CARTER LEDYARD

client advisory

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

January 23, 2023

2023 will be an exciting (at least, interesting) year for cybersecurity, data privacy, and crypto. Several state data privacy laws went into effect on January 1, 2023, momentum continues towards a federal data privacy law, and cybersecurity will continue to be a top concern for entities and individuals. In addition, crypto will continue to dominate the news, with likely regulatory developments in 2023 and the continued evolution of the crypto industry. With these tech-heavy issues appearing in the legal and business news cycle, we are launching a series of published terms and definitions will help non-techies navigate the terminology associated with this area.

This is the first installment of our glossary of tech terms so bookmark this and sign up here for alerts when we publish more!

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

Cybersecurity Terms

Chief Information Security Officer (CISO): A CISO is the executive responsible for an organization's information and data security. It is considered a best practice for companies and and organizations to have a CISO. The New York Department of Financial Services Cybersecurity Regulations require covered entities to appoint a CISO.

Digital Footprint: The digital information that a user's online activity leaves behind, often in the form of "metadata." The "footprint" might show a user's IP address, email address, mailing address, products purchased, websites visited, etc. This information is often tracked by websites, advertisers, and social media companies through cookies or pixel trackers. Network security specialists can sometimes identify hackers by their digital footprints left behind in a hacked network.

Encryption:	A mathematical function that protects information by making it unreadable by everyone except those with the key to decode the information.
Internet of Things (IoT):	The ability of everyday objects to connect to a network by unique identifiers to transfer and exchange data without human interaction. For example, household appliances such as refrigerators and televisions, heating and cooling systems and thermostats, lighting and electronics, medical and healthcare devices, manufacturing equipment, and transportation systems and vehicles have joined the Internet of Things.
Multi-factor Authentication (MFA):	A layered authentication approach which creates an extra step to verify the identity of a person who wants to gain access to servers and databases. It provides access only after presenting two or more proofs of identity, such as a username in combination with a password plus a text message or phone call pushed to the person's mobile device; which is often referred to as "something you know and something you have."
Phishing:	A form of social engineering that uses untargeted mass emails or other messages to request sensitive information from recipients or encourage them to visit a fake website to provide sensitive information. Sending messages or emails to specific individuals is referred to as "spear-phishing."
Social Engineering:	Manipulating people into carrying out specific actions, or divulging information, that is of use to an attacker.

Data Privacy Terms

*Note that some of the below terms may be defined in statutes or interpreted differently by the various data privacy laws and regulations.

Cross-context behavioral advertising:	The tracking of an individual's activities across websites, applications, and services to identify and present advertisements tailored to their behavior. May also be referred to as "targeted advertising."
Data Controller:	An individual or an entity that determines the purposes for collecting or using personal data and how that personal data is processed. The specific obligations and requirements of Data Controllers with respect to personal data differ in the context of various data privacy laws and regulations.
Data Deidentification:	The process of removing identifying information from personal data in a manner that prevents the data from revealing someone's identity. It is a tool that can be used to exempt organizations from obligations under data privacy laws and regulations that only apply to organizations that collect, process, or store personal information. Deidentification is sometimes accomplished through anonymization whereby data can never be re-identified. Notably, pseudonymization, unlike anonymization, removes or replaces personal identifiers such that de-identified data may be re-identified in combination with additional information.
Data Processing:	The collection, use, manipulation, storage, retrieval, or classification of personal data, especially electronically. Sometimes data processing is accomplished by a separate Data Processor who processes data under the control of and in accordance with a Data Controller's instructions. Most organizations process data in some way, and the specific obligations and requirements for processing personal data differ in the context of various data privacy laws and regulations.
Personal data:	Information (typically held electronically) about a particular person or that can be used to identify a person, generally including one's name, email address, home address, government identification number, account numbers, etc. May also be referred to as "personally identifiable information" or "personal information."
Unique identifier:	A unique identifier is a personal identification number, password, or other secure form of identity verification to represent a person's, entity's, or object's specific identity that is used by some agencies for privacy purposes or used for connection and interaction on a particular network. May also be referred to as unique personal identifier.

California Consumer Privacy Act (CCPA) & California Privacy Rights Act (CPRA):	The CCPA is the strictest of all state privacy laws and is intended to enhance privacy rights and consumer protection for residents of California, which became effective on January 1, 2020. The CPRA significantly amends and expands the CCPA, and it is sometimes referred to as "CCPA 2.0." The CPRA became effective on January 1, 2023. The CCPA and CPRA apply to for-profit entities that meet specific collection, processing, jurisdictional, and data volume or financial threshold requirements.
Colorado Privacy Act (CPA):	The CPA provides Colorado residents with certain consumer rights with respect to their personal data and imposes obligations and responsibilities on Data Controllers. Will become effective on July 1, 2023. The CPA applies to Data Controllers that meet specific jurisdictional and data volume threshold requirements.
Connecticut Data Privacy Act (CTDPA):	The CTDPA provides Connecticut residents with certain consumer rights with respect to their personal data and imposes obligations and responsibilities on businesses. Will become effective on July 1, 2023. The CTDPA applies to entities that meet specific jurisdictional and data volume and revenue threshold requirements.
Utah Consumer Privacy Act (UCPA):	The UCPA has the narrowest scope of all state privacy laws and provides Utah residents with certain consumer rights with respect to their personal data and imposes obligations and responsibilities on Data Controllers and Data Processors. Will become effective on December 31, 2023. The UCPA applies to Data Controllers and Data Processors that meet specific jurisdictional, financial, and data volume and revenue threshold requirements.
Virginia Consumer Data Privacy Act (VCDPA):	The VCDPA provides Virginia residents with certain consumer rights with respect to their personal data and imposes obligations and responsibilities on businesses. Became effective on January 1, 2023. The VCDPA applies to entities that meet specific jurisdictional and data volume and revenue threshold requirements.
General Data Protection Regulation (GDPR):	The GDPR was the first of its kind as a comprehensive data protection regulation, which became effective on May 25, 2018. It provides EU residents with certain consumer rights with respect to their personal data and imposes obligations and responsibilities on businesses located anywhere in the world that target or collect personal data from EU residents and the European Economic Area. An almost-identical version of the GDPR that protects UK residents became effective on January 1, 2021.

Crypto Terms

Cryptocurrency: A type of digital currency that is created and verified by cryptography and stored on a decentralized system via a blockchain-based peer-to-peer network. Examples include Bitcoin, Ethereum, Binance, and Tether. Cryptocurrency may also be used as an electronic asset in transactions as an alternative, virtual form of payment instead of a traditional currency controlled by a centralized government or financing authority, or as a store of value, in which ownership of the cryptocurrency is recognized by and transferred on decentralized ledger databases.

Bitcoin: The first cryptocurrency, launched on January 3, 2009. Sometimes referred to as "digital gold." As of January 13, 2:02pm ET, 1 Bitcoin = $19,293.20

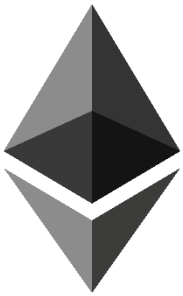
Blockchain: A distributed ledger supported by a decentralized, peer-to-peer shared network system that records transactions by using cryptography to add sequential "blocks" of information that are permanent and immutable because of their chain-like connection in which each block includes information from the previous block so that the blocks continuously build upon each other.

Decentralized Autonomous Organization (DAO): An organization (comparable to a corporation, partnership, or LLC) constructed and operated by rules encoded on a blockchain and collectively controlled by the organization's members rather than a central government or central management (typically ownership is represented by a virtual token). Legal personhood and other features of a DAO are subject to current conjecture and litigation.

Decentralized Finance (DeFi): Financial activities conducted without the involvement of an intermediary. It employs technology to remove third parties and centralized institutions from financial transactions.

Digital Wallet: Also referred to as Electronic Wallet---An electronic device, online service, or software program that enables an individual to make electronic transactions and/or store electronic documents.

Ethereum: Ethereum is a crypto network and software platform that developers can use to create new applications, and has an associated currency called Ether which is the second largest cryptocurrency by trade volume. As of January 13, at 2:03pm ET, 1 Ether = $1,416.26.



Non-Fungible Tokens (NFT): A digital, cryptographic asset that represents the ownership of a unique item by an authentic certificate that is constructed by and stored on blockchain technology underlying the cryptocurrency. NFTs cannot be substituted or replaced because their value is not interchangeable (unlike cryptocurrencies such as Bitcoin, which is a fungible commodity). NFTs can represent virtual collectibles such as digital music and games as well as physical objects such as tangible artwork.

Stablecoin: A type of cryptocurrency with a fixed price or market value because it is directly connected or pegged to an external source as a reference asset, such as fiat money, commodities, or other currencies (e.g., Tether, which is pegged to the U.S. dollar). Also known as a "digital fiat."