CARTER LEDYARD

our resources

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

April 03, 2023

A lot has happened since our first installment of Understanding Tech Terms just a few weeks ago. We have seen increased attention to artificial intelligence issues and products, such as the chatbots ChatGPT and Bard, which have piqued the interest of the media, general public, and government regulators. After issuing investor guidance that crypto is "exceptionally volatile and speculative," the Securities and Exchange Commission is expected to propose rules in the near future that frustrate (or rein in) the growth of crypto as a generally accepted financial asset. U.S. lawmakers and regulators have expressed fear of the privacy risks associated with the widespread use of social media apps, especially TikTok because of the potential for users' private data to be accessed and exploited by China's government.

With these developments affecting businesses across the globe, we provide these simple definitions in this Part II of our series to help "non-techies" navigate the terminology associated with cyber, data privacy, and crypto.

Sign up here for alerts when we publish more!

–

Cybersecurity Terms

Artificial Intelligence (AI): Software designed to acquire and apply knowledge and skills to replicate human intelligence. AI usually includes input channels that are able to recognize patterns in visuals, speech, decision-making, translation, and behavior, then learn from those patterns, assess improvements in its outputs, and adjust its algorithms (that is, modify its software operating instructions) to optimize the process. AI performs tasks that were not specifically programmed into its systems and are not tethered to a particular task or logic. Practical applications include web search engines, targeted online advertising, autonomous vehicles, and chatbots.

Chatbot: A computer program that is used for online internet-based chat conversations to simulate a conversation with a human user by implementing AI, automated rules, and machine learning. Chatbots can be software applications that answer simple questions with brief responses or more sophisticated digital assistants that provide complicated, lengthy replies and increase their databases by collecting and processing information. Also known as a "chatterbot."

Denial-of-Service: A form of cyber attack involving an interruption or shutdown of a network caused by malicious actors to prevent legitimate users from accessing the network. Perpetrators typically inundate the targeted network with information, excessive requests, or other traffic that floods the network and causes the network's servers to crash.

Data Privacy Terms

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

Biometric Data: Personal data about an individual's physical, biological, or behavioral characteristics that can be used for identification purposes. The definition of biometric data can vary based on jurisdiction and may include things like fingerprints, voice recognition, facial images, and retina patterns. Various U.S. states' data privacy laws and the GDPR (the General Data Protection Regulation in force in Europe, defined in Part I of this series) restrict the use of biometric data.

Cookies: Small text files that are placed on a computer or mobile device when browsing websites that allow controllers of a website to distinguish users from one another. Cookies can recognize a user revisiting a website and record certain information, including pages visited, menu choices made, the date of a visit, and other specific information that the visitor may enter on a form on the website. Various data privacy laws may require disclosure of (and consent to) the use of cookies, which is why cookie banners appear on many websites.

Personal Data Breach: An accidental or deliberate breach of computer security defenses that leads to the destruction, loss, modification, or unauthorized disclosure of personal data. While data privacy and breach laws may have distinct definitions, broadly, this includes any security incident that affects the confidentiality, integrity, or availability of personal data. Examples include unauthorized third party access to data, transmission of personal data to an incorrect recipient, lost or stolen data or devices and databases containing personal data, modification of personal data without permission from its owner, or lost access to personal data.

Supervisory Authority: An independent data protection authority or other governmental body responsible for the administration, implementation, investigation, and enforcement of data protection laws. Specific responsibilities and obligations may vary depending on the particular data privacy law under which the supervisory authority operates. In the European Union, pursuant to the GDPR, each member state has a supervisory authority.

Crypto Terms

Decentralized Applications (dApps): Digital programs that run on a blockchain supported by a peer-to-peer network of computers instead of a single centralized computer to protect user privacy, provide freedom from censorship from a single authority, and enable more flexible development. Often built on the Ethereum platform, dApps are developed for numerous purposes and industries, including financial services, supply chain management, gaming, identity verification, healthcare, education, real estate, and social media. For example, Peepeth is a social network dApp and Cryptokitties is a dApp game.

Decentralized Exchange (DEX): A direct peer-to-peer marketplace for cryptocurrency transactions that does not require an intermediary for transfers nor the custody of cryptocurrency funds. DEXs offer transparency in cryptocurrency exchanges because: (i) they are built with blockchain technology and smart contracts and (ii) they reduce the risk of loss because funds do not pass through a third party's cryptocurrency wallet when facilitating a transfer. They are essential to decentralized finance (DeFi).

Mining: A "consensus mechanism" by which members securely add new blocks onto a blockchain to record and confirm transactions by validating those transactions with computer software programs (each computer running such program is called a "node" and the operator of the program on each node is called a "miner"). This process is used by cryptocurrencies, such as Bitcoin, to generate new coins or tokens as a result of verifying the new transactions while simultaneously securing the blockchain. This verification process may also be called “proof of work.”

Token: A digital representation of an asset or interest that has been “tokenized” (meaning that it was built on a cryptocurrency’s blockchain), which can be used as a transactional unit to raise funds through an initial coin offering (ICO). A crypto token differs from a cryptocurrency “coin” because a token represents an ownership interest while a cryptocurrency coin is used as a medium to facilitate exchanges and payments by serving as a measurable unit of value.

Other Publications in this Series:

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

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