OFFICIAL (OPEN)

ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON

THE INFORMATION DOMAIN

Issue 11/23 (November)

Impact of Emerging Technologies on Data Privacy

INTRODUCTION

1. In today's rapidly evolving digital landscape, emerging technologies, such as Artificial Intelligence (AI), the Internet of Things (IoT) and blockchain are revolutionising the way data is collected, analysed and used. IoT sensors and social media have made it easier for vast amount of personal data to be automatically collected from various sources.

2. Data has become the lifeblood of countless industries and services. Be it personal information collected for tailored advertising, healthcare data used to improve patient outcomes, or financial records stored online for convenience, data plays a pivotal role in our interconnected world. Personal data has thus, become a valuable resource for businesses, governments and organisations seeking to gain further insights and to support informed decision making.

3. In particular, AI has emerged as a transformative force in data-driven decision-making. AI algorithms can now process vast datasets, identify trends, provide accurate predictions and make complex decisions, marking a paradigm shift in how organisations, governments and individuals interact with data.

AI & Data Collection

4. AI-driven applications such as virtual assistants like Siri and Alexa, can acquire data by tracking users' online behaviour, and through smart devices. According to *Upstream*, AI analytics can identify complex patterns and provide predictive insights that may

not be readily apparent through manual analysis. For instance, AI-powered recommendation systems analyse users' habits and preferences, purchase history and social interactions to provide tailored content, while autonomous vehicles rely on sensors and cameras to collect real-time traffic data to improve the travel experience.

The Impact of Emerging Technologies on Data Privacy

5. While AI has the potential to enhance security by identifying and mitigating threats, it also introduces new risks. The advanced data analysis capabilities of AI could potentially reveal sensitive information about individuals, raising concerns about privacy infringement. For instance, credit card details, purchase history, location, and even the people sharing the same space, are now commonly tracked and collected during virtual interactions and online transactions. Within this data reservoir lies personal and sensitive information that individuals may be unwilling to disclose or that organisations may now use or exploit, without first obtaining an individual's permission for their personal data to be used beyond the original data collection purpose.

6. As *BuiltIn* reported, with intimate knowledge of individuals' identities, activities, social circle and dietary habits, these data points can allow for malicious actors to generate hyper-realistic phishing emails, deepfake videos, letters, voice recordings. For instance, in Oct 2023, a deepfake video of Rashmika Mandanna, a popular South Indian actress, went viral on social media, garnering over 18 million

views. The original video was posted by Zara-Patel, a British-Indian lady. It was digitally altered subsequently to resemble Rashmika Mandanna (see Figures 1a and 1b for comparison). The video was circulated anonymously on social media platforms, and the identity of the person or group who altered the video was not publicly disclosed. This is an example of how AI can be easily misused to commit identity theft, through the use of manipulated content to falsely represent individuals, and compromise individuals' privacy and personal information.

Figures 1a and 1b: Screenshots of the Original and Digitally Altered Videos of Zara-Patel

Left: Zara-Patel and Right: Rashmika Mandanna

7. Such proliferation of emerging technologies has brought about profound impacts on data privacy and security. As reported by *The Digital Speaker,* the vast amounts of data generated and shared online has enabled businesses, governments and organisations to glean fresh insights and enhance decision-making. As such, the concept of data privacy becomes paramount and have become more urgent with the amount of data generated and shared online.

ASSESSMENT

8. As the use of data grows, the significance of safeguarding it increases. Data privacy encompasses the protection of individuals' personal and sensitive information, guarding against unauthorised access, breaches or misuse. However, achieving a balance between embracing emerging technologies and safeguarding data privacy is a complex task. The impact of emerging technologies on data privacy and security necessitates a proactive approach, from implementing regulations to individual and organisational taking protective measures to mitigate potential risks.

9. According to *Forbes*, policymakers or government around the world should continue working together to develop a set of comprehensive privacy laws that would mitigate the risks of malicious use of data. For instance, the General Data Protection Regulation (GDPR) – a recent privacy and security law – imposes obligations on organisations that collect, process or control personal data of people in the European Union. The Bletchley Declaration, agreed at the United Kingdom's AI Safety Summit on 1 Nov 2023, is another good example of international cooperation towards addressing AI governance and risks. The Declaration recognises the need for AI development and for its use to be human-centric, trustworthy and responsible.

10. Policymakers play a pivotal role in crafting legislation that aligns with best practices in data privacy and in promoting responsible technology development. Governments across the globe

have been striving to formulate strategies and guidelines for data privacy. For instance, within the Asia region, Singapore, Thailand, and Malaysia have implemented Personal Data Protection Acts (PDPA) to regulate the collection, use and disclosure of personal data. These acts were designed to protect the privacy rights of individuals and establish guidelines for organisations handling personal data.

11. In addition, Singapore's Personal Data Protection Commission (PDPC) has taken a significant step by developing and publishing a Model Framework for responsible AI and data privacy. Published by Infocomm Media Development Authority (IMDA), the PDPC Framework offers comprehensive guidance on a range of measures aimed at promoting the responsible use of AI. It recommends the following key areas that organisations should focus on:

- **Internal Governance Structures and Measures.** Organisations should implement ethical AI policies, and ensure that data privacy considerations are embedded in the AI development process.

- **Determining the Level of Human Involvement in AI-Augmented Decision-Making.** Organisations should also evaluate the level of human involvement in AI-augmented decision-making. This involves considering factors like the significance of decision, potential bias, and the ethical implications of AI-driven choices.

- **Operations Management.** Organisations should conduct continuous monitoring and data handling to uphold data privacy and ethical standards throughout the AI lifecycle.

- **Stakeholder Interaction and Communication.** Most importantly, high levels of trust among stakeholders remain a key aspect to responsible AI. Organisations should work with developers to implement or strengthen technical guardrails that prevent the sharing of confidential information, and avoid sending protected data to third party models that use datasets to train AI and generate content.

12. Policymakers can play a vital role in endorsing and reinforcing these initiatives on a global scale, as well as in aligning legislation with global best practices. The dynamic interplay between technology and privacy shapes our digital future, and how individuals, organisations and governments decide to navigate it will have far-reaching consequences.

References:

1. How Emerging Technologies Are Changing The Way We Work
https://www.upstream.com.au/blog/how-emerging-technologies-are-changing-the-way-we-work-process-automation/

2. Privacy In The Age Of AI: Risks, Challenges And Solutions

https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/

3. Why We Can't Ignore The Dark Side Of AI
https://www.builtin.com/artificial-intelligence/why-we-cant-ignore-dark-side-ai

4. AI Deepfake Video Of Actress Rashmika Mandana Going Viral, Amitabh Bachchan Raises Concern
https://www.indiatoday.in/amp/technology/news/story/ai-deepfake-video-of-actress-rashmika-mandana-going-viral-amitabh-bachchan-raises-concern-2458602-2023-11-06

5. Three Ways AI Chatbots Are A Security Disaster
https://www.technologyreview.com/2023/04/03/1070893/three-ways-ai-chatbots-are-a-security-disaster/

6. Thailand Issues First Personal Data Protection Act
https://www.aseanbriefing.com/news/thailand-issues-first-personal-data-protection-act/

7. Data Privacy And AI Governance: An Outlook On Tech Industry Trends
https://www.forbes.com/sites/garydrenik/2023/10/12/data-privacy-and-ai-governance-an-outlook-on-tech-industry

8. Singapore's Approach to AI Governance
https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework

We welcome your contributions and feedback on the issues covered in the report as well as issues that future reports could cover. Please do not hesitate to write to us at ACICE@defence.gov.sg.