Forum: General Assembly 6

Issue: Addressing Digital Privacy

Student Officer: Sophie Chang

Position: Head Chair

Introduction

The vast expansion of digital technologies has transformed into a crucial concern encompassed by how information is collected, utilized, and secured through interconnected networks and devices. Digital privacy approaches beyond the traditional framework of privacy as a physical solute, emphasizing instead the accessibility and control of individuals over their digital identities, information, and communications.

The exponential growth of the internet, mobile technology, and data-driven services has increasingly escalated the personal information being generated daily. Various Data collection practices, such as online shopping and creating digital accounts, constantly involve aggregating detailed personal profiles through online platforms, exposing users' private documents to potential exploitation if inadequately protected. Common internet privacy concerns include tracking through the websites you access, as well as surveillance by advertisers, governments, or organizations. Cybersecurity measures to secure digital privacy are encountering threats from sophisticated cyberattacks and gaps in regulatory enforcement. However, legal and regulatory frameworks differ across the globe, establishing various levels of protection, digital privacy enforcements, and governmental accessibility. Therefore, balancing the convenience of digital technologies and protecting against privacy breaches is crucial to address the ongoing issue. Additionally, possible biased algorithms generated by artificial intelligence may perpetuate discrimination in cooperative and social dimensions, leading to unequal treatments and implementations on the basis of previous or inaccurate data.

Definition of Key Terms

Digital Privacy

Digital Privacy refers to the ability of individual subjects to control, access, and safeguard their personal information. The term is also referred to as online privacy, internet privacy, and cyber privacy. Users should be able to determine and acknowledge the adaptation of their digital information.

Personal Information

Personal Information is the data that can identify or relate to an identifiable or

recognizable individual. The category can include personal details like IP identification, name, address, email, phone number, or digital accounts. Other personal information includes medical records and financial documents that reveal details related to the person.

Consent

Consent refers to the permission or agreement for something to be done, occur, or be accessed. Verbal, digital, and physical agreements are forms of recognition toward a subject, or more recognition of tasks to be done or information to be obtained.

Data Breach

A security incident where personal, sensitive, or confidential information is stolen, leaked, disclosed, or accessed without authorization by a person or entity. Such action includes hacking that exposes personal information, financial documents, and intellectual property.

Shadow AI

The term refers to the AI tools that are used within organizations without formal approval or security oversight, contributing to around 20% of the breaches.

Background Information

The issue of addressing digital privacy is increasingly escalating worldwide. National security concerns, economic interests in data-driven industries, and upholding individual rights are pivotal factors influencing the policies and framework regarding digital privacy. Furthermore, the significant economic value of data, advancement in artificial intelligence, and the complexity of cross-border data flows are key factors that shape the challenges of digital privacy.

Origins of Digital Privacy

Digital privacy concerns are derived from the physical concept of privacy, which is often violated by certain terms. The concept of a modern right emerged from the increasing exploitation of data storage capabilities and computer technology in the mid-20th century, when corporations and individuals began storing information at scale. The history presents privacy as a fundamental human right, continuously challenged by the advances in information technology and online data exposure.

U.S. v. Jones 2012

The first notable court in the context of digital privacy is identified as U.S. v. Jones in 2012. The U.S. Supreme Court ruled that the government's installation of a GPS, a tracking location device, on a suspect's vehicle constituted an unconstitutional search of the suspect under the Fourth Amendment. This was a landmark case highlighting digital privacy in location tracking[1]

Advancement of Artificial Intelligence (AI)

In 2025, the key trends shaping digital technology involve the integration of artificial intelligence. The tool complicates data protection due to extensive data processing and risk in AI governance systems. The application increased legal frameworks both globally and

[1] School, Cornell Law. "United States v. Jones." *Legal Information Institute*, Legal Information Institute, 23 Jan. 2012, www.law.cornell.edu/supremecourt/text/10-1259

domestically; however, it simultaneously increased data breaches and more complex cross-border data sharing rules, such as the U.S. DOJ rule on cross-border data access. These privacy laws are rapidly expanding, covering over 80% of the global population with strict mandates on data minimization and transparency in AI and digital processes.

According to Stanford's 2025 AI Index report, Artificial Intelligence-related privacy incidents surged by 56.4% in 2024, totaling 233 reported cases worldwide. These include unauthorized data access during AI training, synthetic identity creation, model inversion attacks, extracting training data, and long-persisting personal data in AI systems.

In June 2025, massive breaches exposed 16 billion passwords and access credentials to major platforms like Facebook, Google, Apple, and Microsoft through [2]infostealer pathways.

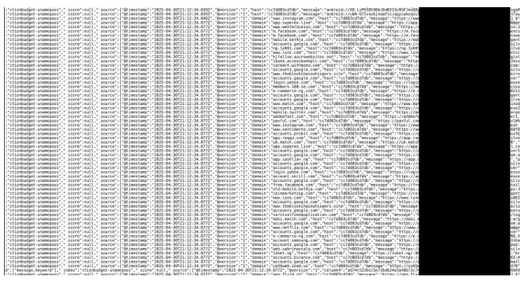

Figure: This is leaked information on the datasets that includes URLs to major platforms

IBM's 2025 report states that 13% of organizations experienced breaches involving AI models or applications, with 97% lacking adequate AI governance or security controls. Furthermore, 63% of the breached organizations either don't have any AI governance policies and applications or are still in development. Only around 34% of the organizations with governance policies perform regular checks to detect unauthorized AI use, often referred to as " shadow AI ".

United Nations' (UN) involvement

The UN has been actively supporting digital privacy rights through multiple resolutions and initiatives. A landmark resolution is General Assembly Resolution 68/167 (2013) and its follow-ups, such as 73/179 (2018), which emphasize the right to privacy in the digital age, urging states to protect individuals from unlawful surveillance and promote transparency in data processing.[3] The UN calls on states to review their surveillance practices regularly and implement oversight mechanisms while encouraging businesses to respect privacy rights. The UN High Commissioner for Human Rights continues dialogue on privacy, especially concerning challenges posed by profiling, automated decision-making, and encryption technologies.

UN Agency Program

UN Personal Data Protection and Privacy Group (UN PPG): The UN PPG was established in 2016 as an inter-agency group co-chaired by UN Global Pulse and the UN Office of Information and Communications Technology. It coordinates data privacy efforts within the UN system, setting principles to harmonize personal data protection, ensure accountability, and respect human rights globally. The Principles on Personal Data

---

[2] *Spencer, Patrick. "AI Data Privacy Wake-up Call: Findings from Stanford's 2025 AI Index Report." Kiteworks, 24 Apr. 2025, www.kiteworks.com/cybersecurity-risk-management/ai-data-privacy-risks-stanford-index-report-2025/*

[3] *"Resolution Adopted by the General Assembly on 18 December 2013." 68/167. The Right to Privacy in the Digital Age, United Nations, 21 Jan. 2014, docs.un.org/en/A/RES/68/167*

Protection and Privacy were formally adopted in 2018 to provide a unified framework for the UN's handling of data.

Major Countries and Organisations Involved

European Union

In 2024, the European Union enacted the AI Act with risk-based categories for AI systems—banning unacceptable-risk AI such as mass biometric surveillance, strict controls for high-risk AI in critical sectors, and transparency requirements for limited-risk AI. AI rules complement GDPR protections and include governance for general-purpose AI, effective August 2025, as the world's first comprehensive legal framework for Artificial Intelligence. This act categorizes the AI system through risk-based approaches from minimal to unacceptable. Therefore, providers of GPAI must comply with obligations, including transparency, maintaining technical documentation, and disclosing copyrighted materials used in training.

United States of America

The United States of America also issued Executive Order 14179 in 2025, refocusing policy to promote innovation and U.S. dominance in AI, while revoking some prior strict AI governance directives. Emphasizing national security, regulatory review, and creating a pro-competitiveness environment, but direct new privacy standards for private AI developers haven't yet been established. The government fosters this intelligence in dimensions such as national defence and economic competitiveness.

Coalition for Secure AI (CoSAI)

CoSAI is an industry coalition formed to address security challenges posed by AI systems globally. The coalition focuses on establishing security standards and best practices for AI supply chains, including secure development, deployment, and operation of AI models. CoSAI promotes incident response frameworks specifically tailored for AI-related breaches and vulnerabilities. It supports organizations and governments by developing guidance on AI risk governance to ensure safe and responsible AI use. The coalition collaborates widely with AI developers, cybersecurity experts, and regulatory bodies to disseminate knowledge and improve AI security postures internationally.

China

China's Generative AI Regulation, effective since August 2023, mandates lawful data use, which requires explicit or implicit labeling of AI-generated content, enforces content moderation aligned with socialist core values, and demands providers maintain system security and assist regulatory inspections.[4] The Cyberspace Administration of China (CAC) oversees mandatory algorithm filings and generative AI service registrations, with thousands already approved, demonstrating active regulatory monitoring and enforcement through inspections and penalties for violations. New AI content labeling rules effective September 2025 require

[4] *Lauren Hurcombe, Carolyn Bigg. "China Released New Measures for Labelling AI-Generated and Synthetic Content." Technology's Legal Edge, 24 Mar. 2025, www.technologyslegaledge.com/2025/03/china-released-new-measures-for-labelling-ai-generated-and-synthetic-content/*

visible or metadata labels on AI-generated text, images, audio, and video, enhancing transparency for users. In July 2025, China announced a 13-point Global AI Governance Action Plan emphasizing international cooperation, ethical standards, infrastructure development, and preventing monopolistic control in global AI development. These regulations operate alongside the Cybersecurity Law (CSL) and Personal Information Protection Law (PIPL), forming a comprehensive legal ecosystem managing data privacy, security, and ethical AI development under state oversight

World Economic Forum (WEF)

The WEF launched the AI and Cyber Initiative in 2024 to address the complexity of cybersecurity risks introduced by AI adoption. This initiative is a collaboration between the WEF's Centre for Cybersecurity, the Global Cyber Security Capacity Centre at the University of Oxford, multiple business partners, governments, international organizations, and civil society. The initiative's goal is to provide guidance and actionable recommendations for organizations to manage AI-related cyber risks while balancing AI's benefits and threats. In January 2025, WEF published a comprehensive white paper titled "Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards," presenting a clear perspective on managing AI cyber risks, highlighting the need for embedding cybersecurity at every stage of AI adoption.

Viable Solutions

United Nations member states may focus on enhancing cross-sector and international collaboration for sharing best practices, intelligence, and developing common security standards to address shared AI vulnerabilities and cyber risks effectively. The collaborative effort may restrict the accessibility of unauthorized use of digital technologies, compiling both domestically and internationally.

Politically democratic countries could also put effort into focusing on governance and transparency, which includes strong AI access controls, regular auditing for unauthorized AI use (shadow AI), clear labeling of AI-generated content, and establishing accountability across AI supply chains. This guarantees the citizens' acknowledgment of how their data is applied and protected by government forces, enhancing legitimacy.

Bibliography

"Ai Act." Shaping Europe's Digital Future, 1 Aug. 2025, *digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai*

"Ai Watch: Global Regulatory Tracker - China: White & Case LLP." Edited by Bob Li, China | White & Case LLP, 29 May 2025, *www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china*

Brancati, Michele. "IBM Report: 13% of Organizations Reported Breaches of AI Models or Applications, 97% of Which Reported Lacking Proper AI Access Controls." IBM Newsroom, 30 July 2025, *newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls*

Breaux, Travis. "Understanding Privacy in the Digital Age." IEEE Digital Privacy, 2023,

digitalprivacy.ieee.org/publications/topics/understanding-privacy-in-the-digital-age/ Accessed 22 Sept. 2025.

"China Announces Action Plan for Global AI Governance." ANSI, American National Standards Institute, 1 Aug. 2025, www.ansi.org/standards-news/all-news/8-1-25-china-announces-action-plan-for-global-ai-governance

"Digital Privacy: Definition, Why It Matters, and How to Protect It." SMOWL Proctoring | Supervision System for Online Exams, 18 June 2025, smowl.net/en/blog/digital-privacy/ Accessed 22 Sept. 2025.

Fiveable. "Digital Privacy Issues – AP US Government." Edited by Becky Bahr, Fiveable, 2024, https://fiveable.me/key-terms/ap-gov/digital-privacy-issues Accessed 22 Sept. 2025.

Husain, Osman. "Digital Privacy Definition: What Is Digital Privacy & Digital Safety." Data Privacy Compliance Software for Apps, Websites, & SaaS, Enzuzo, 17 Mar. 2023, www.enzuzo.com/blog/digital-privacy-definition Accessed 22 Sept. 2025.

Lauren Hurcombe, Carolyn Bigg. "China Released New Measures for Labelling AI-Generated and Synthetic Content." Technology's Legal Edge, 24 Mar. 2025, www.technologyslegaledge.com/2025/03/china-released-new-measures-for-labelling-ai-generated-and-synthetic-content/

Law School, Cornell. "United States v. Jones." Legal Information Institute, Legal Information Institute, 23 Jan. 2012, www.law.cornell.edu/supremecourt/text/10-1259

Spencer, Patrick. "AI Data Privacy Wake-up Call: Findings from Stanford's 2025 AI Index Report." Kiteworks, 24 Apr. 2025, www.kiteworks.com/cybersecurity-risk-management/ai-data-privacy-risks-stanford-index-report-2025/

"Resolution Adopted by the General Assembly on 18 December 2013." 68/167. The Right to Privacy in the Digital Age, United Nations, 21 Jan. 2014, docs.un.org/en/A/RES/68/167

Ribeiro, Anna. "WEF Global Cybersecurity Outlook 2025 Report Addresses Geopolitical Tensions, Emerging Threats to Boost Resilience." Industrial Cyber, 14 Jan. 2025, industrialcyber.co/reports/wef-global-cybersecurity-outlook-2025-report-addresses-geopolitical-tensions-emerging-threats-to-boost-resilience/

Team, Anecdotes. "AI Regulations in 2025: US, EU, UK, Japan, China & More." AI Regulations in 2025: US, EU, UK, Japan, China & More, anecdotes, 4 Sept. 2025, www.anecdotes.ai/learn/ai-regulations-in-2025-us-eu-uk-japan-china-and-more

"Trend Micro State of AI Security Report 1H 2025." Trend Micro (US), 29 July 2025, www.trendmicro.com/vinfo/us/security/news/threat-landscape/trend-micro-state-of-ai-security-report-1h-2025

Yin, Kate, et al. "Data Protection Laws and Regulations Report 2025 AI Regulatory Landscape and Development Trends in China." International Comparative Legal Guides

International Business Reports, Global Legal Group, 21 July 2025, *iclg.com/practice-areas/data-protection-laws-and-regulations/02-ai-regulatory-landscape-and-development-trends-in-china*

“16 Billion Passwords Exposed in Record-Breaking Data Breach: Are You Affected?” Edited by Vilius Petkauskas, 16 Billion Passwords Exposed in Record-Breaking Data Breach: What Does It Mean for You?, 18 June 2025, *cybernews.com/security/billions-credentials-exposed-infostealers-data-leak/*