Privacy In AI: Examining Legal Variations in the EU, US, and Canada

1st Aditi Venkatesh
School of Computer Science
University of Guelph
Guelph, Canada
avenkate@uoguelph.ca

2nd Shreya Bhoje
School of Computer Science
University of Guelph
Guelph, Canada
sbhoje@uoguelph.ca

***Abstract*—The widespread adoption of Artificial Intelligence (AI) technologies has sparked global concerns regarding data privacy and protection. In response, countries worldwide are actively working on formulating and implementing regulations specifically designed for AI. These regulations seek to oversee the collection, storage, utilization, and disposal of individuals' data by organizations employing AI. Our research focuses on the proposed EU legislation known as the Artificial Intelligence (AI) Act, the US AI Bill of Rights, and Canada's AI and data Act, a component of Bill C-27. Through a comparative analysis, this study aims to identify commonalities and disparities among these regulations. The objective is to shed light on strategies for safeguarding privacy in the realm of artificial intelligence and to highlight associated risks. Our primary goal is to pinpoint the inadequacy within the privacy regulation framework adopted by Canada. The research enables to point out the inadequacy in the Artifical Intelligence and Data Act of Canada in serveral sections such as Transparency, Data protection and Automated decision making.**

***Index Terms*—Artificial Intelligence, legislation, privacy protection, data protection, transparency, automated decision making, discrimination**

I. Introduction

In the ever-evolving world of technological growth, one phenomenon stands out as a catalyst for transformative change: Artificial Intelligence (AI). There has been a new realm created in which the complexity of human intelligence is mirrored by machines that can learn, adapt, and make judgments. Imagine living in a world where our daily interactions involve talking to a helpful virtual assistant that understands our needs and responds accordingly. This is the marvel of artificial intelligence (AI) in action. The field of AI has experienced remarkable growth in recent years. From voice assistants and recommendation engines to sophisticated robotics and self-driving cars, technology has swiftly become a part of many aspects of our daily life [1]. AI's applications are expanding in variety as it develops, having an effect on sectors including healthcare, finance, and transportation. However, as our reliance on AI grows, so does the importance of protecting our privacy. Picture this: every time we ask our virtual assistant a question or give a command, it processes and stores that information. The question of how this data is handled, who has access to it, and how it's used becomes a critical concern. This is where privacy laws in AI come into play and has raised concerns about moral application of AI, notably with regard to data privacy.

Global privacy laws are diverse, reflecting a constantly changing regulatory environment a strong standard has been established in the European Union by the General Data Protection Regulation (GDPR) [2], which emphasizes personal data subject's control. In contrast, the US has a more disjointed privacy framework since it depends on industry-specific legislation like Gramm-Leach-Bliley Act (GLBA) [3] and Health Insurance Portability and Accountability Act (HIPAA) [4]. The Personal Information Protection and Electronic Documents Act (PIPEDA) [5], which is relevant to business operations, is followed in Canada. There is a global trend toward the recognition of privacy as a fundamental right and the strengthening of data protection authorities. Understanding the state of privacy laws today is crucial as we work through the complexities of these changing legislation, taking into account the effects they have on data governance and individual rights in an increasingly linked world.

Within this landscape of privacy laws, a particular focus on privacy in the context of AI adds a layer of complexity Now, when it comes to AI, it gets trickier. AI uses data, and we want to make sure it's used responsibly. Governments worldwide are realizing there is need for strong privacy rules to keep people's personal information safe. Europe is big on transparency and control, the U.S. is figuring out a federal law, and Canada is adapting to the digital age. Although privacy regulations currently vary in different parts of the world, there is a global awareness of the concerns associated with AI technologies. Many countries have made or suggested laws to control how AI systems collect, use, and keep personal data [6]. These laws aim to find a good balance between encouraging innovation and safeguarding people's privacy rights. The laws are adapting to the challenges posed by AI advancements and the increasing use of digital technology in society.

Our research aims to examine and compare privacy laws pertaining to artificial intelligence (AI) in the European Union (EU), the United States and Canada. We seek to understand how these regions address challenges associated with AI-driven data processing and ensure the protection of individuals' personal data by evaluating legal consequences and structures. The background section provides an overview of AI reg-

ulatory frameworks in these areas, annotate key principles. In our methodology, we categorize the analysis into aspects such as data protection, automated decision-making, discrimination, and civil rights transparency and explainability. The discussion section presents our findings in a tabular format, showcasing comparisons across privacy categories. The conclusion summarizes crucial insights, evaluates the effectiveness of privacy regulations, and provides recommendations for improvement, offering a comprehensive conclusion to our study.

II. Background

The use of AI systems, when not implemented or managed appropriately, poses significant privacy risks that can impact individuals, communities, and society at large. The risk becomes most significant when there is interference with the fundamental human right of making decisions referred to as "Hacking the Mind" by Manheim and Caplan [7]. One popular example of this is when the data analytics company Cambridge Analytica involved in Donald Trump's election campaign and the successful Brexit campaign obtained millions of Facebook profiles of American voters, resulting in one of the largest data breaches in the history of the tech giant. These profiles were then utilized to develop a robust software program, enabling the prediction and manipulation of choices during the electoral process [8]. This shows that the results were predominantly influenced by a manipulative and undemocratic strategy involving targeted psychological online profiling, demonstrating a cynical and calculated approach to sway the general public [9].

The AI laws and regulations are gaining traction as AI is spanning wide day by day. This is evident from few of the recent implementation of the same in various regions. In 2021, the Australian Information Commissioner's Office determined that Clearview AI had contravened the Australian Privacy Act by collecting images and biometric data without obtaining proper consent. Subsequently, the United Kingdom's Information Commissioner's Office (ICO) and privacy authorities in France and Canada took similar actions against the organization [10]. Despite the identification of risks and implementation of laws against privacy breaches, it is difficult to carve the perfect framework to regulate AI due to its dynamic nature. Owing to the responsibility towards the users, the authorities are required to establish comprehensive AI regulations.

A. Artificial Intelligence Act

To regulate the Artificial Intelligence, EU proposed a regulatory framework, Artificial Intelligence Act, in April 2021 [11]. The objectives of the framework were listed as to ensure AI systems used should comply with current laws and adhere to safety standards, establish legal clarity to promote investment and foster innovation in AI, focus on governance and enforcement of the existing laws and standards concerning AI and promote the creation of a unified market for lawful, safe, and reliable AI applications [12]. The primary emphasis is on enhancing regulations related to data quality, transparency, human oversight, and accountability to tackle ethical concerns and navigate implementation challenges across diverse sectors, including but not limited to healthcare, education, finance, and energy [11]. The Act has proposed a AI classification system where AI systems are categorized into four risk categories: unacceptable, high, limited and minimal/none with focus on unacceptable and high risk systems [13]. The Act was amended on June 14, 2023 and stands in negotiating position.

B. AI Bill of Rights

In October 2022, the Blueprint for AI Bill of Rights was released by the US White House Office of Science and Technology Policy (OSTP) which entails how government, technology firms, and citizens can collaborate to guarantee increased accountability in AI [14]. The Blueprint for an AI Bill of Rights comprises five principles and their corresponding practices. These are intended to provide guidance in the design, utilization, and implementation of automated systems, with the overarching goal of safeguarding the rights of the American public in the era of artificial intelligence [15]. The bill's principles include ensuring the safety and effectiveness of systems, preventing algorithmic discrimination and inequitable practices, safeguarding against abusive data practices and ensuring agency over the use of personal data, providing awareness of when automated systems are employed and understanding their impacts, and granting individuals the option to opt out of automated systems in favor of human alternatives.

C. Artificial Intelligence and Data Act

The Artificial Intelligence and Data Act was proposed in June 2022 by the federal government of Canada which if passed will be the inaugural AI legislation in Canada. It aims to collaborate with international allies, including the European Union (EU), the United Kingdom, and the United States (US), drawing inspiration from their practices and working collectively to synchronize approaches. The goal is to guarantee comprehensive protection for Canadians on a global scale and to establish Canadian businesses as internationally acknowledged entities adhering to high standards [16]. The objectives of the Act are to regulate trade and commerce of AI systems on an international and inter provincial level and prevent actions of AI systems that may cause substantial harm to individuals or their interests where harm is defined as (a) harm to an individual's physical or mental well-being, (b) impairment or destruction of an individual's property, or (c) financial detriment suffered by an individual.[17].

III. Comparative Analysis

Our methodology involves a comparative analysis of the regulatory frameworks put forth or enacted by the European Union (EU), the United States (US), and Canada. This analysis will be conducted across the following categories:

1) **Transparency and explainability:** This category focuses on informing individuals about the processing and utilization of their personal information.

TABLE I
COMPARATIVE ANAYLSIS FOR TRANSPARENCY AND EXPLAINABILITY

Sub-categories	Region		
	EU	***US***	***Canada***
Interpretability of Models	Ch.2 Art.13 outlines a categorization of AI systems based on three risk levels: unacceptable, high risk, and low to minimal risk. Each level is associated with specific requirements, with stringent regulations regarding interpretability applying exclusively to high-risk AI systems [12].	The Bill does not provide explicit provisions or requirements related to making AI models interpretable for the purpose of maintaining transparency [15].	The Act demands that there should sufficient information that will help the public understand the capabilities, restrictions, and consequences of the systems [16].
Explainable Algorithms	The Act does not explicitly differentiate between Interpretability and Explainability [12]. Considering the complexity of AI algorithms, we find the absence of clarification on explainability in the act is justified.	Notice and Explanation principle of the bill specifies that individuals understand how does the AI system work and how it influences the results that affect them and it also mentions that explanation must be documented, not necessarily in plain language but should allow the users to understand the purpose of using AI system [15]. But the Bill does not consider how the explanation can be provided for the self-learning part of the AI	The Act does not specify any obligations foe explainable highimpact AI [16].
Model Documentation	Ch.3 Art.11 and Art. 12 mention about technical documentation and record keeping for High-risk AI systems explicitly [12]. But do not correlate it with transparency.	Notice and Explanation principle of the bill The automated system must guarantee that publicly accessible and easily locatable documentation outlines the entire system, encompassing any human elements. This documentation should provide a clear explanation of the system's functioning and the role of any automated components in influencing actions or decisions [15].	The act does not provide clarity on how the model documentation should be done. While it outlines essential design and development requirements, it falls short in providing clear guidance on the practical implementation of these requirements [16].
Human-in-the-loop Systems	According to the Ch.3 Art.29, users' oversight is ensured through adherence to provided instructions, legal compliance, monitoring, reporting of issues, log keeping, and data protection impact assessments.Ch.2 Art.14 entitles how the providers can monitor the High-Risk AI throughout its life cycle [12].	Safe and Effective Systems principle focuses on considering public consultation on early-stage implementation of AI system. It also requires the entities to have appropriate governance structure and process to be in place before the deployment of the AI system [15].	The act mentions about the involvement of the organizations in the design and development of operations of the High Impact AI system but does not consider public insights [16].
Continuous Monitoring and Updating	Ch.1 Art.61 provides guidance on how the provider can monitor and update the High-Risk AI systems [12]. But do not correlate it with transparency.	Safe and Effective Systems principle states that the AI systems should be continuously monitored based on performance requirement, updates in the system while considering technical and human aspects of the system [15].	The act states that the AI systems must be monitored by conducting measurements and evaluations of the outcomes of high impact AI systems [16]. But it does not have guidance on how to monitor and update the functioning of the AI systems.

2) **Data protection:** This category refers to the specifics of data collection, including the type of data gathered, the purpose behind its collection, the duration for which it is retained, and the measures in place to ensure its protection.
3) **Automated decision-making, discrimination, and civil rights:** This category refers to determining the extent to which AI products are permitted to make automated decisions while safeguarding the civil rights of individuals and ensuring non-discrimination.

These categories can be further subdivided into relevant subcategories to facilitate a thorough comparative analysis. The subsections below outline the specific sub-categories employed for the comparison.

A. Transparency and Explainablity

Transparency: There are multiple aspects of transparency need to be considered [18]:

1) Disclosure of information should align with the significance of the exchange, with the impact of AI ap-

TABLE II
COMPARATIVE ANAYLSIS FOR DATA PROTECTION

Sub-categories	Region		
	EU	***US***	***Canada***
Data Minimization	The act does not specify any guidelines on data minimization. For EU, GDPR applies for the data protection concerning AI systems. But the EU AI Act does not link to GDPR [2].	Data privacy principle of the Bill states that the individuals are to be protected from the abusive data practices against privacy by limiting collection of data [15].	The act does not specify any guidelines on data minimization explicitly.
Privacy by Design and Default	The Act does not provide specific directives regarding data minimization. In the European Union, GDPR governs data protection in the context of AI systems. However, the EU AI Act does not establish a direct connection with GDPR [2].	Data privacy principle of the Bill states that automated systems should be designed and built with privacy protected by default [15].	The Act states that the companies must be aware of the risks of their AI systems but does not explicitly demand privacy by design in AI systems.
Data Subject Rights	The act does not specify any guidelines on data subject rights.	Data privacy principle mentions that individuals whose data is collected and used by automated systems can access the data and correct it if required. Individuals can also withdraw the consent leading to deletion of user data [15].	Bill C-27, especially AIDA, must include mechanisms that offer individuals avenues for recourse to safeguard fundamental rights when AI systems are employed. This includes granting individuals the right to oppose the automated processing of their personal data and the right to challenge decisions made through algorithmic systems[16].
Data Retention and Deletion	Ch.5 Art. 54 states that any personal data processed within the sandbox environment will be erased either when participation in the sandbox concludes or when the personal data's retention period comes to an end [12]. But it does not specify for high risk system.	Data Privacy principle states that establishing explicit timelines for data retention is essential, and data should be deleted as promptly as feasible, aligning with legal or policy constraints. These determined data retention periods need to be documented and justified [15].	The Act does not explicitly outline specific guidelines regarding data retention and deletion.
Data Breach Response	Ch.2 Art.62 states that high-risk AI system providers must report breach within 15 days [12].	Data privacy principle states that in case of sensitive data breach the description of the breach should be made public but does not specify the timeline for that [15].	The Act does not clearly specify detailed guidance on the data breach response.

plications influencing the feasibility and desirability of disclosure.

2) Transparency involves informing consumers about how an AI system is developed, trained, utilized, and adapted in specific domains, emphasizing relevant information and clarity.
3) Transparency also includes fostering public, multi-stakeholder discussions and, when necessary, establishing specialized organizations to enhance general understanding of AI systems and foster acceptance and confidence.

Explainability: Explainability in AI refers to the capacity of those affected by a system's decision to understand the factors, data, logic, or algorithm that influenced the outcome, whether it involves clarifying key decision-making elements, determinant factors, or why similar circumstances led to different outcomes, presented in a straightforward manner based on the context [18].

From the preceding explanation of transparency and explainability, we have identified the following subcategories:

- **Interpretability of Models:** Ensuring models are clear and transparent, allowing for a comprehensive understanding of how decisions are made.
- **Explainable Algorithms:** Utilizing algorithms designed for clarity, providing explicit and easily understandable reasons for their outputs.
- **Model Documentation:**Creating detailed records that outline the development, training, and evaluation processes of models to ensure reproducibility and facilitate collaboration.
- **Human-in-the-Loop Systems:** Integrating human expertise into the decision-making process of AI models to enhance decision quality and adaptability.
- **Continuous Monitoring and Updating:**Consistently assessing and updating models to maintain accuracy and relevance in dynamic real-world scenarios.

B. Data protection

This category addresses the types of data collected, the reasons behind their collection, the duration of retention,

TABLE III
COMPARATIVE ANAYLSIS FOR AUTOMATED DECISION-MAKING, DISCRIMINATION, AND CIVIL RIGHTS

Sub-categories	Region		
	EU	***US***	***Canada***
Explicit Consent	The Act does not specify that the entities should take explicit consent from individuals.	Human alternatives and Considerations and Fallback principle states that the individuals can opt out of the automated decision-making system [15].	The Act does not specify that the entities should take explicit consent from individuals
Diversity and Inclusion	The Act states that diverse community must be included in the data used by the High-risk AI system [12].	Algorithmic Discrimination Protections principle states that for the assessed group must be inclusive including individuals from all sectors of society, i.e. gender, sex, age, ethnicity, religion[15].	The Act addresses the issue of discrimination and points on inclusion of diverse community for assessment [16].
Human Oversight	Ch.2 Art.14 states that any action or decision based on the system's identification must undergo verification and confirmation by at least two individuals [12].	Human alternatives and Considerations and Fallback principle states that automated systems should be prohibited from directly intervening in high-risk scenarios, such as making sentencing decisions or providing medical care, without human deliberation [15].	The act does not mention guidelines for how the automated decisions from the high-impact AI systems are to handled [16].
Fairness and Bias Mitigation	The Act states the model to be tested at every stage for unbiased output [12].	Algorithmic Discrimination Protections principle states that data utilized in system development or assessment must accurately represent local communities in the intended deployment setting, undergo bias review based on historical and societal context, and be robust enough to identify and mitigate biases and potential harms [15].	The Act mandates implementation of measures to identify, assess, and mitigate potential harm or biased output risks before making a high-impact system available for use [16].
Periodic Audits and Assessments	Ch.3 Art.16 states that the High-risk AI system owners must perform periodic assessments for maintaining quality of the results [12].	Algorithmic Discrimination Protections principle states that the entities should perform ongoing monitoring for mitigation [15].	The act states that the High-impact AI systems must conduct assessments throughout the AI lifecycle [16].

and the protective measures in place. Data protection is the safeguarding process against unauthorized access. Central to data privacy is the empowerment of users to determine who has access to and utilizes their data [19].

From the preceding explanation of data protection, we have identified the following subcategories:

- **Data Minimization:** Restricting the collection and storage of personal data to the essential information required for the intended purpose, minimizing exposure risks by avoiding unnecessary data.
- **Privacy by Design and Default:** Integrating privacy considerations into the design and default settings of systems, ensuring that data protection is a fundamental aspect woven into the early stages of development.
- **Data Subject Rights:** Granting individuals control over their personal data through rights such as access, correction, and the right to be forgotten, promoting transparency and individual empowerment.
- **Data Retention and Deletion:** Setting guidelines for the appropriate duration of personal data retention and ensuring timely deletion when data is no longer needed, fostering responsible data management.
- **Data Breach Response:** Enacting a structured and prompt response plan to address data breaches, including notifying affected parties and relevant authorities, cultivating accountability and upholding trust.

C. Automated Decision-Making, Discrimination, and Civil Rights

This category outlines the scope of AI products engaging in automated decision-making while ensuring the preservation of each individual's civil rights inclusively.

Automated Decision-Making: The use of personal information in automated decision-making and AI systems raises significant concerns regarding the fairness, accuracy, and potential bias of AI algorithms, as well as the risk of discrimination. The progress of technology in social and economic realms is neither practical nor sustainable without the protection of rights [20].

Discrimination: AI systems possess the potential to maintain existing biases and disproportionately impact marginalized groups, including women, children, the elderly, individuals of color, and those with lower levels of education or skill. There is a specific risk of disparate impact in low- and middle-income nations. Cultivating public trust and understanding

of AI can be achieved through an inclusive, informed, and iterative public discourse involving all stakeholders [21].

Civil Rights: Some applications or uses of AI systems may affect human rights, leading to intentional or unintentional violations of values centered on people. Thus, AI systems should have the capacity for human supervision and intervention when necessary. This alignment ensures that AI systems operate in a manner upholding human rights, safeguarding them, and promoting them [22]. Upholding shared democratic ideals will support the application of AI to protect human rights, mitigate discrimination, and achieve just and equitable outcomes while fostering public confidence in the technology [23].

From the preceding explanation of automated decision-making, discrimination, and civil rights, we have identified the following subcategories:

- **Explicit Consent:** Obtaining clear and specific agreement from individuals before collecting and processing their personal data, ensuring transparency and user control in data handling.
- **Diversity and Inclusion:** Encouraging a varied and inclusive representation in data collection and model development to prevent biases and ensure equitable treatment across diverse demographics.
- **Human Oversight:** Introducing human judgment and supervision into AI systems for ongoing monitoring and intervention when necessary, acknowledging the limitations of automated decision-making.
- **Fairness and Bias Mitigation:** Implementing measures to identify and address biases in AI models, ensuring fair treatment and preventing discrimination based on sensitive attributes.
- **Periodic Audits and Assessments:** Conducting regular evaluations and audits of AI systems to assess performance, detect potential issues, and maintain continuous compliance with ethical standards.

IV. DISCUSSIONS

While comparing AI regulations in context of transparency and explainablity approaches as provided in TABLE I for the EU, the United States, and Canada, distinct patterns emerge. In the EU, AI systems are classified by risk levels, emphasizing interpretability for high-risk cases. However, there's no explicit differentiation between interpretability and explainability. Model documentation is stressed for high-risk AI in the EU, but a direct link to transparency is absent. Oversight for human-in-the-loop systems involves user adherence and legal compliance. On the other hand United States, the Bill lacks specific provisions for AI model interpretability, but the Notice and Explanation principle prioritizes documentation for user understanding. Public consultation and governance structures are key for human-in-the-loop systems.Finally in Canada, the legislation emphasizes providing information for public understanding of AI but lacks obligations for explainability. Design requirements are outlined, but practical model documentation guidance is lacking. Organizational involvement is acknowledged, but public insights are overlooked. Continuous monitoring is mandated, yet specific methods for updating AI systems are not provided.

When examining the strategies for data protection in three regions, as outlined in TABLE II, noticeable variations in frameworks become evident. In the EU, the AI Act lacks specificity on data minimization, relying on GDPR without a direct link and lacking explicit details on data subject rights. Discussions are prompted on the need for clearer guidelines on data minimization, defining data subject rights, and refining breach reporting, especially for high-risk AI systems. In the US, proposed data privacy principles prioritize individual protection, emphasizing limited data collection, privacy in automated systems, and defined timelines for data retention. However, the principle lacks a specific timeframe for publicly disclosing breach details. Whereas Canada, the act does not provide explicit guidance on data minimization, privacy by design, and data retention and deletion, raising discussions on these critical aspects of AI system regulation in the Canadian context.

Comparing on Automated Decision-Making, Discrimination, and Civil Rights as provided in TABLE III reveals distinctive approaches. In the EU, while explicit consent isn't mandated, a focus on diversity inclusion and human oversight ensures fairness through testing and periodic audits. The US emphasizes the right to opt out and prevents discrimination by ensuring inclusive representation, with strict human oversight and continuous fairness measures. In Canada, explicit consent isn't required, and the focus is on countering discrimination, promoting diversity, and mandating fairness measures with periodic audits throughout the AI system's lifecycle.

V. LIMITATIONS IN CANADA'S ARTIFICIAL INTELLIGENCE AND DATA ACT

The comprehensive comparison between the AI regulation frameworks between EU, USA and Canada led to finding gaps in the Canada's Artificial Intelligence and Data Act. The act lacks clear and sufficient guidance on transparency, explainability, and public engagement throughout the AI system lifecycle. It also falls short in providing guidelines for continuous monitoring, updates to address unexpected outputs, data protection measures like data minimization and privacy by design, as well as specifics on data retention and deletion for ensuring data security. Additionally, there is a lack of guidance on obtaining explicit consent for automated decision-making and handling the outcomes of such decisions.As per the federal government, the act is drawn from the frameworks built in EU, UK and USA.The act is one of its kind but still has a lot of room improvements. The framework can be designed considering the Canadian citizens and businesses.

VI. CONCLUSION

The research gives a clear idea that the AI Bill of Rights of USA stands out to be most comprehensive of the three. The EU's AI Act has a refined approach towards the classification of AI systems but as it is uncertain in some areas such interpretability and data protection, the act still be reinforced

before being approved. The objective of the research is to put forth the voids that the Artificial Intelligence and Data Act of Canada needs to fill and with the comparison performed has resulted in multiple domains.

REFERENCES

[1] Manyika, J., Chui, M., Brown, B. "Where machines could replace humans and where they can't (yet)" https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/where-machines-could-replace-humans-and-where-they-cant-yet

[2] European Union "General Data Protection Regulation (GDPR)" https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[3] United States Congress "Gramm-Leach-Bliley Act (GLBA)" https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act

[4] U.S. Department of Health Human Services "Health Insurance Portability and Accountability Act (HIPAA)" https://www.hhs.gov/hipaa/index.html

[5]] Office of the Privacy Commissioner of Canada "Personal Information Protection and Electronic Documents Act (PIPEDA)" https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

[6] Rutkoff, A. "Global Privacy Laws 2020: 1 Year After GDPR" https://trustarcblog.wpengine.com/

[7] Karl Manheim, Lyric Caplan "Artificial Intelligence: Risks to Privacy and Democracy," in 21 Yale J.L. Tech. (2019)

[8] Carole Cadwalladr, Emma Graham-Harrison "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach" https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[9] None of the Above UK, "Meet Cambridge Analytica: the Big Data communications company responsible for Trump Brexit" https://nota-uk.org/2017/02/02/meet-cambridge-analytica-the-big-data-communications-company-responsible-for-trump-brexit/

[10] Katharina Koerner "Privacy and Responsible AI" https://iapp.org/news/a/privacy-and-responsible-ai/

[11] Spencer Feingold "The European Union's Artificial Intelligence Act – explained" https://www.weforum.org/agenda/2023/06/european-union-ai-act-explained/

[12] European Comission "Laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts" https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex

[13] Mia Hoffmann "The EU AI Act: A Primer" https://cset.georgetown.edu/article/the-eu-ai-act-a-primer/

[14] Kay Firth-Butterfield, Karen Silverman, Benjamin Larsen "Understanding the US 'AI Bill of Rights' - and how it can help keep AI Accountable" https://www.weforum.org/agenda/2022/10/understanding-the-ai-bill-of-rights-protection

[15] The White House "Blueprint for an AI Bill of Rights- MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE" https://www.whitehouse.gov/ostp/ai-bill-of-rights/

[16] Government of Canada "The Artificial Intelligence and Data Act (AIDA) – Companion document" https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document

[17] Alycia Riley "Bill C-27: A deeper dive into Canada's proposed Artificial Intelligence and Data act" https://gowlingwlg.com/en/insights-resources/articles/2022/canada-s-artificial-intelligence-and-data-act/

[18] OECD.AI Policy Observatory "Transparency and explainability (Principle 1.3)" https://oecd.ai/en/dashboards/ai-principles/P7

[19] [3] GDPR.EU "A guide to GDPR data privacy requirements" https://gdpr.eu/data-privacy/: :text=Data

[20] Office of Privacy Commissioner Canada "A Regulatory Framework for AI: Recommendations for PIPEDA Reform" https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai

[21] OECD.AI Policy Observatory "Inclusive growth, sustainable development and well-being (Principle 1.1)" https://oecd.ai/en/dashboards/ai-principles/P5

[22] OECD.AI Policy Observatory "Human-centred values and fairness (Principle 1.2)" https://oecd.ai/en/dashboards/ai-principles/P6

[23] Information Commissioner's Office https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/what-about-fairness-bias-and-discrimination/