General Assembly 6: Legal

The Issue of Privacy Implications in AI Systems

Head Chair: Navya Bhambi

Deputy Chair: Cindy Dai

Assistant Chair: Rosabel Song

NORTHBRIDGE INTERNATIONAL SCHOOL
CAMBODIA
A NORD ANGLIA EDUCATION SCHOOL
WELCOME

Nord Anglia SEAME&I REGIONAL
Model United Nations 2024

Contents

Introduction

Artificial intelligence (AI) technologies have advanced and become more integrated into various aspects of society throughout the past years. It is known to make advancements in many industries of the world such as healthcare, finance, manufacturing, social media, etc. Most AI systems focus on creating machines capable of performing tasks that typically require human involvement. These systems can analyze large amounts of data, recognize patterns, make predictions, and learn from experience, all without the intervention of humans, which enables them to perform complex tasks with immense speed and accuracy.

However, the issue of privacy implications in AI systems has become a significant concern as AI continues to expand and develop. There is a growing awareness of the potential risks they pose to individual privacy, such as profiling and discrimination, consent, data breaches, surveillance and tracking, re-identification, and other ways in which privacy can be compromised. The primary privacy concern with AI systems is the potential for unauthorized access, use, or disclosure of personal data and the mix of AI and privacy has become a critical focal point, sparking debates and ethical considerations.

Definition of Key Terms

Data Privacy

Protection of individuals' personal information and the right to control the collection, usage, and sharing of their data.

Algorithmic Bias

The systematic and unfair discrimination in AI algorithm outcomes, which is typically caused by biases in the training data.

Machine Learning

A computer science technique that focuses on the use of data and algorithms to replicate the way that humans learn, eventually improving its accuracy.

De-identification

Removal of personally identifiable information from databases to protect the confidentiality and privacy of individuals.

Re-identification

The opposite of the de-identification process, which allows the identification of individuals using their data given from datasets that are allegedly anonymous or de-identified.

Informed Consent

Gaining individual's clear and informed consent before acquiring, using, or processing their personal information or data for AI purposes.

Transparency

Enhancing disclosure practices by utilizing procedures and data analytics to guarantee complete user protection.

Consent Management

Systems and processes that facilitate the obtaining, recording, and management of individuals' consent for data processing, particularly in the context of AI systems.

Security Risks

Potential flaws in AI systems that could be used to obtain unauthorized access and breach confidentiality and privacy.

Cross-Border Data Flow

The movement of data across national borders presents difficulties for complying with various privacy laws and standards in different jurisdictions.

Ethical Use of AI

Respecting individual's right to privacy and minimizing potential harms by developing AI systems in accordance with ethical principles and guidelines.

Accountability

The responsibility of organizations as well as individuals for the consequences of AI systems' activities.

Explainable AI (XAI)

This term refers to the capability of an AI system to provide understandable explanations for its decisions and actions. Since the inner workings and decision processes can often be complex or difficult for humans to understand, XAI aims to help this by making AI systems more transparent and interpretable.

Background Information

At the emergence of personal computing, privacy concerns focused on securing physical access to personal computers, but online privacy discussions began with the further development of the internet and following concerns regarding data transfer and storage. At the rise of the internet, increased data sharing and storage brought about by e-commerce and online services gave way to discussions concerning the handling and sharing of personal information as more and more people start to use the internet. In the 2000's, AI underwent a change with the introduction of big data and machine learning technologies. Privacy concerns continued to expand as organizations started collecting and analyzing huge amounts of data to train AI algorithms. With the rise of social media platforms in the 2010's, AI algorithms began to leverage user data for targeted advertising and content recommendations. As time moved on, algorithmic bias and discriminatory outcomes in AI systems have brought attention to issues with privacy, particularly in fields like hiring, finance, and criminal justice. Responsible development and ethical AI are becoming more popular topics of conversation, and researchers and organizations started emphasizing the need to ensure transparency, reduce bias, and build privacy-by-design into AI systems.

Current Situation

At the moment, there is a lot of focus and worry concerning the relationship between AI and privacy. With the development of AI technology and its increasing integration into other areas of society, many significant privacy concerns have emerged over the past 10 years. These concerns include increased regulatory scrutiny, AI in surveillance and security, algorithmic bias and fairness, ethical AI frameworks, and corporate responsibility.

Due to bad management of the issue, the Equifax, one of the credit reporting agencies that assesses the financial health of nearly everyone in the United States, exposed sensitive personal information of millions of individuals back in 2017. This data breach was one of the largest in history. The Equifax breach investigation highlighted several security lapses that allowed attackers to enter supposedly secure systems and exfiltrate terabytes of data. This incident demonstrated the potential consequences of lax cybersecurity measures in handling vast amounts of financial and personal data, leading to identity theft and financial fraud concerns. 143 million people, more than 40 percent of the population of the United States, were affected, with their names, addresses, dates of birth, social security numbers, and drivers' licenses numbers all exposed to the public.

Major Parties Involved

Technology Companies

Major technology companies like Google, Microsoft, Amazon, and Facebook are leading the way in AI development. They create AI algorithms and implement AI-driven applications and in some cases, they face scrutiny over how they handle user data and ensure privacy in AI applications. These companies all face a similar challenge: how to achieve a balance between the need to safeguard user privacy and the offering of individualized services, which requires substantial data collecting. These companies must negotiate a challenging regulatory environment as privacy laws worldwide, such as the GDPR, are constantly changing. They must modify their business processes to comply with various legal frameworks.

Finance and Banking Systems

AI is being used by financial institutions like PayPal, JPMorgan Chase, and Bank of America for customer service, fraud detection, and credit scoring. Concerns about privacy have grown in relation to handling sensitive financial data in an ethical and secure way. Regarding credit scoring in particular, these institutions have difficulties ensuring that AI algorithms are unbiased and equitable.

European Union (EU)

The EU has been at the forefront of privacy regulations with the implementation of the General Data Protection Regulation (GDPR) in 2018. GDPR sets strict guidelines for the processing and protection of personal data, emphasizing user consent, transparency, and individual rights. GDPR requires that before collecting and using personal data, organizations must get explicit and informed consent. This consent needs to be freely given, specific and amendable whenever needed. The rule places a strong emphasis on transparency, enforcing companies to give explicit information regarding data processing processes, the reason for collecting data, and the duration of data preservation.

United States

The U.S. has been struggling with AI-related privacy issues, with debates intensifying around the need for federal privacy legislation. The absence of a unified federal privacy framework has led states to take matters into their own hands, with the Consumer Privacy Act (CCPA) in California and other state-level programs setting forward to increase efforts being made to improve user rights and data protection. Without comprehensive federal privacy laws, AI has the power to give organizations and governments more ability to monitor, track, and profile US consumers and internet users. These profiles might then be utilized to influence behavior in ways that are hard to resist or even notice.

China

The rapid adoption and usage of AI technologies in China have been accompanied by a set of considerations, particularly in relation to privacy. The Chinese government's initiatives, such as the social credit system, have raised significant concerns globally regarding the potential impact on individuals' privacy rights. The Social Credit System was designed to assess and score individual's and businesses' financial and social behavior. It uses AI and data analytics to assess a range of factors, such as online conduct, interactions, and financial transactions. The system has generated discussions concerning the invasive nature of surveillance and the possible erosion of privacy, even though it has been presented as a tool to increase trust and integrity.

Canada

Canada has taken steps to address privacy challenges in terms of AI. The Personal Information Protection and Electronic Documents Act (PIPEDA) regulates the use of personal information, and discussions around AI's impact on privacy are ongoing.

United Kingdom (UK)

While GDPR standards still apply post-Brexit, the UK is exploring additional measures to regulate the use of AI, including the exploring of development of its own regulatory framework. This framework aims to address specific challenges posed by AI technologies, including algorithmic transparency, accountability for AI driven decisions, and the protection of individual privacy rights.

Australia

Australia is actively considering and implementing policies to address AI related privacy issues. Discussions include the development of a national AI ethics framework and amendments to existing privacy laws to accommodate the challenges posed by AI technologies. The use of AI in Australia is governed by existing legislation. For example, the Privacy Act 1988 (Cth) (the Act) applies in relation to any collection of personal information.

Timeline of Relevant Events

Date	**Description**
June 2013	**Edward Snowden Revelations** Edward Snowden's disclosures on nation leaders reveal secret, extensive government surveillance programs, sparking a significant global debate on privacy and data collection.

25 May 2018	**General Data Protection Regulation (GDPR) Implementation** The GDPR comes into effect in the European Union, setting strict standards for data protection and privacy, as the GDPR aimed to empower individuals and enhance their control over their personal data in the digital age. The GDPR granted individuals rights over their personal data, including the right to access and erase their information. It also introduced the right to data portability, allowing individuals to transfer their data between service providers. These regulations established a standard for ethical data processing and impacted future privacy laws in other jurisdictions. Globally, businesses continue to navigate the complexities of compliance, and the GDPR continues to be referenced when talking about responsible and legal uses of personal data in the digital age.
March 2018	**Cambridge Analytica Scandal** Revelations emerged about the misuse of Facebook user data by the political consulting firm Cambridge Analytica. The scandal brought to light how personal information from millions of Facebook profiles were being harvested without explicit user consent and subsequently used for targeted political advertising during the 2016 U.S. presidential election.
2019	**Facial Recognition Scrutiny** Facial recognition technology, powered by AI, gained widespread adoption in various sectors, including law enforcement, retail, and public spaces. While praised for its potential benefits in security and convenience, the increased deployment of facial recognition systems raised significant concerns about privacy, surveillance, and potential misuse. Critics argued that widespread use without proper regulations could result in a surveillance state, where individuals' movements and activities are continuously monitored without their knowledge or consent.
2020	**AI Ethics and Accountability Gaining Traction** A heightened focus on the ethical use of AI in healthcare was noticed this year. As AI technologies played a crucial role in addressing healthcare challenges, concerns emerged regarding patient privacy, bias in medical algorithms, and the need for transparent decision-making processes.

2020	The global COVID-19 pandemic prompted the deployment of AI driven contact tracing and surveillance systems. Ethical questions arose about the balance between public health needs and individual privacy rights. Governments and tech companies faced challenges in ensuring these technologies were deployed responsibly and with due regard for privacy concerns.
1 November 2021	**Personal Information Protection Law (PIPL) Implementation in China** This implementation represents a significant step towards enhancing personal information protection and data governance. It reflects a broader global trend of strengthening data protection regulations and underscores the importance of responsible and transparent data practices. The PIPL complements existing laws such as the Cybersecurity Law (CSL) and the Data Security Law (DSL), creating a comprehensive legal framework for the protection of personal information.

Related UN Treaties and Events

- **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108):** Started in 1981, this Council of Europe treaty focuses on the protection of individuals concerning the automatic processing of personal data. It has influenced data protection legislation globally and is relevant to AI systems that involve processing personal data.

- **General Data Protection Regulation (GDPR):** It is a comprehensive regulation enacted by the European Union. It sets high standards for personal data protection and has significantly impacted global discussions around data privacy. Its principles are applicable to AI systems that involve the processing of personal data.

- **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data:** The OECD has guidelines that include principles for the protection of privacy and the transborder flow of personal data.

- **The Internet Governance Forum (IGF):** The IGF is a global multi-stakeholder platform that facilitates discussions on public policy issues related to the Internet. Privacy and data protection, including those related to AI, are recurrent themes in these discussions.

- **United Nations Open-Ended Working Group on Artificial Intelligence:** The UN has established an Open-Ended Working Group on Artificial Intelligence in 2021, aiming to discuss and formulate recommendations on issues related to the governance of AI, which may include considerations of privacy and human rights.

Previous Attempts

Many nations around the world have tried to resolve this issue in the past as they have recognized the importance of addressing privacy issues associated with AI and have made these attempts to regulate and safeguard individual privacy. Some of these attempts have ended with successful results, others not. South Korea has enacted the Personal Information Protection Act (PIPA) in February of 2023 to regulate the processing of personal information. The law includes provisions for user consent, data breach notification, and the appointment of data protection officers. South Korea has been actively updating its privacy laws to address emerging challenges, including those posed by AI. South Korea's commitment to updating its privacy laws and addressing the challenges posed by AI demonstrates a forward-thinking approach to data protection for other nations. As the country continues to navigate the evolving digital landscape, its initiatives contribute to the global discourse on privacy, ensuring that individuals' rights are respected.

With South Korea being an example of a successful attempt to resolve the issue, there are also many failed attempts. For example, India’s Draft Personal Data Protection Bill (PDPB), its most recent draft of the bill released in late 2022, faced a lot of criticism for certain reasons, including those related to government surveillance powers and data localization requirements. Critics argue that these elements may compromise user privacy and hinder the free flow of data.

Possible Solutions

Addressing privacy issues associated with AI requires a complicated approach involving technological, legal, and ethical considerations. One of the biggest reasons why an individual's privacy is being invaded is because of lack of transparency from big organizations, such as technology companies, social media platforms and government surveillance programs. They must ensure that AI systems are designed to be transparent and explainable, and users should have access to understandable explanations of how algorithms make decisions. This can empower individuals to understand and trust the technology they use. Organizations should implement techniques for Explainable AI (XAI) that provide insights into the decision-making process of AI systems. It must be mandatory that they clearly communicate to users what impact AI decisions may have on them.

Furthermore, websites should empower users with clear information about how their data will be used, and give them control over their data, including the ability to agree or disagree to certain data processing activities. Users should be able know where their data is going and how it will be handled after its purpose. This way, individuals who agree for organizations to collect data can trust and feel safe with it, and once they don't, they can immediately opt-out for a data processing choice.

Suggested Reading

- Ferm, Lars-Erik Casper, et al. "AI and Its Implications for Data Privacy." *Www.routledge.com*, 30 Aug. 2023, **www.routledge.com/blog/article/ai-and-its-implications-for-data-privacy**.

This article discusses the implications of AI and its impact on data privacy, as well as how AI uses the data and possible solutions to this issue.

- OVIC. "Artificial Intelligence and Privacy - Issues and Challenges." *Office of the Victorian Information Commissioner*, ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/#discrimination.

This reading covers and explains the challenges and issues related to artificial intelligence and privacy in organizations, and many considerations and factors within the implications of privacy.

- van rijmenam, mark. “Privacy in the Age of AI: Risks, Challenges and Solutions.” *Dr Mark van Rijmenam, CSP - the Digital Speaker | Strategic Futurist*, 17 Feb. 2023, www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/.

The digital speaker in this article discusses the risks and challenges associated with privacy age AI, offering solutions to address these issues.

- MacAskill, Ewen, et al. “NSA Files Decoded: Edward Snowden’s Surveillance Revelations Explained.” *The Guardian*, The Guardian, 1 Nov. 2013, www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

The Guardian has decoded surveillance reports from Snowden's National Security Agency files and linked them to many national leaders around the world, explained with text and pictures.

- Local Government Association. *The General Data Protection Regulation (GDPR) Guidance for Members*. 2018.

This document provides guidance for members on the General Protection Data Regulation (GDPR) and its corresponding regulations.

- Satter, Raphael, et al. “US, Britain, Other Countries Ink Agreement to Make AI “Secure by Design.”” *Reuters*, 27 Nov. 2023, www.reuters.com/technology/us-britain-other-countries-ink-agreement-make-ai-secure-by-design-2023-11-27/.

This article explains how the US, Britain, and other countries have signed an agreement to make AI secure by design and how they will make it happen with low risks.

Bibliography

Baig , Edward C. “Should You Be Worried about Facial Recognition? .” *AARP*, 11 May 2022, www.aarp.org/home-family/personal-technology/info-2022/facial-recognition-technology.html#:~:text=Facial%20recognition%20has%20long%20been.

Bartneck, Christoph, et al. “Privacy Issues of AI.” *An Introduction to Ethics in Robotics and AI*, vol. 22, 12 Aug. 2020, pp. 61–70, link.springer.com/content/pdf/10.1007%2F978-3-030-51110-4_8.pdf, https://doi.org/10.1007/978-3-030-51110-4_8.

Bradley, PJ. “Understanding India’s Personal Data Protection Bill (PDPB).” Tripwire.com, 2023, www.tripwire.com/state-of-security/understanding-india-personal-data-protection-bill-pdpb. Accessed 11 Jan. 2024.

Chakravorti, Bhaskar, et al. “Charting the Emerging Geography of AI.” *Harvard Business Review*, 12 Dec. 2023, hbr.org/2023/12/charting-the-emerging-geography-of-ai#:~:text=The%20fact%20that%20the%20U.S. Accessed 8 Jan. 2024.

Council of Europe. “Convention 108 and Protocols.” *Data Protection*, www.coe.int/en/web/data-protection/convention108-and-protocol.

Didomi. “South Korea Data Protection Law (PIPA): Everything You Need to Know | Didomi.” Blog.didomi.io, 2 May 2023, blog.didomi.io/en/south-korea-pipa-everything-you-need-to-know.

Ferm, Lars-Erik Casper, et al. “AI and Its Implications for Data Privacy.” *Www.routledge.com*, 30 Aug. 2023, www.routledge.com/blog/article/ai-and-its-implications-for-data-privacy.

Fruhlinger, Josh. “Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?” *CSO Online*, 12 Feb. 2020, www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

Intersoft Consulting. “General Data Protection Regulation (GDPR).” *General Data Protection Regulation (GDPR)*, Intersoft Consulting, 2018, gdpr-info.eu/.

Local Government Association. *The General Data Protection Regulation (GDPR) Guidance for Members*. 2018.

MacAskill, Ewen, et al. “NSA Files Decoded: Edward Snowden’s Surveillance Revelations Explained.” *The Guardian*, The Guardian, 1 Nov. 2013, www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

OEDC. “Personal Data Protection at the OECD.” *Www.oecd.org*, www.oecd.org/general/data-protection.htm#:~:text=The%20OECD.

“Open-Ended Working Group Cyber 201: Framework Recap → UNIDIR.” Unidir.org, 7 Dec. 2021, unidir.org/event/open-ended-working-group-cyber-201-framework-recap/. Accessed 11 Jan. 2024.

OVIC. “Artificial Intelligence and Privacy - Issues and Challenges.” *Office of the Victorian Information Commissioner*, ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/#discrimination.

Rodgers, Cathy McMorris, and Jay Obernolte. “AI’s Rise Flags Need for Federal Privacy and Security Protection.” *News.bloomberglaw.com*, 6 Nov. 2023, news.bloomberglaw.com/us-law-week/ais-rise-flags-need-for-federal-privacy-and-security-protection.

Romanek, Broc. “What Is “Transparency”?” *RealTransparentDisclosure.com*, 26 July 2023, www.realtransparentdisclosure.com/blog/2023/07/26/what-is-transparency/#:~:text=Transparency%20is%20about%20taking%20disclosure. Accessed 8 Jan. 2024.

Sainty, Katherine, and Ottilia Thomson. “Australia: Privacy Concerns of Large Language AI.” *DataGuidance*, 27 July 2023, www.dataguidance.com/opinion/australia-privacy-concerns-large-language-ai.

Satter, Raphael, et al. “US, Britain, Other Countries Ink Agreement to Make AI “Secure by Design.”” *Reuters*, 27 Nov. 2023, www.reuters.com/technology/us-britain-other-countries-ink-agreement-make-ai-secure-by-design-2023-11-27/.

van rijmenam, mark. “Privacy in the Age of AI: Risks, Challenges and Solutions.” *Dr Mark van Rijmenam, CSP - the Digital Speaker | Strategic Futurist*, 17 Feb. 2023, www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/.

NISCMUN

Nord Anglia SEAME&I REGIONAL
Model United Nations 2024