CARTER LEDYARD

our resources

Understanding Tech Terms: Cybersecurity, Data Privacy, Cryptocurrency, and AI — Part VI

October 28, 2024

The digital frontier continues to expand at an unprecedented pace, with innovations in artificial intelligence, cybersecurity, cryptocurrencies, and data privacy reshaping our technological landscape. As these fields evolve, they bring forth a constellation of new concepts, each a star in its own right, forming galaxies of knowledge waiting to be explored.

Part VI of this series introduces the intricate world of quantum computing to the nuanced concepts of zero-knowledge proofs. We aim to illuminate these complex ideas, making them accessible to both the curious novice and the seasoned tech enthusiast.

Our previous publications in this series of helpful tech terms can be accessed via the following links: Part I, Part II, Part III, Part IV, and Part V.

For questions, please don't hesitate to contact: Matt Dunn, Ron Feiman, Jon Trafimow, Jenny Frank, Joe Basrawi.

Cybersecurity Terms

Patch: A patch is a software and operating system update to improve security by addressing security vulnerabilities within a program, such as fixing a performance bug or enhancing security features and functionality. For individual consumers and firms, it is important to implement patches when they are made available to avoid or mitigate security vulnerabilities. Patches may come in the form of updates to programs or applications that, once installed, protect devices or systems from potential cyber attackers and hackers, which can either be manually updated by visiting the vendor's website or automatically updated with push notifications after a consumer provides consent upon the program's initial installation or configuration. Some patches may be more complicated to install or deploy, and/or may have unintended consequences.

Quantum Computing: Quantum computing involves using systems of electrons, photons, or ions as quantum bits (or "qubits") as the basic unit of information to represent information and perform calculations, instead of the on-off transistor systems used in standard digital computers. This technology uses the behavior and properties of subatomic particles and waves to multiply the number of simultaneous calculations on massive compilations of data, enabling quantum computers to solve complex optimization problems almost instantaneously by choosing the best alternative from a large range of options (such as the translation of encrypted data).

Zero-Day: A zero-day vulnerability or zero-day threat in a system or device is one which has been disclosed before the vendor becomes aware of it, so security researchers and software developers have not yet implemented a patch to fix it. Any attack on such a vulnerability is called a "zero-day exploit." Zero-day vulnerabilities pose high risks to consumers and firms because cybercriminals and hackers may exploit these vulnerabilities via cyber-attacks before a patch is implemented by the vendor and applied by consumers. Many zero-day exploits are targeted attacks, such as planting malware that enables the attacker to steal, encrypt, or destroy data, which causes economic damage or loss of proprietary assets. Because the security threat has not previously been identified, existing antivirus software solutions or other threat detection technologies do not address the "zero day" exploit.

Data Privacy Terms

*Note that some data privacy statutes or regulations, or interpretations of them, may define the following terms differently.

Data Localization: Data localization is a requirement imposed by countries' individual laws that data must be kept and stored within a particular country's borders. This approach is based upon the concept that a country's citizens/residents should have their personal data collected, processed, and stored within the region where it originated to protect such data, increase data security, and control access to data. Data localization involves protecting individual rights to privacy, securing national security, and regulating cross-border commerce because it provides a way for countries to control how personal data is stored and managed by ensuring compliance with local laws and regulations that are created and maintained by that particular country. For example, the EU's GDPR requires that certain acceptable safeguards be in place prior to transferring personal data out of the EU unless other safeguards in place.

Iris Identification: Iris identification is a type of biometric identification that utilizes an automated method of mathematical pattern-recognition techniques on videos to identify one or both of the irises of an individual's eyes. For each individual, irises (the colored part of the eye surrounding the pupil) include complex, random patterns that are unique, stable (usually unchanging), and visible and identifiable by this technology from a reasonable distance away, so an individual's identity can be verified with a high degree of certainty. Iris identification is a digital image/video processing that is now commonly used by many security systems instead of traditional methods (e.g., passwords and swipe/access cards).

Crypto Terms

Initial Coin Offering (ICO): An ICO is a form of fundraising for a new cryptocurrency, which is similar to an initial public offering (IPO). While IPOs have a very structured process for launch by listing the stock on a public exchange, ICOs are not as strictly regulated. However, depending on whether the ICO meets certain criteria in its launch country, it is possible that the cryptocurrency may be considered a security (e.g., in the U.S., the SEC would force its standard compliance protocols upon an unregistered security sale of cryptocurrency).

Pig Butchering: Pig butchering is a type of long-term scam conducted through social media or other online communication in which the victim is gradually lured through manipulation of trust or affection into making increasing contributions, usually in the form of cryptocurrency, for fraudulent rationales, such as achieving certain gains or enabling a "loved one" to escape a crisis. The "butchering" or "slaughtering" of the victim transpires when the victim's assets or funds are stolen rather than used as promised.

Zero Knowledge Proofs (ZKPs): ZKPs are cryptographic methods by which one party (the prover) proves to another party (the verifier) that the prover possesses certain information without revealing the actual information itself. A successful ZKP requires: completeness (in the verification process), soundness (blocking all false statements from being accepted as true), and zero-knowledge (of the actual information being verified). Thus, ZKPs are particularly valuable in scenarios where maintaining privacy is crucial but verification of information is also necessary. ZKPs have wide-ranging applications, including enhancing privacy in blockchain and cryptocurrency transactions, secure authentication systems, confidential voting processes, and financial audits.

Artificial Intelligence Terms

Automated Decision-Making:

Automated decision-making is the process by which automated systems via algorithms or artificial intelligence make decisions without direct human involvement. These systems analyze large amounts of data to make determinations that can significantly impact individuals in areas such as financial services (credit scoring and lending), housing eligibility, insurance underwriting, educational admissions, criminal justice (risk assessments and sentencing), employment opportunities (hiring algorithms), healthcare services, and access to essential goods or services. Automated-decision making is strictly governed by the GDPR and CCPA/CPRA ("CCPA/CPRA and "GDPR" are defined in Part I of this series), and many other states' comprehensive privacy laws are beginning to or already incorporate restrictions and regulations on automated-decision making. Additionally, automated-decision making comes in many forms, such as Automated Employment Decision Tools ("AEDTs," which are discussed here) which are used to make decisions in employment contexts and are subject to regulations in certain jurisdictions, including New York City, and may also be of concern under U.S. federal law, as discussed here.

ChatGPT o1

ChatGPT o1 is a new series of the ChatGPT artificial intelligence or machine learning language models, specifically designed to enhance reasoning capabilities and solve complex problems. The o1 models are an improved version of their former series because they spend more time "thinking" through tasks before responding to challenging question, such as those including science, coding, and mathematics. Rather than merely responding to a prompt by a user, the o1 model develops its own prompts to better understand the user's prompt. Its process would include clarifying the task, guiding neutral recommendations to aid the user, compiling accurate advice based upon specifics of the user's prompt, providing options, and evaluating those options for the best solution or an array of possible sufficient solutions.

Explainability

Explainability of artificial intelligence reasoning is AI's ability to construct, after making decisions or predictions, understandable and transparent logical steps from input to output for the purposes of evaluating the data sources and endpoint conclusions in a rational and coherent manner understood by humans that is also fair and unbiased. Explainability is one method to assess whether the AI system is hallucinating ("hallucinating" is defined in Part III of this series).

related professionals

Matthew D. Dunn / Partner
D 212-238-8706
mdunn@clm.com

Jonathan Trafimow / Partner
D 212-238-8651
trafimow@clm.com

Ronald M. Feiman / Partner
D 212-238-8880
feiman@clm.com

Jodutt Marwan Basrawi / Associate
D (212) 238-8767
basrawi@clm.com

Jennifer "Jenny" Frank / Associate
D 212-238-8650
frank@clm.com