CARTER LEDYARD

our resources

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

July 11, 2023

In today's fast-paced and interconnected world, understanding the terminology surrounding data privacy, cybersecurity and cryptocurrencies has become essential. New concepts are constantly emerging, from the advent of airtagging to the complexities of cross-border data transfers and the evolving EU-U.S. Data Privacy Framework. Recent cybersecurity breaches and data leaks have underscored the importance of implementing effective "KYC" (Know Your Customer) practices that mitigate risks from malicious actors. The increasingly digital nature of our world has also increased concerns surrounding sensitive personal information (SPI) and how it is collected, used and shared with third parties. Recent regulatory changes and international disputes have brought these issues to the forefront.

As our reliance on technology deepens, the need for a common understanding of these concepts becomes increasingly vital. We hope that this Part IV of our series on Understanding Tech Terms will serve as a guide to offer insight and clarity on the innovations, events and regulations that are shaping our digital future.

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

–

Cybersecurity Terms

Bring Your Own Device (BYOD):	An organization's policy that allows employees to bring and use their own personal devices for work purposes instead of using similar devices provided by the organization itself. Most commonly, employees are allowed to use their own smartphones to access emails, connect to the organization's network, and utilize other apps or data that are shared on the organization's network. Employees may also be allowed to use their own laptops, tablets, and USBs. Because of security concerns, an organization's BYOD policy typically outlines what activities and devices the organization permits on its network, how to operate personal devices effectively and appropriately, whether IT support is provided for personal devices, and how to prevent cyber threats such as ransomware and data breaches.
Generative AI:	Algorithms such as ChatGPT that utilize machine learning to create content and media, including text, images, audio, videos, and code by recognizing patterns in (usually very large) datasets to create new outputs without the need for direct human interaction or commands. Some practical uses so far include diagnosing medical conditions, designing product brands and logos, optimizing business processes, and producing art and music.
NIST Cybersecurity	A voluntary cybersecurity framework based on existing standards, guidelines, and practices for organizations

Framework (CSF):	to better manage and improve their overall cybersecurity posture and exposure to risk. The framework was created by The National Institute of Standards and Technology (NIST), a federal agency and non-regulatory body under the United States Department of Commerce. It was initially published in 2014 and has since been widely adopted by governmental agencies and by various industries such as finance and banking, energy and utilities, and healthcare. Typically, the CSF is used as a starting point and then customized to meet the specific cybersecurity needs of individual organizations regardless of their size or sophistication.
The Health Insurance Portability and Accountability Act (HIPAA):	A U.S. federal law that regulates the use and disclosure of sensitive patient health data, focusing on privacy protection, security, and breach notification. Covered entities such as healthcare providers, health plans and healthcare clearing houses that handle protected health information (PHI) are required to have physical, network, and process security measures in place to protect PHI and to ensure that the privacy rights of individuals are protected.

Data Privacy Terms

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

Airtagging:	A method of tracking personal objects such as keys, bags, and small digital devices by attaching a device that uses Bluetooth instead of GPS. The most common tracking device is the AirTag by Apple. While initially designed for practical uses such as finding lost objects, malicious actors use airtagging to track and follow their victims, potentially for the purposes of personal stalking, stealing whatever object they are tracking, or gaining access to a location or device to execute a cyberattack.
Cross-Border Data Transfer (CBDT):	The movement or transmission of personal data from one jurisdiction or country to another. The term most often refers to the transfer of personal data by controllers located in the EU to recipients outside the EU who act as controllers or processors, which is governed by the GDPR ("controller," "processor," and "GDPR" are defined in Part I of this series). The GDPR imposes significant obligations on the sender and recipient of such personal data and sets forth acceptable ways of transferring such data securely. Some of the appropriate safeguards enumerated in the GDPR for CBDTs include legally binding and enforceable written contracts between the transferor and transferee, binding corporate rules and standard data protection contractual clauses adopted by a supervisory authority ("binding corporate rules" is defined in Part III and "supervisory authority" is defined in Part II of this series).
EU-U.S. Data Privacy Framework (DPF):	A legal mechanism for personal data transfers between the EU and the U.S. that aims to ensure an adequate level of protection for transferred personal data with the basic principles of transparency, accountability, and oversight safeguards. The EU-U.S. DPF is meant to replace the prior EU-U.S. Privacy Shield, which was struck down by the EU, and is intended to address the EU's concerns about U.S. intelligence agencies gathering data on individuals, in particular, the rights of data subjects, certain transfers, exemptions, bulk collection of data, etc. On July 10, 2023, the European Commission announced its adequacy decision for the DPF, which concludes that measures taken by the United States under the new framework ensure an adequate level of protection for Europeans' personal data transferred across the Atlantic for commercial use. Thus, unless obstacles or challenges are encountered, US companies that comply with and participate in the DPF will be able to transfer personal data from the EU to the United States as they once did under the Privacy Shield framework.
Sensitive Personal	Highly confidential and private data about an individual, such as personally identifiable information (e.g., name,

Information (SPI): Social Security number), financial details, health records, biometric data, or other sensitive identifiers that, if exposed or misused, could lead to harm, identity theft, or other adverse consequences. Specific state and international laws may vary in their interpretation of what constitutes SPI and may require that additional protections be afforded to individuals and consumers regarding their SPI, including data breach notifications, data security requirements, and consent and opt-out procedures.

Crypto Terms

Bridge: A tool that serves as a connection between multiple blockchains, allowing assets to be sent from one blockchain to another. Because blockchain assets are typically not compatible with one another, a bridge enables token and coin transfers, smart contracts, and data exchanges between the different sets of rules coded on multiple blockchains to permit access, enhance interoperability, and expand the reach of blockchains. Unfortunately, any transfer of assets to or from a blockchain may compromise the security of such assets during the transfer because some protection is lost when moving from the original blockchain and crossing a bridge. In some instances, cybercriminals have been able to hack and steal assets while they were being transferred across a bridge. For example, a hacker stole $100 million from Harmony's Horizon Bridge during a transfer when the assets were more vulnerable.

Central Bank Digital Currency (CBDC): A digital form of a government-issued currency that would be available to the general public and is not pegged to a physical commodity. CBDCs would be issued by central banks which support financial services for a government and its banking system, monetary policy, and issued currency. CBDCs are theoretically similar to stablecoins ("stablecoin" is defined in Part I of this series) but they would not be pegged to another currency, commodity, or financial instrument, and, unlike general cryptocurrencies which are decentralized, would be state issued, operated, and controlled.

Know Your Customer (KYC): A verification process used by financial institutions in the U.S. and other countries to confirm the identity of customers in order to, among other things, prevent money laundering, terrorism financing, and financial fraud. KYC may require proof of address or other identifying information. Crypto exchanges often use KYC to gain a better understanding of an individual's activities and determine whether their actions are legal. Many central exchanges (CEX) require KYC to admit new customers and may impose KYC to connect an individual to a cryptocurrency wallet.

Mining Contract: An agreement whereunder a miner is paid for their services in the form of mining power from computer hardware that is used to add new blocks to a blockchain ("mining" is defined in Part II of this series). Rather than the conventional scenario of any miner independently adding new blocks onto a blockchain via solving complicated algorithms to receive tokens or coins (as first practiced with Bitcoin), a mining contract permits a sponsor to hire a miner to add new blocks onto a blockchain so that the sponsor may passively receive tokens or coins without mining themselves. The advantages of using a mining contract include: (i) potentially earning money without personally mining blocks and maintaining adequate hardware and servers; (ii) avoiding electricity costs; and (iii) expanding the pool of investors involved in mining and blockchain by simplifying the entry into mining and making the process more accessible. Since the cost of certain cryptocurrencies is incredibly volatile, the return on investment may vary widely depending on the current value of the coins being mined and the maintenance costs and service fees under the mining contract.

–

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

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