Privacy, Security and Bias in Emerging Technologies

Emerging technology is an obvious and oft-repeated term, usually referring to digital technology recently developed. The first use of social messaging tools to make calls or send messages was approximately 12 years ago. Digital payments are another example; people all over the world can leave their physical wallet behind and use their phones to book a taxi or pay at a nearby supermarket. There are enterprises that provide tools to help consumers virtually try on outfits or glasses before deciding to make a purchase. It would not be absurd to say that authors could be writing future *ISACA® Journal* articles using a digital twin (i.e., technology that creates a digital copy of a physical object or process) in 2024.[1]

Although there are endless possibilities associated with emerging technology, there is also confusion regarding how new technologies will use personal information. There are several regulations that force organizations in the European Union, the United States and elsewhere to safeguard personal information collected via connected devices, but those do not guarantee privacy and security around how those data can be utilized or misused. This is a warning sign and a neglected topic that needs addressing either via stricter and well-rounded regulations, an end-to-end bias-free solution, or both. It is also essential to ensure that bias is not baked into the regulations or solutions designed.

SHINI MENON | CISA, CISM, CDPSE

Is a senior manager within the risk advisory practice at Deloitte Canada. She has nearly 15 years of experience working at product, service and consulting firms such as Oracle, Infosys, MetricStream, PricewaterhouseCoopers and KPMG. Her expertise lies in governance, risk and compliance platforms, and setting up and managing teams for IT auditing, risk and control transformation programs, International Organization for Standardization (ISO) certification, US Sarbanes–Oxley Act of 2002 compliance, pharma and banking regulatory compliance, third-party risk assessments, data privacy standards such as the US Health Insurance Portability and Accountability Act (HIPAA), and other integrated risk areas. She is associated with ISACA® and other professional bodies.

Defining Emerging Technology

Emerging technologies are defined as technologies that are still evolving and whose development and practical applications are still largely unrealized, such that they are figuratively emerging into prominence from nonexistence or obscurity.[2] In some cases, these technologies are starting to develop into innovative solutions to everyday problems. Emerging technology spans most sectors, including finance, construction, retail, energy management, IT and healthcare. Some of these technologies such as artificial intelligence (AI), robotics, augmented reality (AR) and virtual reality (VR) are in use today and continue to be developed in the hopes of solving specific cross-industry problems.

Some of the emerging technologies that have made headlines include VR, digital currency, digital scent technology[3] and concentrated solar power for electricity generation.[4] All of these have moved past the research and development stage and are rapidly being tested for commercialization. One of the recent discussions has been about the metaverse.[5] The metaverse takes human imagination to the next level by helping users visualize an all-virtual economy that includes virtually buying cars, building virtual homes, and virtually hosting events or talk shows. The dependencies of many of the individual components for the metaverse relate to enabling AR, flexible working, 5G, artificial intelligence (AI), the Internet of Things (IoT) and related emerging technologies.

Privacy and Security Concerns

In the universe of these coexisting technologies, privacy and security experts are raising concerns about what the future holds.[6] Although these technologies positively impact rapid digitalization, at the same time, they can cause worry with regard to sharing sensitive and private information.[7] Common issues include:

- Sensitive data is shared across IoT devices.[8] There is also the added risk that there are very few skilled resources available to implement IoT security.
- There is a lack of frameworks or regulations to fully support security and privacy issues.

- Mobile payments have become the new normal, but they contain a great deal of personally identifiable information (PII) that is shared across networks. The concern is whether PII is protected from data breaches.
- Vulnerability management and protection against malware continues to be a concern as organizations move toward DevOps and cloud-based container implementations.

Opportunity in the Threat?

The good news is that many of these concerns can be addressed by a newer set of technologies[9] that began with biometrics-based security solutions. These include current security and privacy technologies such as:

- Decentralized identity management (i.e., technologies such as blockchain that can help distribute the storing of digital identities across a large array of systems)
- Cloud infrastructure entitlement management (CIEM) where a standalone tool can monitor identities and permissions over the cloud
- Secure access service edge (SASE), which focuses on decentralized, dynamic and evolving security architecture
- Passwordless authentication that allows biometrics, facial recognition and other alternate mechanisms to enable access

Biased Emerging Technology

Security and privacy teams have many hurdles to pass. The most important of these is the biased approach (forming opinions and making decisions based on previous experiences rather than focusing on objective facts and current security and privacy risk) to tackling information security problems. Common biases (mostly stemming from judgements and subconscious decision making) include:

- **Affection bias or affect heuristic**—Relying on emotions rather than concrete information. For example, "We as a security team feel this is a low-risk incident and will not investigate any further."
- **Anchoring bias**—Relying on the first piece of information available. For example, "The chief information officer (CIO) and chief information security officer (CISO) think ABC vulnerability is the most critical aspect of our security threat landscape, so we will focus on that."

- **Optimism bias**—Relying on the fact that the security and privacy teams are less likely to experience negative emotions, even if the data suggest otherwise. For example, "This threat does not affect our organization."

Human judgements are inhibitors to effective implementation of any privacy or security program, and it is safe to say that bias is also driven by this dependency on human intervention.[10] A lot of these biases are related to the security practitioner's ability to make the right security decisions. As a result, some organizations implement security risk assessments to identify, assess and implement key controls that could mitigate risk and overcome subjective biases.

Some organizations implement security risk assessments to identify, assess and implement key controls that could mitigate risk and overcome subjective biases.

AI to the Rescue: Superhero or Super Evil?

AI is an emerging technology that has grown exponentially over the past decade. Can AI (or any other emergent technology, such as blockchain) be the solution to avoiding bias when addressing security and privacy? AI is certainly one of the emerging technologies that can be a potential solution, as it can be used to make decisions based on available data, trained responses and historical

LOOKING FOR MORE?

- Read *The Pulse: State of Emerging Technologies. www.isaca.org/pulse-emerging-technology-2021*
- Learn more about, discuss and collaborate on emerging technology in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

There is a need to build training data sets that are based on objective incident response mechanisms and the type of security and privacy responses solely focused on the given controls that need to be built in.

evidence. However, AI can only be a viable selection if security teams and organizations are conscious of influencing factors, such as:

- **Business rules and related biases**—Attention needs to be paid when business rules are created within algorithms that could lead to biased outcomes. Bias may depend on whether the business rule algorithms are focused on the end-user data set or are based on the biases arising from human judgment.
- **Limited training sets**—The data used to train AI also have a long history of human judgment and prejudice There is a need to build training data sets that are based on objective incident response mechanisms and the type of security and privacy responses solely focused on the given controls that need to be built in.
- **Collaborators' effect**—Rather than approaching security and privacy in a balanced manner, security team decisions are viewed based on the experience of one person as opposed to varied takeaways.[11] There is a need to address this factor by building in a solution that provides for objective and data-based decision-making.

Conclusion

The future of emerging technology is promising. While there may be specific solutions that can target each of the biases that occur, there is an urgent need for:

- A responsible and ethical AI solution that is bias free and based on objective data sets targeted at specific data privacy and security concerns
- Creation or amendment of privacy and security regulatory frameworks to address emerging technologies
- A single platform for capturing permutations and combinations of the types of data sets that include user privacy and specific solution statements for each of the data sets

If there is a mechanism to build a single platform that addresses the concerns, then this can be a potential solution. It will require tremendous efforts to understand security and privacy postures while society continues to move into the metaverse and the virtually connected world.

Endnotes

[1] Marr, B.; "What Is Digital Twin Technology—And Why Is It So Important?" *Forbes*, 6 March 2017, *https://www.forbes.com/sites/bernardmarr/2017/03/06/what-is-digital-twin-technology-and-why-is-it-so-important/?sh=577b2dc02e2a*

[2] IGI Global, "What Is Emerging Technologies?" *https://www.igi-global.com/dictionary/emerging-technologies/37736*

[3] Future of Smell, "Perfumery Science Meets Digital Scent Technology," *https://www.futureofsmell.com/*

[4] Solar Energy Industries Association (SEIA), "Concentrating Solar Power," *https://www.seia.org/initiatives/concentrating-solar-power*

[5] Ravencraft, E.; "What Is the Metaverse, Exactly?" *Wired*, 25 April 2022, *https://www.wired.com/story/what-is-the-metaverse/*

[6] Huddleston, J.; A. Hobson; A. Miller; "Mitigating Privacy Risks While Enabling Emerging Technologies," George Mason University Mercatus Center, Fairfax, Virginia, USA, 24 October 2019, *https://www.mercatus.org/publications/regulation/mitigating-privacy-risks-while-enabling-emerging-technologies*

[7] Sentas, "Emerging Technology Data Security Concerns," *https://www.senetas.com/emerging-technology-data-security-concerns/*

[8] Clearswift, "The Top-Three Emerging Technologies Posing a Cyber-Threat to Our Critical National Infrastructure," *https://www.clearswift.com/blog/top-3-emerging-technologies-posing-cyber-threat-our-critical-national-infrastructure*

[9] Alspach, K.; "Emerging Tech in Security and Risk Management to Better Protect the Modern Enterprise," VentureBeat, 26 November 2021, *https://venturebeat.com/2021/11/26/emerging-tech-in-security-and-risk-management-to-better-protect-the-modern-enterprise/*

[10] Durbin, S.; "Ten Cognitive Biases That Can Derail Cybersecurity Programs," *Security Magazine*, 17 January 2022, *https://www.securitymagazine.com/articles/96918-10-cognitive-biases-that-can-derail-cybersecurity-programs*

[11] Henry, J.; "Biased AI Is Another Sign We Need to Solve the Cybersecurity Diversity Problem," *Security Intelligence*, 6 February 2020, *https://securityintelligence.com/articles/biased-ai-is-another-sign-we-need-to-solve-the-cybersecurity-diversity-problem/*