CARTER LEDYARD

our resources

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

May 02, 2023

News about cybersecurity, data privacy, and crypto just won't stop. Calls for a moratorium on artificial intelligence by industry leaders compete with aspirations for both public and private sectors to continue their drive for technological growth, stoking further fear and controversy. Cybersecurity precautions have grown more robust but successful cyberattacks continue. Crypto has become a bedrock for all sorts of new and proposed Web3 applications and the EU recently approved first-of-its-kind comprehensive crypto regulations.

Technology jargon is frustrating. We are publishing this series to help non-technical people penetrate the fog of jargon, the better to follow the ongoing discussions of cyber, data privacy, and crypto. We hope that this Part III of our series on Understanding Tech Terms will bring you closer to participating in relevant discussions.

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

–

Cybersecurity Terms

Hallucinating:	A confident response to an inquiry by artificial intelligence ("AI") that is not correct nor rooted in the AI's programming. For example, a hallucinating chatbot ("AI" and "chatbot" are defined in Part II of this series) may respond confidently with an answer that its AI deems plausible but is ultimately false, and the AI can't or won't explain how the hallucination occurred. AI hallucinations include nonsensical responses or instances in which the AI or chatbot claims to actually be a human or in love.
Ransomware:	A form of malware that renders data and/or systems unusable by encrypting, overwriting, or deleting files to deny authorized users access to them until a ransom payment is made. Cryptocurrencies such as Bitcoin are commonly required for ransom payments because tracking and pinpointing the attacker is difficult and may be impossible.
Transport Layer Security (TLS):	A cryptographic security protocol intended to provide data privacy and security in email and other online communications by authenticating and encrypting the data shared and transferred between servers, machines, and applications that operate in the same network. For example, TLS encrypts the communication in a web browser when loading a website.
Web3:	A concept proposed for the next generation of the World Wide Web that is an open-source (computer software that may be used without charge or copyright infringement concerns if the user complies with the terms of the open source license) and decentralized amalgamation of connected software applications that would operate on a

blockchain and incorporate AI and machine learning. Web3 is proposed as a decentralized platform that would be verified via distributed ledgers and would provide a system for securely exchanging information; such communications and data would be owned by its respective individuals.

Data Privacy Terms

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

Binding Corporate Rules (BCRs):	Legally binding and enforceable data protection policies that provide appropriate safeguards per EU requirements for transfers of personal data between a company's database in an EU nation and another database of the same company in a non-EU nation. BCRs often apply to controllers and also apply to processors ("data controller" and "data processing" are defined in Part I of this series) when acting under the direct instruction of controllers. Companies, particularly corporate groups and their related companies that engage in transferring data internationally among themselves, must submit BCRs to the relevant supervisory authority, which then submits the BCRs to the European Data Protection Board for a final opinion on whether the BCRs are approved.
Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act):	A federal statute that dictates the requirements for commercial messages and provides recipients the right to unsubscribe from emails, text messages, and other similar contact methods. The CAN-SPAM Act applies to any electronic mail message with the primary purpose of commercial advertisement for a product or service, including the promotion of content on a website. Congress exempted political solicitations from the operation of the CAN-SPAM Act but the CAN-SPAM Act may apply to some messaging of nonprofits.
Customer Relationship Management (CRM):	A system that businesses use to manage their interactions with customers to improve their customer service relationships, increase customer retention, and promote sales growth. CRM tracks customers to analyze data such as when the customer last interacted with the system, what promises and quotes were exchanged, what questions were asked by the customer, any competitors the customer may be considering, subscriptions to emails and other media and newsletters, readership statistics, and more. CRM also helps orient new employees about customers and assists executives in understanding their customer base.
Pseudonymization:	A data de-identification process that removes identifying information from personal data and replaces it with artificial identifiers to improve data security and protect the privacy of the owner's identity during data processing. Unlike anonymization, which removes all identifying information for a particular data subject such that the data cannot be traced back to that data subject, pseudonymization only reduces the likelihood of connecting personal data with its owner's original identity.
Standard Contractual Clauses (SCCs):	Model contract clauses for the transfer of personal data that have been pre-approved by the European Commission. Under the GDPR ("GDPR" is defined in Part I of this series), agreements including SCCs provide a permissible way for data to be transferred between entities in EU and non-EU nations. SCCs for the transfer of personal data from the EU to a third country can be found

here. SCCs between controllers and processors can be found here.

Crypto Terms

Markets in Crypto-Assets (MiCA):	Approved in April 2023 and taking effect in phases in 2024, an EU law that provides the world's first set of governmental regulations for cryptocurrencies in digital asset markets, including stablecoins ("stablecoin" is defined in Part I of this series) and unbacked crypto-assets such as Bitcoin. As part of the EU's digital finance strategy, this regulation aims to establish a legal framework for crypto-assets that supports fair and safe competition, protects consumers and investors, and ensures financial stability with safeguards against potential risks. MiCA imposes requirements on crypto platforms, issuers of cryptocurrencies, and traders to provide transparency and supervision over relevant transactions. Also, MiCA includes measures to prevent market manipulation and other illegal activities as well as required disclosures about energy consumption to address concerns about the impact of digital assets on the environment.
Proof-of-Stake:	A consensus mechanism that validates transactions and adds new blocks (new blocks are "forged" or "minted") onto a blockchain as an energy-conscious alternative to the more common "mining" in Proof-of-Work. "Validators" or "forgers" are owners of coins that offer a specific number of their coins as collateral for the chance to be randomly selected to validate blocks for a particular cryptocurrency or other type of token in exchange for transaction fees as a reward for their participation in the staking process. This process requires significantly less computational effort than mining blocks, thus it consumes less energy.
Proof-of-Work:	A consensus mechanism (also known as "mining") by which network 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 requires a significant amount of computing effort to solve a complicated algorithm (a 64-digit encrypted hexadecimal number known as a "hash") of which each resulting solution connects the additional block to the previous block by using that previous block's hash when creating the newest block's hash. Network members are incentivized to participate because miners receive a reward for completing each validating transaction, typically the ownership of a cryptocurrency.
Smart Contract:	A program stored on a blockchain that runs automatically when certain conditions are met based on its programmed code. Smart contracts automate the execution of contract terms, which can be entirely written into the smart contract's code on the blockchain or partially written into the blockchain and partially located outside the blockchain as terms in a traditional contract. For example, a smart contract may be coded to execute a sale and transfer title of an asset to a purchaser when the purchaser deposits a certain amount of money into a seller's crypto wallet, then ownership of the asset is transferred to the purchaser by adding a block onto a blockchain to record the transaction and verify the new owner of the asset.

related professionals

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

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

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

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

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