AI and Privacy Unveiled: Safeguarding Your Data in the Digital Era

Contents

What is AI

Artificial Intelligence is a system or technology designed to mimic certain human cognitive abilities, such as learning, problem-solving, reasoning, or even creativity abilities utilizing algorithms and data. AI enables machines to analyze information, recognize patters, and make decisions or predictions, often improving over time through experience (a concept known as "machine learning".

AI Models

1. **Generative AI**: AI systems that create new content, including text, images, and music, like ChatGPT or DALL·E.
2. **Expert Systems**: These are designed for decision-making within a specific domain by mimicking human expertise. For example, medical diagnosis systems.
3. **Robotics AI**: AI that is integrated into robots to perform tasks, whether in manufacturing, exploration (like Mars rovers), or personal assistance.
4. **Computer Vision**: AI focused on visual perception, enabling machines to interpret and process images or video data.
5. **Natural Language Processing (NLP)**: AI systems that interact with and analyze human language, like translation tools or sentiment analysis.

Large Language Models (LLM)

Large Language Models: are a type of AI specifically designed for understanding and generating human-like text. They are trained using vast amounts of text data and can handle tasks such as answering questions, writing essays, summarizing information, or even creative writing. LLMs, like GPT-4 are often a foundation for generative AI related to text-based outputs.

Common Features of Large AI Products

1. **Web Search**: Perform real-time web searches to provide up-to-date information and cite reliable sources.
2. **Image Understanding**: Analyze and describe images uploaded by users, helping to interpret visual content.
3. **Image Generation**: Create custom visuals based on descriptive prompts, enabling creative and illustrative projects.
4. **Context Management**: Keep track of conversation history within a single chat session, allowing for seamless and relevant discussions.
5. **Multilingual Proficiency**: Support a wide range of languages, adapting to the user's needs for communication.

Prominent AI Platforms

1. **OpenAI**: Known for its advanced models like ChatGPT and DALL-E, OpenAI focuses on generative AI for text and image creation.
2. **Google Cloud AI**: Offers tools like Vertex AI for building, deploying, and managing machine learning models, as well as natural language and vision APIs.
3. **Microsoft Azure AI**: Provides a suite of AI services, including Azure Machine Learning, Cognitive Services, and integrations with tools like Copilot.
4. **IBM Watson**: Specializes in enterprise AI solutions, including conversational AI, natural language processing, and data analytics.
5. **Amazon Web Services (AWS) AI**: Features services such as SageMaker for building, training, and deploying machine learning models at scale, as well as other machine learning and AI tools for text, speech, and vision processing.
6. **Hugging Face**: A popular platform for open-source AI models, particularly in natural language processing and machine learning.
7. **Anthropic**: Focuses on creating AI systems that are safe and aligned with human values, with offerings like Claude.
8. **Meta AI**: Known for its advancements in AI research and tools for natural language processing, computer vision, and more.

Privacy vs Security

Privacy focuses on the rights of individuals regarding their personal information, whereas security focuses on protecting data and systems from threats.

Privacy refers to the right of individuals to control their personal information and how it is collected, used, and shared.

- Examples of privacy protection: Data protection laws, privacy policies, user consent forms, anonymity.

Security refers to the measures and practices put in place to protect data, systems, and networks from unauthorized access, threats, and attacks. The goal of security is to maintain the confidentiality, integrity and availability of information, as well as confirm its authenticity and ensure non-repudiation.

- Examples of security measures: Firewalls, encryption, intrusion detection systems, antivirus software.

Security Without Privacy: It is possible to have security without privacy. For example, a company might implement robust security measures to protect its systems and data.

Privacy Without Security: Without security measures, personal information is vulnerable to breaches, making it difficult to ensure privacy.

In essence, while security and privacy are distinct concepts, they are closely related and often go hand in hand. Strong security measures are necessary to ensure privacy, and respecting privacy involves implementing adequate security controls.

Privacy – Classifications and Roles

Personal Information Data Classifications

PII (Personally Identifiable Information)

Personally Identified Information refers to information which can be used to identify a specific individual, either directly or indirectly. PII data includes:

- Names
- Addresses
- Email addresses
- Telephone numbers
- Dates of birth
- Social Security / Social Insurance numbers
- Internet browsing history
- Biometric data

NPI (Nonpublic Personal Information)

NPI refers to any information provided by an individual to obtain financial products or services. Examples of NPI data include:

- Name
- Address
- Social Security / Social Insurance numbers
- Income information
- Account numbers
- Payment History

PII is broader in scope and includes any information that can identify an individual while NPI is a subset of PII specifically related to financial products and services. NPI data is often regulated under specific financial privacy laws, such as the Gramm-Leach-Bliley Act (GLBA), where as PII is regulated under various country, federal or state privacy laws.

PHI (Private Health Information)

Private Health Information covers individually identifiable health records which are governed under HIPAA in the US, and in Canada under the PIPEDA (Personal Information Protection and Electronic Documents Act which is a larger document in scope covering NPI, PII, and PHI data. Additionally, some provinces such as Ontario have additional privacy laws. Ontario has legislation under the PHIPA (Personal Health Information Protection Act) which specifically governs the collection, use,

and disclosure of personal health information by healthcare providers and other organizations involved in healthcare services.

Understanding Privacy Terminology

Privacy policies associated with a company's products often rely on standard terms. For end-users, it's essential to understand these terms to make informed decisions when reviewing such policies. Below are some key roles and concepts in data management:

Data Management Roles:

- **Data Subject**: the individual whose personal data is being collected, held or processed
- **Data Controller**: an entity that determines the purposes and means of processing personal data and makes decisions regarding the types of data collected, why it's collected and how it will be processed (EG: business, government agencies)
- **Data Processor**: an entity that processes data on behalf of the controller, including the storing, modifying, retrieving, or erasing of data (EG: Cloud service providers, payroll companies)
- **Data Recipient**: an entity to whom personal data is disclosed (EG business partners, third-party service providers)
- **Data Subject Rights**: The rights granted to data subjects under data protection laws (EG: rights to be informed, right to access, right to rectification, right to erasure)

Privacy Legislation - Overview

Numerous laws and regulations have been enacted across various levels of government within different countries. Below are the most notable examples, with further details and additional legislation outlined later in this document.

European Union – GDPR (General Data Protection Regulation)

Canada – PIPEDA (Personal Information Protection and Electronic Document Act)

United States – The United States has federal regulations concerning privacy, though they are generally less comprehensive than the GDPR and often focused on specific sectors or types of data.

Privacy Concerns

Large language models (LLMs)have revolutionized AI, but they come with significant privacy concerns. Here are some of the key issues:

1. **Data Collection Without Consent**: LLMs are trained on vast datasets, which may include sensitive or personal information collected without explicit user consent.

2. **Data Leakage**: These models can inadvertently reveal sensitive information from their training data, such as private conversations, personal identifiers, or proprietary content.
3. **Membership Inference Attacks**: Adversaries can determine whether specific data points were part of the training set, potentially exposing private information.
4. **Model Inversion Attacks**: Attackers can reconstruct sensitive data by exploiting the model's outputs, effectively reversing the training process.
5. **Unchecked Surveillance**: The use of LLMs in applications like facial recognition or predictive policing raises concerns about mass surveillance and potential misuse.
6. **Bias and Discrimination**: Training data often contains biases, which can lead to discriminatory outputs, impacting privacy and fairness.
7. **Compliance Challenges**: Organizations using LLMs must navigate complex privacy regulations, such as GDPR or CCPA, which can be challenging given the opaque nature of these models.

Protecting Your Privacy

It is the responsibility of the service provider or organization to safeguard your privacy in accordance with their privacy policies and to implement the necessary security measures, however there are also steps you, can take to actively protect your personal information."

Safeguarding Your Privacy – Practical Steps and Behaviour

1. **Understand Privacy Policies**:
    - Read and understand the privacy policy of the AI platform to understand how your data is collected, stored and used.
2. **Be Mindful of What you Share:**
    - Avoid providing sensitive personal, financial, or confidential information, such as social insurance numbers, passwords, or detailed identifying details.
    - If you must utilize this information within an AI system (e.g. within a corporate AI system) ensure you are authorized under the organizations policies and practices and if possible employ pseudonymization or anonymization.
    - **Pseudonymization** – replace personally identifiable names with pseudonyms
        1. Unlike anonymization can allow re-identification under certain conditions.
    - **Anonymization**
        1. Data masking – replace sensitive data with random characters or symbols.

2. Generalization – reduce precision such as replacing an exact age with an age range.

3. Data Swapping – move data attributes to break the link between identifiers and individuals (e.g. within a data set move certain values to help protect identity. For example, if a table has names, addresses, and age, you can manipulate the age category, for the purpose of still using the name and address, but now the age column is invalid).

4. Perturbation – adding noise or slight modifications to data values to obscure identities. (e.g. modifying values while still maintaining trending and statistical information. Adjusting salaries of 50K and 60K to 51,200 and 59599.)

3. **Leverage Privacy Features**:

- Use privacy settings or tools offered by the AI platform, such as disabling chat history or using private / incognito mode if available.
- Clear your conversation history regularly if the platform retains logs of your interactions.
- Look for options to opt out of data retention or sharing, if available.
- Ensure the platform uses HTTPS to protect your data during communication.

4. **Use Secure Networks**:

- Access the platform over a secure network (e.g. avoid public Wi-Fi unless using a VPN).
- Employ a Virtual Private Network (VPN) to encrypt your internet connection which provides the following benefits:

    1. Hides your IP Address: A VPN masks your real IP address. Your IP address can reveal your general location and other identifiable details.

    2. Protects Data During Transmission: If accessing AI tools over public Wi-Fi or unsecured networks, a VPN will encrypt the traffic.

    3. Mitigate ISP Tracking: Without a VPN, your Internet Service Provider (ISP) might log your interaction with AI services. Utilizing a VPN encrypts your activity ensuring that the ISP cannot see the content of transmissions.

    4. Adds an Extra Privacy Layer: Even if the AI platform collects information about your interactions using a VPN makes it more difficult to tie this information back to your identity and location.

    5. NOTE: While VPNs can enhance your privacy, they aren't a foolproof solution. They don't prevent AI tools from collecting and processing data

you directly provide, so combining a VPN with mindful data-sharing practices is key!

5. **Limit Device Access**
    - Consider utilizing browsers which have a focus on privacy such as FireFox or Brave.
    - Use incognito or private browsing mode to prevent browser caching of your activity.
    - Regularly clear your browser's cookies, cache, and saved data to reduce potential tracking.
    - Consider using browser extensions which which block trackers and intrusive ads which may collect data such as Privacy Badger, or uBlock Origin.
6. **Use Anonymous Accounts**: When possible, interact with AI systems using accounts that do not link back to your personal identity. (e.g. don't use firstname.lastname@gmail as your login to the AI system.) Note: in the cases of enterprise AI systems such as Copilot for business you will be reliant on your legitimate email address, but these corporate systems often offer additional protections and controls that are managed by your organizations administration team.
7. **Be Cautious with Uploaded Content**: When uploading files or images, ensure they don't contain private or identifiable data unless necessary. Example:
    - **Text** – is there visible text such as signs, screens, or papers in the image that might reveal location, address, or other private information.
    - **Metadata** – often overlooked, image files can contain metadata such as GPS coordinates, timestamps, and device information which could expose the location, identity or other private information.
    - **Unique Patterns** – Distinctive tattoos, clothing, accessories, or even background details might link the image to an individual.
    - **Environment** – Home interiors, landmarks, or workspaces can provide contextual clues about someone's identity or location.
    - **Faces** – Photos of people, even in crowds, can expose identity through facial recognition technology.
        1. Tips to safeguard privacy when uploading images
            1. Blur or Crop: Remove obscure sensitive parts of the image before uploading
            2. Check Metadata: Strip the image metadata using photo editing tools or online services
            3. Use Anonymization Tools: Certain tools can blur faces and identifying features automatically.

8. **Voice Recording Options**: For voice-enabled AI, ensure that recordings are not stored or shared if privacy settings allow customization, consider if you should record at all, and if recording a meeting, notify participants that the sessions is being recorded.
9. **Avoid using Confidential Information**: If discussing sensitive or confidential matters, consider whether that information should even be shared with an AI platform. (alternatively obscure this information through pseudonymization and anonymization if necessary)
10. **Advocate for Transparency**: Push for greater transparency from AI developers about how they handle and protect user data.
11. **Stay Updated**: Keep yourself informed about evolving privacy standards and AI capabilities to recognize potential risks early.

Each interaction with AI presents unique considerations, so developing a mindful and cautious approach is key.

Organizational Data Governance

Data governance roles are part of a data governance framework employed by organizations to guarantee that data is consistent, trustworthy, and not misused. A data governance program usually includes a governance team, a steering body, and a group of data stewards responsible for developing data governance standards and policies.

There are multiple resources and documents that outline various data governance frameworks. It should be noted that as these are frameworks, many organizations will develop their own framework or adapt existing frameworks to meet their specific needs. A few of the well-known frameworks are as follows:

- Atlan's Guide to Data Governance Frameworks
- Twillio Segment's Data Governance Framework
- The Data Governance Document Example

Data Governance Roles

Most data governance frameworks include the following roles to assign responsibilities for the governance of data within an organization.

1) Data Owner – responsible for data in a certain data domain. The data owner must guarantee that the information inside the domain is correctly maintained across various platforms and business processes. Data owners are frequently represented on the executive committee as voting members or attending members with no voting powers. The following are there specific responsibilities:
    - Approving data glossaries and definitions
    - Ensuring accuracy of the information
    - Supervision of operations related to data quality

    - Provide feedback within the organization regarding software solutions, policy, or regulatory requirements that may impact the data owner's data domain.
2) Data Stewards – are in charge of managing the quality of defined datasets on a daily basis, being the SME (subject matter expert) who understands the importance of the information and it's use. Typically the data steward represents the data owner. Additional responsibilities of the data steward includes
    - Creating data definitions and describing allowed values
    - Definition of rules for data generation and data usage
    - Documenting the current and desired data systems
    - Establishing data quality objectives
3) Data Custodian – responsible for the safe custody, transport, storage, and management of data. The role is focused on the technical aspects of data management including:
    - Data Storage and Backup
    - Data Security – Implement security measures to project data from unauthorized access, breaches, and threats
    - Access Control – control and limit access, and the ability to modify data to only authorized individuals
    - Data Integrity – maintain accuracy, completeness, and reliability of the data
    - Compliance – Ensure data handling practices comply with relevant laws, regulations, and organizational policies
    - Technical Support – provide technical support for data-related issues and assisting in data recovery processes.

Privacy Principles and Legislation

Generally Accepted Privacy Principles (GAPP)

GAPP is a framework that consists of 10 components to help organizations maintain data privacy and was developed collaboratively by:

- American Institute of Certified Public Accountants (AICPA)
- Canadian Institute of Charted Accountants (CICA)
- Information Systems Audit and Control Association (ISACA)
- Institute of Internal Auditors (IIA)

While GAPP is a principle and does not have legal authority, it provides guidelines for organizations to proactively manage privacy and is often used alongside legal requirements to strengthen compliance efforts.

The 10 components of GAPP include:

1) **Management** – Organizations handling private information should have policies, procedures, and governance structures in place to protect privacy. The organization must clearly define the roles of data owner, data steward, and data custodian.

2) **Notice** – Data subjects should receive notice that their information is being used and collected, as well being provided with access to the privacy policies and procedures followed by the organization
3) **Choice and Consent** – inform data subjects of their options regarding the data they own and obtain consent from those individuals for the collection, storage, use, and sharing of that information.
4) **Collection** – the organization should only collect personal information for the purposes disclosed in their privacy notices.
5) **Use, Retention, and Disposal** – only collect and use personal information for disclosed purposes and dispose of the data securely when it is no longer required for the disclosed purpose.
6) **Access** – data subjects should have the ability to review and update their personal information.
7) **Disclosure to Third Parties** – organizations should only share information with third parties if that sharing is consistent with the purposes disclosed in privacy notices and they have the consent of the individual to share that information
8) **Security** – must secure private information against unauthorized access, either physically or logically
9) **Quality** – take reasonable steps to ensure that private information they maintain is accurate, complete, and relevant.
10) **Monitoring and Enforcement** – the organization should have a program in place to monitor compliance with its privacy policies and provide a dispute resolution mechanism.

Privacy Regulations/Legislation

As mentioned previously, legislation and regulations pertaining to privacy are often unique by country, or by state and province, and even municipalities.

Canada

Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA is a Canadian **federal** privacy law that defines how private sector organizations collect, use and disclose personal information during commercial activities. The document is published on the Office of the Privacy Commissioner of Canada Website.

PIPEDA implements ten fair information principles to protect personal information. In many of the privacy regulations and legislation there is an overlap with the GAPP framework. The ten principles are:

1) **Accountability**: Organizations must appoint someone to be responsible for compliance with PIPEDA, typically the Privacy Officer, or the Data Protection Officer (DPO).
2) **Identifying Purposes**: Organizations must identify the purposes for which personal information is collected at or before the time of collection.

3) **Consent**: Organizations are required to obtain an individual's consent when collecting, using, or disclosing personal information.
4) **Limiting Collection**: Organizations must limit the collection of personal information to that which is necessary for the identified purposes.
5) **Limiting Use, Disclosure, and Retention**: Organizations must not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information must be retained only as long as necessary for the fulfillment of those purposes.
6) **Accuracy**: Personal information must be as accurate, complete, and up to date as necessary for the purposes for which it is to be used.
7) **Safeguards**: Organizations must protect personal information with appropriate security safeguards.
8) **Openness**: Organizations must make their policies and practices relating to the management of personal information readily available to individuals.
9) **Individual Access**: Upon request, individuals must be informed of the existence, use, and disclosure of their personal information and be given access to that information. Individuals must be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10) **Challenging Compliance**: Individuals must be able to challenge an organization's compliance with the above principles.

PIPEDA applies to:

- Private-Sector Organizations (businesses etc.)
- Federally Regulated Organizations (banks, telecommunications companies etc.)

PIPEDA does not apply to:

- Organizations in provinces that have their own private-sector privacy laws that are deemed substantially similar to PIPEDA are generally exempt from PIPEDA with respect to the collection, use, or disclosure of personal information within that province. This currently includes Alberta, British Columbia, and Quebec.
    - NOTE PIPEDA applies to PII data that crosses provincial or national borders, regardless of the province or territory in which the organization is based.
- Public Sector Organizations. Federal, provincial, and municipal governments, as well as their agencies and departments are not covered by PIPEDA. These organizations are subject to different privacy laws, such as the Privacy Act at the federal level.
- Non-Commercial Activities: PIPEDA does not apply to information collected, used, or disclosed for non-commercial activities, such as personal information collected by individuals for personal, domestic, or recreational purposes
- Journalistic, Artistic, and Literary Purposes: PII collected used or disclosed for journalistic, artistic, or literary purposes is exempt from PIPEDA

Ontario Privacy Regulations

The province of Ontario has its own privacy legislation separate from PIPEDA, however these laws work along side PIPEDA to provide comprehensive privacy protection in Ontario: For more details you can visit the Ontario Government's website.

Ontario has three privacy legislations separate from PIPEDA:

- Personal Health Information Protection Act (PHIPA)
    - Governs the collection, use, and disclosure of personal health information (PHI) by healthcare providers and other organizations involved in healthcare services. This applies to public-sector organizations (hospitals), private businesses (pharmacies, long-term care homes), and healthcare professionals (doctors)
- Freedom of Information and Protection of Privacy Act (FIPPA)
    - Applies to provincial government institutions, including ministries, agencies, boards, and commissions. This Act ensures the protection of personal information held by these institutions and provides individuals with the right to access information.
- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
    - Applies to municipal institutions, including municipalities, school boards, and police services. Like the FIPPA it ensures the protection of personal information and provides access rights to individuals.

European Union

GDPR (General Data Protection Regulation)

GDPR is one of the best-known privacy regulations. It came into effect in 2018 unifying privacy regulations and enabling data exchange. This regulation protects all personal data in the EU and applies to anyone physically located in the EU, not just its citizens. It covers any information which can identify an individual, from name and birth date to geolocation information.

GDPR provides the following rights for Data Subjects:

- Transparency: Clear notice of data collection and usage.
- Consent: Obtaining meaningful consent for data collection.
- Right to be Forgotten: Data erasure upon request.
- Right of Access: Knowing what data is collected, processed, shared.
- Right to Rectification: Request corrections to collected data.
- Restriction of Processing: Request to halt data processing activities.
- Data Portability: Right to obtain data in machine-readable format.
- Objection: Right to object to non-compliant data processing.
- Automated Decision-Making: Right to opt-out of decisions made solely by AI or automated processing.

In addition, GDPR stipulates requirements for the transfer of data

- Within the EU: Allowed
- Outside EU: requires one of the following

- Standard contractual clauses
- Binding Corporate Rules
- Privacy Shield (safe Harbor Agreements) – although this is no longer valid as of a 2020 ruling by the European Court of Justice, it may be implemented in the process is modified to be acceptable under the current GDPR.

United States of America

The U.S. does not have a single, comprehensive privacy law such as the PIPEDA in Canada, or the GDPR in Europe, instead it is a patchwork of sector-specific federal and state-level regulations. The following are a few of the key federal privacy laws:

Privacy Act of 1974 (Office of Privacy and Civil Liberties)

- Governs the collection, use, and dissemination of personal information by federal agencies.
- Provides individuals with rights to access and amend their records held by federal agencies.

Health Insurance Portability and Accountability Act (HIPAA) (US Department of Health)

- Protects the privacy and security of health-related information.

Children's Online Privacy Protection Act (COPPA) (Federal Trade Commission)

- Regulates the collection of personal information from children under 13 by online services and websites

Gramm-Leach-Bilely Act (GLBA) (Federal Trade Commission)

- Focuses on safeguarding financial information and requires financial institutions to explain their information-sharing practices.

U.S. State Law

The state of California has some of the most comprehensive privacy laws in the United States. Here are the key ones:

- California Consumer Privacy Act (CCPA)
- California Privacy Rights Act (CPRA)
- Online Privacy Protection Act (CalOPPA)