CARTER LEDYARD

our resources

Understanding Tech Terms: AI, Cybersecurity, Crypto, and Data Privacy — Part V

January 05, 2024

The constant evolution of artificial intelligence, cybersecurity, cryptocurrencies, and data privacy make these domains and industries exciting and, at many times, overwhelming. For many of us, they may look like different planets, each being their own worlds to explore.

New worlds bring new concepts and languages. Part V of this series aims to assist our readers with getting a few steps closer to understanding and navigating these new worlds and languages.

Our previous sets of helpful tech terms can be accessed via the following links: Part I, Part II, Part III, Part IV.

For questions, please don't hesitate to contact: Matt Dunn, Tom Davis, Jenny Frank, Joe Basrawi, Brielle Kilmartin

Artificial Intelligence Terms

Chatbot: A chatbot is a software that mimics human-like conversations. It uses advanced AI techniques such as natural language processing and machine learning to comprehend user queries and respond accordingly. Chatbots provide instant responses to user inquiries, making information retrieval quick and efficient.

Deep Learning: Deep learning is a more advanced form of machine learning that uses neural networks with at least three layers. These networks try to replicate the human brain's functioning, enabling the system to learn from vast data. Deep learning powers many AI applications and services, enhancing automation and performing tasks without human intervention. It's the technology behind many everyday products and services like digital assistants, voice-enabled TV remotes, and credit card fraud detection, as well as emerging technologies like self-driving cars.

Watermark: A method used to indicate that a video or audio file has been created by artificial intelligence. This is similar to an artist signing their work. For instance, if an insurance company made a commercial featuring a digital version of a celebrity created by AI, they would need to include a watermark. This watermark serves as a notification to viewers that what they're seeing is a computer-generated representation of the celebrity, not the actual person.

Cybersecurity Terms

Intrusion Prevention System ("IPS"): A form of network security that works to detect and prevent identified threats. An IPS continuously monitors networks, looking for possible malicious incidents and capturing information about the incidents. An example of an IPS is a home network, in which an IPS program monitors router traffic and flags a malicious IP address. Another example of an IPS is a company network, where the company's IPS would monitor strategic network points to

monitor and protect all network traffic.

Whitelisting: Unlike blacklisting, whitelisting is authorizing approved applications for use within organizations to protect systems from potentially harmful applications. Whitelisting can be in the form of IP address whitelisting, application whitelisting, and whitelisting for nodes. For instance, a company wishing to ensure a safe software environment would employ a whitelist of approved software applications on its machines and networks. Commonly whitelisted applications include Microsoft Office applications, Adobe programs, specific web browsers, and video-conferencing software.

Data Privacy Terms

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

Data Mapping: A system for cataloging collected data, such as in the form of a spreadsheet detailing the collected data or the form of a flow chart depicting the movement of data through an organization. Data mapping enables the accurate connection of sensitive data to the identity of a particular person. It allows for the identification of data subject records within all data sources, then the matching and linking of those records across systems to create a 360-degree view of each individual data subject for data analysis purposes.

Sale of Data: The practice of exchanging a data subject's personal information collected, processed, or stored by a business with a third party for monetary or other valuable consideration. The various U.S. state comprehensive data privacy laws define a "sale" differently such that what constitutes a "sale" in the data privacy context of those different states depends on whether a "sale" must be made for monetary consideration. Otherwise, under some laws, essentially any transfer of personal information may be considered a "sale" because the business transferring such personal information could be deemed to receive some form of valuable consideration in exchange for that personal information. The most broad definition of a "sale" of personal information is under the CPRA which conflates the definitions of "sale" and "sharing" (the "CPRA" is defined in Part I of this series).

Crypto Terms

Consensus: A mechanism that allows a decentralized peer-to-peer system to make decisions without a central authority figure. There are many kinds of consensus algorithms in blockchain environments, and each consensus algorithm has its own proper application scenario. Proof-of-work (PoW) and proof-of-stake (PoS) are the two most prevalent consensus mechanisms in the context of blockchains and cryptocurrencies. (PoW and PoS are defined in Part III of this series). A novel consensus algorithm called proof of vote (PoV) has been proposed, where the distributed nodes controlled by consortium members could reach consensus and come to a decentralized arbitration by voting. The production and verification of PoV blocks are decided by the voting results among the core consortium members.

Node: A device that participates in running the protocol software of a decentralized network. Nodes work together to form the governing infrastructure of a blockchain. Their primary functions are to run a blockchain's software to validate and store a complete history of transactions on the network and to monitor activity to ensure security. There are different types of nodes in a blockchain network, including full nodes, light nodes, and miner nodes. Full nodes store a complete copy of the blockchain ledger, while light nodes only store the necessary data to verify transactions. Nodes communicate with each other through a peer-to-peer network, which allows them to exchange information and maintain consensus on the state of

	the blockchain.
Private Key:	Similar to a password, a private key is a code of letters and numbers used to access a crypto wallet, authorize crypto transactions, and prove ownership of a blockchain asset. A typical private key consists of dozens of digits (in some cases, hundreds), and safe storage of private keys is very important. An example of a private key on Ethereum is: afdfd9c3d2095ef696594f6cedcae59e72dcd697e2a7521b1578140422a4f890.

–

Other episodes in this series:

Understanding Tech Terms: Cybersecurity, Crypto, and Data Privacy — Part I

Understanding Tech Terms: Cybersecurity, Crypto, and Data Privacy — Part II

Understanding Tech Terms: Cybersecurity, Crypto, and Data Privacy — Part III

Understanding Tech Terms: Cybersecurity, Crypto, and Data Privacy — Part IV

related professionals

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

H. Thomas Davis, Jr. / Partner
D 212-238-8850
davis@clm.com

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

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

Brielle E. Kilmartin / Associate
D 212-238-8652
kilmartin@clm.com