcementtracker.com/?insightsV; *enforcementtracker.com, provided by CMS Law.Tax*

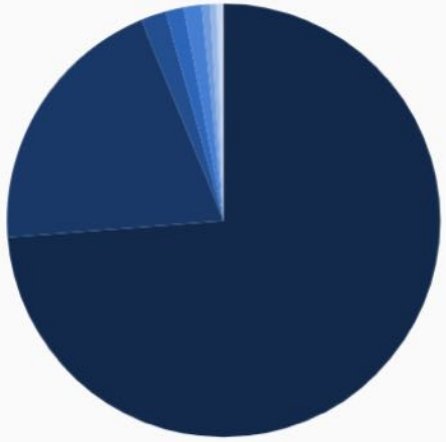
# LESSONS FROM GDPR: FINES

1. By total sum of fines:



| Violation | Sum of Fines |
|---|---|
| Non-compliance with general data processing principles | **€ 2,081,255,059** (at 572 fines) |
| Insufficient legal basis for data processing | **€ 1,650,044,012** (at 629 fines) |
| Insufficient technical and organisational measures to ensure information security | **€ 391,456,875** (at 364 fines) |
| Insufficient fulfilment of information obligations | **€ 247,848,060** (at 189 fines) |
| Insufficient fulfilment of data subjects rights | **€ 98,442,670** (at 199 fines) |
| Unknown | **€ 9,300,700** (at 10 fines) |
| Insufficient cooperation with supervisory authority | **€ 6,238,029** (at 110 fines) |
| Insufficient fulfilment of data breach notification obligations | **€ 3,021,182** (at 42 fines) |
| Insufficient data processing agreement | **€ 1,057,110** (at 11 fines) |
| Insufficient involvement of data protection officer | **€ 955,300** (at 20 fines) |

1. By total sum of fines:



| Sector | Sum of Fines |
|---|---|
| Media, Telecoms and Broadcasting | **€ 3,312,889,366** (at 290 fines) |
| Industry and Commerce | **€ 898,673,101** (at 445 fines) |
| Transportation and Energy | **€ 84,594,570** (at 109 fines) |
| Finance, Insurance and Consulting | **€ 60,664,758** (at 214 fines) |
| Employment | **€ 59,396,177** (at 132 fines) |
| Public Sector and Education | **€ 27,793,063** (at 238 fines) |
| Accomodation and Hospitalty | **€ 22,490,048** (at 65 fines) |
| Health Care | **€ 16,892,709** (at 194 fines) |
| Real Estate | **€ 2,601,831** (at 60 fines) |
| Individuals and Private Associations | **€ 1,858,166** (at 276 fines) |
| Not assigned | **€ 1,765,208** (at 123 fines) |

https://www.enforcementtracker.com/?insightsV; *enforcementtracker.com, provided by CMS Law.Tax*

# WHAT'S COMING IN THE CPPA?

# NEW RECORD KEEPING & SPOTCHECKS

**Policies and practices**

**62 (1)** An organization must make readily available, in plain language, information that explains the organization's policies and practices put in place to fulfil its obligations under this Act.

**Privacy management program**

**9 (1)** Every organization must implement a privacy management program that includes the organization's policies, practices and procedures put in place to fulfil its obligations under this Act, including policies, practices and procedures respecting

**(a)** the protection of personal information;

**(b)** how requests for information and complaints are received and dealt with;

**(c)** the training and information provided to the organization's staff respecting its policies, practices and procedures; and

**(d)** the development of materials to explain the organization's policies and procedures put in place to fulfil its obligations under this Act.

**Volume and sensitivity**

**(2)** In developing its privacy management program, the organization must take into account the volume and sensitivity of the personal information under its control.

**Appropriate purposes**

**12 (1)** An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

**Factors to consider**

**(2)** The following factors must be taken into account in determining whether the purposes referred to in subsection (1) are appropriate:

**(a)** the sensitivity of the personal information;

**(b)** whether the purposes represent legitimate business needs of the organization;

**(c)** the effectiveness of the collection, use or disclosure in meeting the organization's legitimate business needs;

**(d)** whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and

**(e)** whether the individual's loss of privacy is proportionate to the benefits in light of any measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual.

**Purposes**

**12(3)** An organization must determine at or before the time of the collection of any personal information each of the purposes for which the information is to be collected, used or disclosed and record those purposes.

**New purpose**

**12(4)** If the organization determines that the personal information it has collected is to be used or disclosed for a new purpose, the organization must record that new purpose before using or disclosing that information for the new purpose.

**Access by Commissioner — policies, practices and procedures**

**10** An organization must, on request of the Commissioner, provide the Commissioner with access to the policies, practices and procedures that are included in its privacy management program.

**Prohibition — use for initiating complaint or audit**

**110** The Commissioner must not use the information they receive under section 10 or paragraph 109(e) as grounds to initiate a complaint under subsection 82(2) or to carry out an audit under section 96.

# SAFEGUARDS & SERVICE PROVIDERS

**Security safeguards**

**57 (1)** An organization must protect personal information through physical, organizational and technological security safeguards. The level of protection provided by those safeguards must be proportionate to the sensitivity of the information.

**Factors to consider**

(2) In addition to the sensitivity of the information, the organization must, in establishing its security safeguards, take into account the quantity, distribution, format and method of storage of the information.

**Transfer to service provider**

**19** An organization may transfer an individual's personal information to a service provider without their knowledge or consent.

**Accountability — personal information under organization's control**

**7 (1)** An organization is accountable for personal information that is under its control.

**Personal information under control of organization**

**(2)** Personal information is under the control of the organization that decides to collect it and that determines the purposes for its collection, use or disclosure, regardless of whether the information is collected, used or disclosed by the organization itself or by a service provider on behalf of the organization.

**Same protection**

**11 (1)** If an organization transfers personal information to a service provider, the organization must ensure, by contract or otherwise, that the service provider provides substantially the same protection of the personal information as that which the organization is required to provide under this Act.

**Service provider obligations**

**(2)** The obligations under this Part, other than those set out in sections 57 and 61, do not apply to a service provider in respect of personal information that is transferred to it. However, the service provider is subject to all of the obligations under this Part if it collects, uses or discloses that information for any purpose other than the purposes for which the information was transferred.

# PENALTIES & PRIVATE RIGHT OF ACTION

**Imposition of penalty**

**94 (1)** The Tribunal may, by order, impose a penalty on an organization if

**(a)** the Commissioner files a copy of a decision in relation to the organization in accordance with subsection 93(4) or the Tribunal, on appeal, substitutes its own decision to recommend that a penalty be imposed on the organization for the Commissioner's decision not to recommend;

**(b)** the organization and the Commissioner are given the opportunity to make representations; and

**(c)** the Tribunal determines that imposing the penalty is appropriate.

**Maximum penalty**

**(4)** The maximum penalty for all the contraventions in a recommendation taken together is the higher of $10,000,000 and 3% of the organization's gross global revenue in its financial year before the one in which the penalty is imposed.

**Offence and punishment**

**125** Every organization that knowingly contravenes section 58, subsection 60(1), section 69 or 75 or subsection 124(1) or an order under subsection 92(2) or that obstructs the Commissioner or the Commissioner's delegate in the investigation of a complaint, in conducting an inquiry or in carrying out an audit is

**(a)** guilty of an indictable offence and liable to a fine not exceeding the higher of $25,000,000 and 5% of the organization's gross global revenue in its financial year before the one in which the organization is sentenced; or

**(b)** guilty of an offence punishable on summary conviction and liable to a fine not exceeding the higher of $20,000,000 and 4% of the organization's gross global revenue in its financial year before the one in which the organization is sentenced.

**Damages — contravention of Act**

**106 (1)** An individual who is affected by an act or omission by an organization that constitutes a contravention of this Act has a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the contravention if …

**Limitation period or prescription**

**(3)** An action must not be brought later than two years after the day on which the individual becomes aware of

**(a)** in the case of an action under subsection (1), the Commissioner's finding or, if there is an appeal, the Tribunal's decision; and

**(b)** in the case of an action under subsection (2), the conviction.

# (C-27) OTHER NEW LIABILITIES AND DEFENCES

***Artificial Intelligence and Data Act***

**Offences and Penalties**

**30(3)** A person who commits an offence …

**(a)** is liable, on conviction on indictment,

**(i)** to a fine of not more than the greater of $10,000,000 and 3% of the person's gross global revenues in its financial year before the one in which the person is sentenced, in the case of a person who is not an individual, and

**(b)** is liable, on summary conviction,

**(i)** to a fine of not more than the greater of $5,000,000 and 2% of the person's gross global revenues in its financial year before the one in which the person is sentenced, in the case of a person who is not an individual.

**Defence of due diligence**

30(4) A person is not to be found guilty of an offence under subsection (1) or (2) if they establish that they exercised due diligence to prevent the commission of the offence.

**Competition Act**

**Directors and officers of corporations**

**52** An officer, director or agent or mandatary of a corporation that commits a contravention of any of sections 6 to 9 of this Act or of Part 1 of the *Consumer Privacy Protection Act* that relates to a collection or use described in subsection 52(2) or (3) of that Act, or that engages in conduct that is reviewable under section 74.011 of the *Competition Act*, is liable for the contravention or reviewable conduct, as the case may be, if they directed, authorized, assented to, acquiesced in or participated in the commission of that contravention, or engaged in that conduct, whether or not the corporation is proceeded against.

**Vicarious liability**

**53** A person is liable for a contravention of any of sections 6 to 9 of this Act or of Part 1 of the *Consumer Privacy Protection Act* that relates to a collection or use described in subsection 52(2) or (3) of that Act, or for conduct that is reviewable under section 74.011 of the *Competition Act*, that is committed or engaged in, as the case may be, by their employee acting within the scope of their employment or their agent or mandatary acting within the scope of their authority, whether or not the employee or agent or mandatary is identified or proceeded against.

**Defence**

**54 (1)** A person must not be found to have committed a contravention of any of sections 6 to 9 of this Act or of Part 1 of the *Consumer Privacy Protection Act* that relates to a collection or use described in subsection 52(2) or (3) of that Act, or to have engaged in conduct that is reviewable under section 74.011 of the *Competition Act*, if they establish that they exercised due diligence to prevent the contravention or conduct, as the case may be.

# NEW RIGHTS: AUTOMATED DECISIONS, DISPOSAL & MOBILITY

**Disposal at individual's request**

**55 (1)** If an organization receives a written request from an individual to dispose of personal information that it has collected from the individual, the organization must, as soon as feasible, dispose of the information, unless

**(a)** disposing of the information would result in the disposal of personal information about another individual and the information is not severable; or

**(b)** there are other requirements of this Act, of federal or provincial law or of the reasonable terms of a contract that prevent it from doing so.

**Automated decision system**

**63(3)** If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual, the organization must, on request by the individual, provide them with an explanation of the prediction, recommendation or decision and of how the personal information that was used to make the prediction, recommendation or decision was obtained.

**Disclosure under data mobility framework**

**72** Subject to the regulations, on the request of an individual, an organization must as soon as feasible disclose the personal information that it has collected from the individual to an organization designated by the individual, if both organizations are subject to a data mobility framework provided under the regulations.

**Data mobility frameworks**

**120** The Governor in Council may make regulations respecting the disclosure of personal information under section 72, including regulations

**(a)** respecting data mobility frameworks that provide for

**(i)** safeguards that must be put in place by organizations to enable the secure disclosure of personal information under section 72 and the collection of that information, and

**(ii)** parameters for the technical means for ensuring interoperability in respect of the disclosure and collection of that information;

**(b)** specifying organizations that are subject to a data mobility framework; and

**(c)** providing for exceptions to the requirement to disclose personal information under that section, including exceptions related to the protection of proprietary or confidential commercial information.

# WHAT'S NEW IN QUEBEC?

# GOVERNANCE AND TRANSPARENCY

## Governance - Policies and Practices

3.2 Any person carrying on an enterprise must establish and implement governance policies and practices regarding personal information that ensure the protection of such information.

Such policies and practices must, in particular, provide a framework for the keeping and destruction of the information, define the roles and responsibilities of the members of its personnel throughout the life cycle of the information and provide a process for dealing with complaints regarding the protection of the information. The policies and practices must also be proportionate to the nature and scope of the enterprise's activities and be approved by the person in charge of the protection of personal information.

Detailed information about those policies and practices, in particular as concerns the content required under the first paragraph, must be published in simple and clear language on the enterprise's website or, if the enterprise does not have a website, made available by any other appropriate means.

## Transparency

8. Any person who collects personal information from the person concerned must, when the information is collected and subsequently on request, inform that person

(1) of the purposes for which the information is collected;

(2) of the means by which the information is collected;

(3) of the rights of access and rectification provided by law; and

(4) of the person's right to withdraw consent to the communication or use of the information collected.

If applicable, the person concerned is informed of the name of the third person for whom the information is being collected, the name of the third persons or categories of third persons to whom it is necessary to communicate the information for the purposes referred to in subparagraph 1 of the first paragraph, and the possibility that the information could be communicated outside Québec.

On request, the person concerned is also informed of the personal information collected from him, the categories of persons who have access to the information within the enterprise, the duration of the period of time the information

## Transparency – technological means

8.2. Any person who collects personal information through technological means must publish on the enterprise's website, if applicable, a confidentiality policy drafted in clear and simple language and disseminate it by any appropriate means to reach the persons concerned. The person must do the same for the notice required for any amendment to such a policy.

# PROFILING, PRIVACY BY DEFAULT & AUTOMATED DECISIONS

## Profiling

8.1 In addition to the information that must be provided in accordance with section 8, any person who collects personal information from the person concerned using technology that includes functions allowing the person concerned to be identified, located or profiled must first inform the person

(1) of the use of such technology; and

(2) of the means available to activate the functions that allow a person to be identified, located or profiled. “Profiling” means the collection and use of personal information to assess certain characteristics of a natural person, in particular for the purpose of analyzing that person’s work performance, economic situation, health, personal preferences, interests or behaviour.

## Privacy by Default

9.1 Any person carrying on an enterprise who collects personal information when offering to the public a technological product or service having privacy settings must ensure that those settings provide the highest level of confidentiality by default, without any intervention by the person concerned.

The first paragraph does not apply to privacy settings for browser cookies.

## Decisions Based On Automated Processing

12.1 Any person carrying on an enterprise who uses personal information to render a decision based exclusively on an automated processing of such information must inform the person concerned accordingly not later than at the time it informs the person of the decision.

He must also inform the person concerned, at the latter’s request,

- (1) of the personal information used to render the decision;
- (2) of the reasons and the principal factors and parameters that led to the decision; and
- (3) of the right of the person concerned to have the personal information used to render the decision corrected.

The person concerned must be given the opportunity to submit observations to a member of the personnel of the enterprise who is in a position to review the decision.

# PRIVACY IMPACT ASSESSMENT

## Project to acquire, develop or overhaul an information system or electronic service delivery system

3.3 Any person carrying on an enterprise must conduct a privacy impact assessment for any project to acquire, develop or overhaul an information system or electronic service delivery system involving the collection, use, communication, keeping or destruction of personal information.

For the purposes of such an assessment, the person must consult the person in charge of the protection of personal information within the enterprise from the outset of the project.

The person must also ensure that the project allows computerized personal information collected from the person concerned to be communicated to him in a structured, commonly used technological format.

The conduct of a privacy impact assessment under this Act must be proportionate to the sensitivity of the information concerned, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.

## Communication outside of Québec

17. Before communicating personal information outside Québec, a person carrying on an enterprise must conduct a privacy impact assessment. The person must, in particular, take into account

- (1) the sensitivity of the information;
- (2) the purposes for which it is to be used;
- (3) the protection measures, including those that are contractual, that would apply to it; and
- (4) the legal framework applicable in the State in which the information would be communicated, including the personal information protection principles applicable in that State.

The information may be communicated if the assessment establishes that it would receive adequate protection, in particular in light of generally recognized principles regarding the protection of personal information. The communication of the information must be the subject of a written agreement that takes into account, in particular, the results of the assessment and, if applicable, the terms agreed on to mitigate the risks identified in the assessment.

The same applies where the person carrying on an enterprise entrusts a person or body outside Québec with the task of collecting, using, communicating or keeping such information on his behalf. This section does not apply to a communication of information under subparagraph 7 of the first paragraph of section 18.

## Study or research purposes or for the production of statistics

21. A person carrying on an enterprise may communicate personal information without the consent of the persons concerned to a person or body wishing to use the information for study or research purposes or for the production of statistics.

The information may be communicated if a privacy impact assessment concludes that

- (1) the objective of the study or research or of the production of statistics can be achieved only if the information is communicated in a form allowing the persons concerned to be identified;
- (2) it is unreasonable to require the person or body to obtain the consent of the persons concerned;
- (3) the objective of the study or research or of the production of statistics outweighs, with regard to the public interest, the impact of communicating and using the information on the privacy of the persons concerned;
- (4) the personal information is used in such a manner as to ensure confidentiality; and
- (5) only the necessary information is communicated.

# PENALTIES & PRIVATE RIGHT OF ACTION

## Administrative Monetary Penalties

90.12 The maximum amount of the monetary administrative penalty is $50,000 in the case of a natural person and, in all other cases, $10,000,000 or, if greater, the amount corresponding to 2% of worldwide turnover for the preceding fiscal year.

## Penal Sanctions

91. Anyone who

- (1) collects, uses, communicates, keeps or destroys personal information in contravention of the law,
- (2) fails to report, where required to do so, a confidentiality incident to the Commission or to the persons concerned,
- (3) contravenes the prohibition set out in section 8.4,
- (4) does not take the security measures necessary to ensure the protection of the personal information in accordance with section 10,
- (5) identifies or attempts to identify a natural person using de-identified information without the authorization of the person holding the information or using anonymized information,
- (6) is a personal information agent and contravenes any of sections 70, 70.1, 71, 72, 78, 79 and 79.1,
- (7) impedes the progress of an inquiry or inspection of the Commission or the hearing of an application by the Commission by providing it with false or inaccurate information, by omitting to provide information it requires or otherwise,
- (8) contravenes section 81.1,
- (9) refuses or neglects to comply, within the specified time, with a demand made under section 81.3, or (10) fails to comply with an order of the Commission

commits an offence and is liable to a fine of $5,000 to $100,000 in the case of a natural person and, in all other cases, of $15,000 to $25,000,000, or, if greater, the amount corresponding to 4% of worldwide turnover for the preceding fiscal year.

## Private Civil Right of Action

93.1 Where the unlawful infringement of a right conferred by this Act or by articles 35 to 40 of the Civil Code causes an injury and the infringement is intentional or results from a gross fault, the court shall award punitive damages of not less than $1,000.

# MANAGING CHANGE: TECHNOLOGY RISKS

# STRATEGIC TECHNOLOGY RISKS

- OBJECTIVE:  Align technology investments to business strategy to sustain / deliver competitive advantage
- FOUR KEY RISKS:
  - *Operational*
    - Functional (does the technology delivery the required business process)
    - Non-Functional (is the technology reliable, resilient, secure and cost effective over expected life)
  - *Information* - Utility, Availability, Reliability, Quality
  - *Compliance* – Data, Technology (tool) and Outcome (dependent upon use case & jurisdiction)
  - *Change Management*
    - Currency (support, maintenance and continuous improvement)
    - Ecosystem (applications, data sources, systems, integrations, environments)
    - Project Delivery
    - Organizational Change Management

# TECHNOLOGY PROJECTS OFTEN FAIL… WHY?

**Table 4**
IT project failure factors and causes in the literature.

| Failure Factor (F1 - 12) | Cause of Failure (CF1 – CF33) |
|---|---|
| 1. Objectives | 1. Unrealistic objectives<br>2. Unclear objectives<br>3. Changing objectives |
| 2. Senior Management | 4. Lack of management involvement<br>5. Lack of management commitment<br>6. Lack of management support |
| 3. Planning | 7. Unrealistic planning<br>8. Underestimation<br>9. Schedule pressure |
| 4. Requirements | 10. Unclear requirements<br>11. Requirement changes |
| 5. Project Execution and Control | 12. Inadequate project execution and control<br>13. Inadequate change management<br>14. Inappropriate method |
| 6. Technology | 15. Immature technology<br>16. Technology new to the organisation<br>17. Too much customisation |
| 7. Software Development Method | 18. Inadequate system engineering<br>19. Excessive scale and complexity<br>20. Method and process |
| 8. User Involvement | 21. Lack of user input and user involvement<br>22. Lack of user training<br>23. Failure to manage user expectations |
| 9. Staff | 24. Lack of skills and experience<br>25. Insufficient staff<br>26. Unmotivated staff |
| 10. Contractors | 27. Poor performance<br>28. Underestimation by contractors and consultants<br>29. Lack of experience in contractor management |
| 11. Risk Management | 30. Inadequate analysis and management of risk |
| 12. Other | 31. External changes<br>32. Organisational complexity<br>33. Lack of trouble-shooting capability |

**Table 3**
Consistency of identified failure factors over time.

| Dice Correlation Coefficients | 1. | 2. | 3. | 4. | 5. | 6. | 7. | 8. | 9. | 10. | 11. | 12. | 13. | 14. | 15. | 16. | 17. | 18. | 19. | 20. | 21. | 22. | 23. | 24. | MEAN | VAR | STDDEV |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1. 2014 Kerzner** | | .8 | .9 | .6 | .9 | .9 | .8 | .7 | .6 | .8 | .5 | .8 | .9 | .8 | .8 | .8 | .8 | .8 | .7 | .8 | .8 | .8 | .7 | .6 | .753 | .014 | .119 |
| **2. 2014 Standish** | | | .8 | .6 | .8 | .9 | .8 | .6 | .7 | .9 | .6 | .8 | .8 | .8 | .8 | .9 | .6 | .8 | .7 | .6 | .8 | .9 | .8 | .7 | .754 | .010 | .102 |
| **3. 2009 Chua** | | | | .4 | .9 | .9 | .8 | .7 | .5 | .7 | .5 | .7 | .9 | .9 | .9 | .8 | .9 | .7 | .6 | .9 | .8 | .8 | .6 | .5 | .744 | .022 | .147 |
| **4. 2009 Cerpa** | | | | | .6 | .6 | .7 | .5 | .6 | .5 | .2 | .3 | .5 | .5 | .6 | .5 | .3 | .3 | .5 | .3 | .5 | .6 | .7 | .6 | .510 | .017 | .129 |
| **5. 2008 McManus** | | | | | | .9 | .8 | .8 | .6 | .8 | .5 | .8 | .8 | .8 | .9 | .8 | .8 | .8 | .7 | .8 | .9 | .8 | .7 | .6 | .763 | .015 | .137 |
| **6. 2008 El-Emam** | | | | | | | .8 | .6 | .6 | .8 | .5 | .8 | .8 | .8 | .7 | .9 | .7 | .8 | .6 | .7 | .8 | .8 | .7 | .6 | .739 | .014 | .118 |
| **7. 2008 Verner** | | | | | | | | .6 | .5 | .7 | .5 | .7 | .9 | .8 | .8 | .8 | .7 | .7 | .4 | .7 | .8 | .6 | .6 | .5 | .685 | .018 | .133 |
| **8. 2008 Meier** | | | | | | | | | .5 | .6 | .2 | .8 | .6 | .5 | .7 | .7 | .6 | .6 | .7 | .6 | .9 | .6 | .3 | .4 | .597 | .024 | .154 |
| **9. 2007 Fowler** | | | | | | | | | | .6 | .0 | .6 | .5 | .6 | .5 | .7 | .4 | .6 | .7 | .4 | .5 | .7 | .7 | .5 | .544 | .023 | .181 |
| **10. 2006 Kappelman** | | | | | | | | | | | .7 | .8 | .7 | .7 | .7 | .8 | .7 | .7 | .7 | .7 | .8 | .8 | .7 | .8 | .716 | .008 | .089 |
| **11. 2005 Charette** | | | | | | | | | | | | .4 | .5 | .4 | .5 | .4 | .4 | .4 | .3 | .4 | .5 | .4 | .5 | .6 | .437 | .022 | .164 |
| **12. 2003 Ewusi-Mensah** | | | | | | | | | | | | | .7 | .7 | .6 | .9 | .7 | .8 | .5 | .7 | .8 | .6 | .5 | .6 | .675 | .018 | .144 |
| **13. 2002 Yeo** | | | | | | | | | | | | | | .8 | .8 | .8 | .8 | .7 | .6 | .8 | .8 | .8 | .6 | .5 | .712 | .021 | .129 |
| **14. 2002 Yardley** | | | | | | | | | | | | | | | .7 | .8 | .8 | .7 | .5 | .8 | .7 | .8 | .7 | .6 | .695 | .015 | .121 |
| **15. 2001 Brown** | | | | | | | | | | | | | | | | .7 | .7 | .6 | .6 | .7 | .8 | .8 | .6 | .5 | .696 | .014 | .132 |
| **16. 2001 Schmidt** | | | | | | | | | | | | | | | | | .6 | .9 | .5 | .6 | .8 | .7 | .7 | .5 | .715 | .020 | .141 |
| **17. 1998 Glass** | | | | | | | | | | | | | | | | | | .5 | .7 | 1. | .8 | .8 | .5 | .6 | .667 | .024 | .155 |
| **18. 1998 Keil** | | | | | | | | | | | | | | | | | | | .4 | .5 | .7 | .6 | .5 | .4 | .624 | .023 | .152 |
| **19. 1995 Jones** | | | | | | | | | | | | | | | | | | | | .7 | .7 | .8 | .6 | .7 | .604 | .017 | .130 |
| **20. 1995 Cole** | | | | | | | | | | | | | | | | | | | | | .8 | .8 | .5 | .6 | .667 | .024 | .124 |
| **21. 1987 Morris** | | | | | | | | | | | | | | | | | | | | | | .8 | .6 | .6 | .731 | .015 | .124 |
| **22. 1987 Pinto** | | | | | | | | | | | | | | | | | | | | | | | .8 | .7 | .726 | .012 | .108 |
| **23. 1984 Keider** | | | | | | | | | | | | | | | | | | | | | | | | .9 | .638 | .015 | .123 |
| **24. 1983 Baker** | | | | | | | | | | | | | | | | | | | | | | | | | .586 | .015 | .122 |
| Max | | | | | | | | | | | | | | | | | | | | | | | | | | .024 | .181 |

- **KEY CONSIDERATIONS**:
  - Failure to understand business process and desired change
  - Failure to develop comprehensive requirements (functional and non-functional)
  - Failure to address ecosystem complexity
  - Failure to scale governance to risk and complexity (currency vs transformation projects)

- **CONSIDER**: Complexity of the evolution and dynamic nature of AI

J. Schmidt, "Mitigating risk of failure in information technology projects: Causes and mechanisms" *Project Leadership and Society* , 4 (2023) 100097

# GOVERNANCE OF TECHNOLOGY – SUMMARY

**External Opportunity**
(Market, Customers, Suppliers, Competitors, Regulators)

**Strategy**
(Align Business Operations to Opportunities)

**Business Process**
(Align Business Process and Technology to Strategy)

**Governance of Delivery**
(Alignment of Delivery to Strategy, Operational Stability, Ecosystem Optimization, Data Driven Decision Making, Preservation of Rights, Security, Compliance & Diligence Defence)

**Governance of Change**
(Currency (support and maintenance), Ecosystem Change Management, Project Delivery, Organizational Change Management, Compliance & Diligence Defence)

**Governance of Transformation**
(Procurement, Mergers & Acquisitions, Divestiture, Ecosystem Integration and Change Management, Project Delivery, Organizational Change Management, Compliance & Diligence Defence)

# INCREASING COMPLEXITY OF SECURITY

# AI BEING USED FOR HACKING AND MISINFORMATION, TOP CANADIAN CYBER OFFICIAL SAYS

By Raphael Satter - July 20, 2023

*WASHINGTON, July 20 (Reuters) - Hackers and propagandists are wielding artificial intelligence (AI) to create malicious software, draft convincing phishing emails and spread disinformation online, Canada's top cybersecurity official told Reuters, early evidence that the technological revolution sweeping Silicon Valley has also been adopted by cybercriminals.*

*In an interview this week, Canadian Centre for Cyber Security Head Sami Khoury said that his agency had seen AI being used "in phishing emails, or crafting emails in a more focused way, in malicious code (and) in misinformation and disinformation.“ ....*

*In recent months several cyber watchdog groups have published reports warning about the hypothetical risks of AI - especially the fast-advancing language processing programs known as large language models (LLMs), which draw on huge volumes of text to craft convincing-sounding dialogue, documents and more.*

*In March, the European police organization Europol published a report, saying that models such as OpenAI's ChatGPT had made it possible "to impersonate an organisation or individual in a highly realistic manner even with only a basic grasp of the English language." The same month, Britain's National Cyber Security Centre said in a blog post, that there was a risk that criminals "might use LLMs to help with cyber attacks beyond their current capabilities.“ ....*

https://www.reuters.com/technology/ai-being-used-hacking-misinfo-top-canadian-cyber-official-says-2023-07-20/

# THE NEAR-TERM IMPACT OF AI ON THE CYBER THREAT

•Artificial intelligence (AI) will **almost certainly increase the volume and heighten the impact of cyber attacks** over the next two years. However, the **impact on the cyber threat will be uneven**

•The threat to 2025 comes from **evolution and enhancement of existing tactics, techniques and procedures**

•**All types of cyber threat actor** – state and non-state, skilled and less skilled – are already using AI, **to varying degrees**

•AI provides **capability uplift in reconnaissance and social engineering**, almost certainly making both more effective, efficient, and harder to detect.

https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

# THE NEAR-TERM IMPACT OF AI ON THE CYBER THREAT

•More **sophisticated uses of AI in cyber operations** are highly likely to be restricted to threat actors with access to **quality training data, significant expertise (in both AI and cyber), and resources.** More advanced uses are unlikely to be realised before 2025.

•AI will almost certainly make cyber attacks against the UK more impactful because **threat actors will be able to analyse exfiltrated data faster and more effectively, and use it to train AI models.**

•AI lowers the barrier for novice cyber criminals, hackers-for-hire and hacktivists to carry out effective access and information gathering operations. This **enhanced access will likely contribute to the global ransomware threat** over the next two years.

•Moving towards 2025 and beyond, commoditisation of AI-enabled capability in criminal and commercial markets will almost certainly make **improved capability available to cyber crime and state actors.**

https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

# HONG KONG CLERK DEFRAUDED OF $25 MILLION IN SOPHISTICATED DEEPFAKE SCAM

By Drew Todd,  February 13, 2024,

*...  A finance clerk working at a Hong Kong branch of a large multinational corporation recently fell victim to an elaborate scam utilizing deepfake technology to impersonate senior executives and swindle more than $25 million, according to reports.*

*The scam began with the employee receiving a phishing message purportedly from the company's chief financial officer requesting an urgent confidential transaction. Despite initial skepticism, the clerk's doubts were eased after joining a video conference call where deepfakes impersonated both the CFO and other senior managers familiar to the clerk.*

*Police investigations revealed that the deepfakes likely relied on publicly available company videos and audio to digitally recreate the likenesses and voices of executives. By not engaging the clerk directly beyond an introduction, the fakes appeared more genuine and authoritative. Over multiple transactions, the criminals accumulated $25 million transferred to Hong Kong accounts before the company discovered and reported the fraud.*

*This complex scam represents the first known case of using customized deepfakes to mimic an entire group meeting to manipulate staff. Authorities described it as a "new deception tactic" showing sophisticated technological capabilities.*

https://www.secureworld.io/industry-news/hong-kong-deepfake-cybercrime

# WE STUDENTS ARE FINDING WAYS TO FIGHT BACK AGAINST THE AI INTERVIEW

Finn O'Mahony,  April 22, 2024

*In the past three months, in my final year at a Russell Group university studying business management, I've applied for 50 jobs in finance — filling out forms in between lectures, dissertation research and pulling all-nighters to hit the word count for coursework essays.*

*The job market today looks nothing like it did for graduates even a few years ago. Applications to the country's top employers jumped by almost a third in 2023 on the previous year, according to the Graduate Market in 2024 report from High Fliers Research. For banking and finance, employers typically receive 90-100 applications per job space, so 99 percent of applicants are being turned down.*

*Gone are the days of uploading a CV and cover letter outlining your motivations for wanting to join a company. Those seeking to start out in finance in 2024 will face up to six rounds of assessments, the first three conducted by AI, and students are finding ways to fight back.*

https://thetimes.co.uk/article/university-grad-scheme-ai-job-interview-stage-robots-9hdct76qk

# THE GLAZE PROJECT (NIGHTSHADE)

The Glaze Project (including Glaze, Nightshade, WebGlaze and others) is a research effort that develops technical tools with the explicit goal of protecting human creatives against invasive uses of generative artificial intelligence or GenAI. Our team is composed of computer science professors and PhD students from the University of Chicago. We perform research studies and develop tools that artists can use to disrupt unauthorized AI training on their work product.

Ultimately, our goal is to ensure the continued vitality of human artists, and to restore balance and ensure a healthy coexistence between AI and human creatives, where the human creatives retain agency and control over their work products and their use.

Since 2022, our team has released multiple tools, including Glaze, a tool to disrupt art style mimicry, Nightshade, a tool to disincentivize training without consent on scraped images, and WebGlaze, a free web service to make Glaze accessible to artists with limited computing resources. ...

To date, artists across the globe have downloaded Glaze more than 2.3 million times in the last year, and Nightshade more than 300,000 times in 2 months.

https://nightshade.cs.uchicago.edu/aboutus.html

# MISINFORMATION / DISINFORMATION

Cyber spy agency warns foreign adversaries will 'weaponize' AI to influence next federal election: *CSE says capacity to generate deepfakes exceeds its ability to detect them* - Catharine Tunney · CBC News · Dec 06, 2023

https://www.cbc.ca/news/politics/artificial-intelligence-cse-election-1.7050563

AI-powered disinformation is spreading — is Canada ready for the political impact? The rise of deepfakes comes as billions of people around the world prepare to vote this year - Catharine Tunney · CBC News · Jan 21, 2024

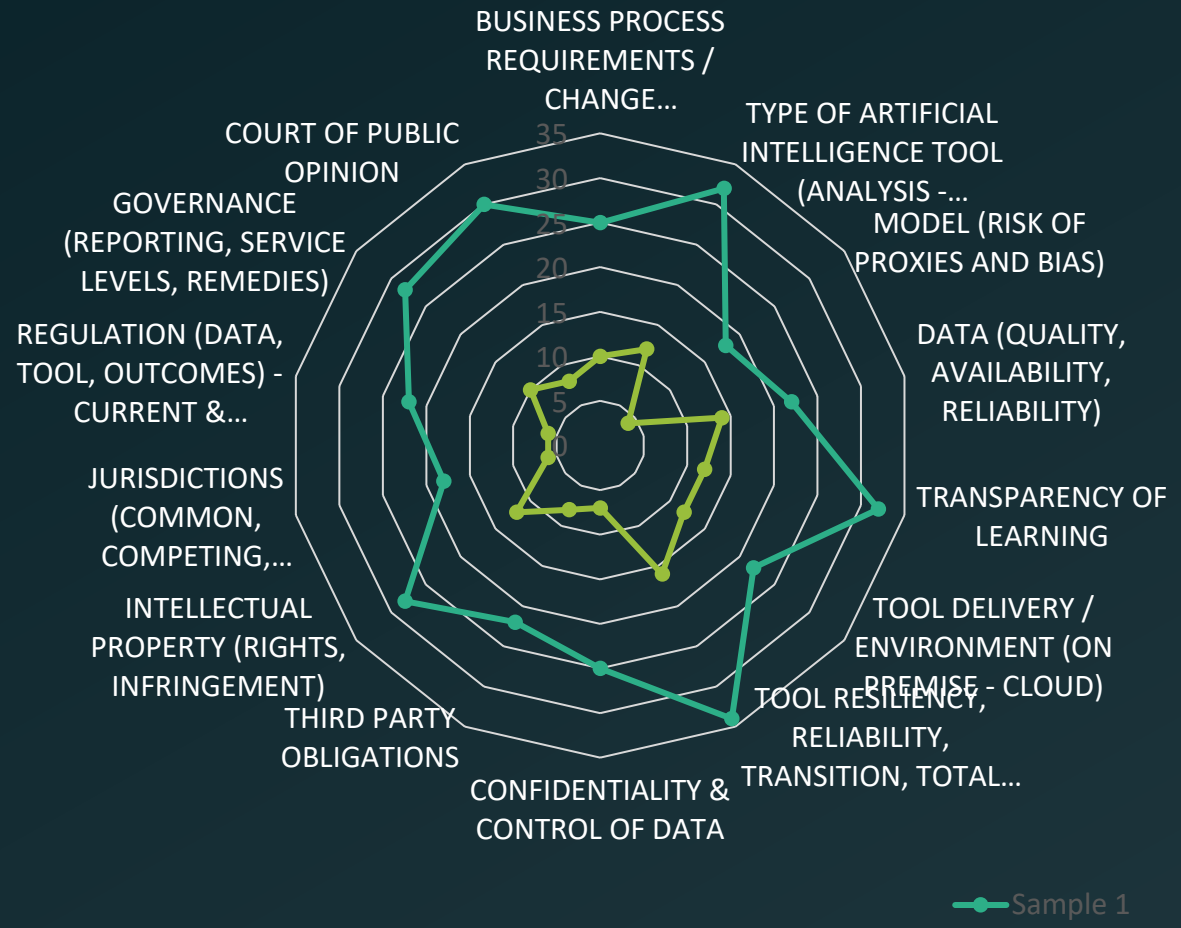
https://www.cbc.ca/news/politics/ai-deepfake-election-canada-1.7084398

**AI-powered misinformation is the world's biggest short-term threat, Davos report says - Kelvin Chan January 10, 2024 - LONDON (AP) — False and misleading information supercharged with cutting-edge artificial intelligence that threatens to erode democracy and polarize society is the top immediate risk to the global economy, the World Economic Forum said in a report Wednesday.**

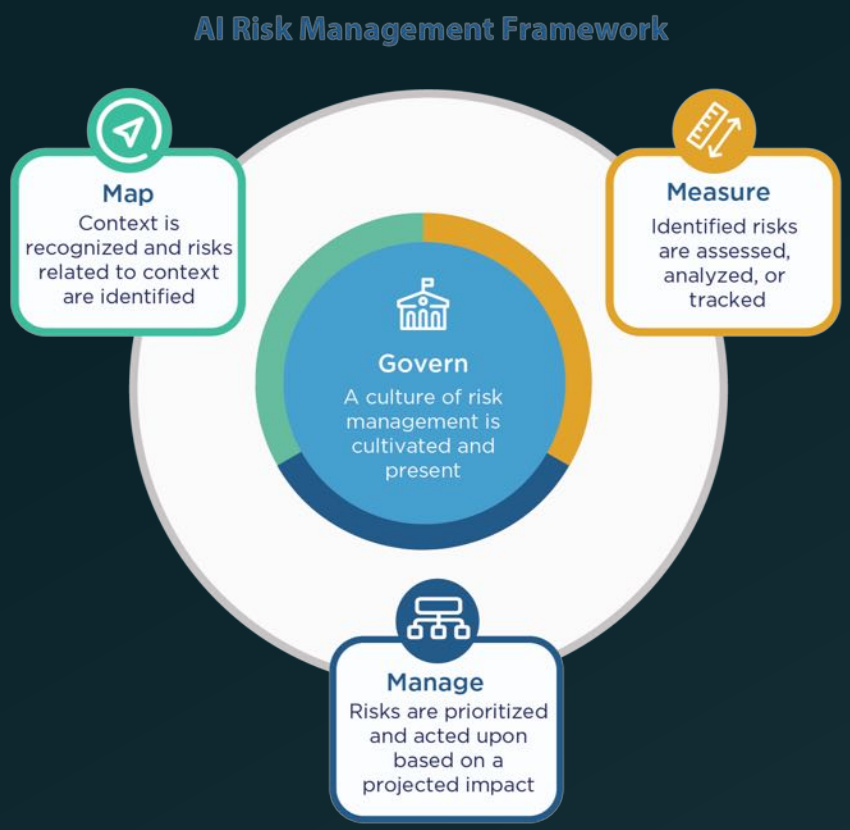
**https://apnews.com/article/artificial-intelligence-davos-misinformation-disinformation-climate-change-106a1347ca9f987bf71da1f86a141968**

# GOVERNACE: PRACTICAL APPROACH REQUIRED

# REMEMBER: GOVERANCE IS MORE THAN A CHECKLIST



# NATIONAL INSTITUE OF STANDARDS AND TECHNOLOGIES (NIST): AI RISK MANAGEMENT FRAMEWORK




https://airc.nist.gov/AI_RMF_Knowledge_Base/AI_RMF

- Many competing definitions and frameworks, consensus not yet established
- Each Regulator and Industry Group advocating for their viewpoint
- Consider also:
  - *IT General*: ITIL, ISO, COBIT, PMI
  - *AI Specific*: ISDE *(Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems), G-7 (Hiroshima Process International Code of Conduct for Advanced AI Systems)* as well as numerous other voluntary or industry codes

# AI COMPLIANCE PROGRAM


- Key Components of AI Compliance Program:
  - *Champion:* Key Sponsor Support
  - *Scope:* Governance & Policy
  - *Identify:* Environmental Scan
  - *Assess:* Evaluate
  - *Recommend:* Mitigate & Report
  - *Document:* Defensive Documentation
  - *Support:* Training & Audit

- Never forget - you will be tested against your documentation.

# AMARA'S LAW

"Humans tend to overestimate the effect of a technology in the short-term and underestimate its effect in the long-term."

Bennett Jones

# THANK YOU