Metaverse Law:
Intro to ARVR, Issues, IP Ownerships, Monetization, Cyber Currency, and Licensing

Instructor:

Suzanne D. Meehle, Esq.
Meehle & Jay
1215 E. Concord Street
Orlando, FL 32803
(407) 792-0790
suzanne@meehle.com

ACROSS THE METAVERSE:
SOMETHING'S GONNA CHANGE YOUR WORLD

SUZANNE D. MEEHLE, ESQ.

Suzanne Meehle is the founder and managing shareholder of Meehle & Jay P.A. For over a decade, her practice has focused on the needs of small businesses and start-ups. She has a special affinity with technology services clients thanks to a 12-year career in the software industry before entering law school. To put it simply, she speaks geek. Her clients include app and game developers, AR/VR, biometrics, and engineering firms, and IT service providers.

WHAT IS THE METAVERSE ANYWAY?

met·a·verse

/ˈmedəˌvərs/

a virtual-reality space in which users can interact with a computer-generated environment and other users.

-Oxford English Dictionary

GLOSSARY (A-C)

Artificial Intelligence (AI): computer systems that can perform tasks that normally require human intelligence, comprehension and understanding.

Augmented Reality (AR): Technology that superimposes a computer-generated image on a user's view of the actual world, providing a composite view that often includes perceptual information.

Blockchain: A shared, immutable digital ledger that records and maintains transactions and tracks assets across a peer-to-peer business network in digital "blocks" where data is stored and encrypted.

Consensus Mechanism: A fault-tolerant process used in blockchain systems to obtain the necessary agreement on a single data value among distributed processes or multi-agent systems.

Creator Economy: A class of businesses made up of content creators, curators and community builders which enable the content producers to monetize their creations.

Cryptocurrency: A digital currency — designed to work as a medium of exchange — in which transactions are verified and records maintained by a decentralized computer network using cryptography, rather than going through a centralized, trusted authority. Ex.: Bitcoin, Ethereum, Dogecoin

Cryptography: The computerized practice of encoding and decoding information for secure communication.

Crypto Wallet: A physical or digital device, computer application or smartphone app that stores the public and/or private keys for cryptocurrency transactions, including sending, receiving, buying, selling, swapping of cryptocurrencies and NFTs and digitally signing information.

GLOSSARY (D)

Decentralization: The transfer of control and decision-making from a centralized, trusted authority (i.e., an individual, organization, group, government, etc.) to a distributed network.

Decentralized Applications (dApps): An application that can operate autonomously using smart contracts on a peer-to-peer network of computers or a decentralized computing, blockchain system.

Decentralized Autonomous Organization (DAO): A group or entity that is represented by rules that are controlled by its members and not influenced or controlled by a central government or power — all governance is done as part of a group or collective.

Decentralized Finance (DeFi): Enables peer-to-peer financial services without reliance on intermediaries such as brokerages, exchanges or banks through the use of smart contracts on a public blockchain.

Digital Twin: A virtual or 3D digital representation that is identical to the real-time version of a physical object or process.

Distributed Ledger: A ledger or database of replicated, shared and synchronized digital data that is maintained in a decentralized form that is spread across multiple sites, countries or institutions without using a central administrator.

Distributed Ledger Technology (DLT): The technological infrastructure and protocols, also known as blockchain technology, that enables simultaneous access, validation and record updating in an immutable manner across a geographically diverse network made up of multiple entities.

GLOSSARY (E-Ma)

Extended Reality (XR): An environment or experience that combines virtual and physical realities through the use of augmented reality (AR), mixed reality, virtual reality (VR) or any similar immersive technologies.

GameFi: An amalgam of the words gaming and decentralized finance (DeFi), GameFi refers to play-to-earn (P2E) games.

Gas: The fee that is charged for successfully conducting a transaction or executing a contract on a blockchain platform.

Haptics: technology that stimulates the senses of touch and motion, especially to reproduce in remote operation or computer simulation the sensations that would be felt by a user interacting directly with physical objects.

Hash or Hash Function: A mathematical one-way cryptographic algorithm that maps an input of arbitrary size to a unique output of a fixed length of bits.

Immersive Social: Enables users to explore and interact with 3D environments and collaborate with other users in a virtual space, all of which facilitates a richer, more compelling, personal way of sharing experiences and relating to one another.

InterPlanetary File System (IPFS): A protocol and distributed peer-to-peer network for storing and sharing data via a distributed file system.

Machine Intelligence: An umbrella term that describes the accuracy of a machine learning (ML), deep learning (DL) or classical algorithm output; also refers to artificial intelligence (AI).

Machine Learning (ML): A part of artificial intelligence; refers to algorithms that can improve automatically through experience and the use of data without human intervention.

GLOSSARY (Me-Pe)

Metaverse: The still-evolving concept of a 3D, virtual network with a focus on social connections. It is not Web3, but it is seen as a part of Web3, the concept of which is a hypothetical iteration of the internet as a single, unified virtual world that is accessed through VR or AR headsets.

Mixed Reality (MR): Mixed reality is the merging of physical and virtual worlds to produce new environments and visualizations, where physical and digital objects co-exist and interact in real-time; the key difference is between mixed reality and augmented reality is the user's ability to interact.

Non-Fungible Token (NFT): A non-interchangeable cryptographic unit of data with unique identification codes and metadata that distinguishes it from another. This form of digital ledger is stored on a blockchain and can be sold and traded. NFTs are typically associated with digital files, including videos, images and audio.

Open Platform: A platform based on open standards that allows developers to build applications or services that work on the platform. Also referred to as "Open Source" development.

Permissionless: Refers to permissionless or trustless blockchains, which are open networks that allow everyone to participate in the consensus process, which itself uses blockchains to validate transactions and data.

GLOSSARY (Pr-Sm)

Proof of Stake (PoS): A cryptocurrency consensus mechanism used for processing transactions, creating new blocks on a blockchain, validating entries into a distributed database and keeping the database secure.

Proof of Work (PoW): A cryptographic method of verifying and tracking the creation of new cryptocurrency and transactions that occur on a blockchain by measuring the amount of a specific computational effort expended.

Private Key: A digital, cryptographic key used to decrypt messages that are received from the sender who used a public key to encrypt it.

Public-Key Cryptography: A cryptographic technique that uses a paired public and private key algorithm for secure digital communication. The sender's public key encrypts the message, and the recipient's private key decrypts a message.

Public Key: A digital, cryptographic key that can be obtained and used to encrypt messages sent to a specific recipient who uses the private key to decrypt it.

Smart Asset: Unique virtual currency tokens that may represent a tangible physical asset (such as a car) or non-tangible ownership (crypto) that can be bought, sold or traded as defined by smart contracts that are on the blockchain network.

Smart Contract: A computer program or a transaction protocol that defines the terms of an agreement, with those terms being executed as code that is running on a blockchain; enables developers to create apps that utilize blockchain security, reliability and accessibility.

GLOSSARY (St-W)

Stablecoin: Cryptocurrencies that attempt to offer stability due to the price being backed by a cryptocurrency, fiat money or exchange-traded commodities.

State: A snapshot of a blockchain system at a specific point in time, which includes multiple aspects such as the order of transactions, amount per transaction and account balances.

Token: A digital currency token or a denomination of a cryptocurrency (such as Bitcoin or Ether coin) that represents a tradable asset or utility on its own blockchain and enables the holder to use it for investment or economic purposes.

Trustless: A core element of blockchain, crypto payments and smart contracts, trustless refers to the fact that transactions don't rely on trusting a third party such as a bank or other entity.

Virtual Currency: A digital representation of currency, typically cryptocurrencies, that can only exist in electronic form, can be accepted for goods and services and can be bought, sold and traded via cryptocurrency exchanges.

Virtual Economy: An emergent economy that exists in a digital virtual world, where virtual goods are bought, sold and exchanged using virtual currency in the context of an online game.

Virtual Reality (VR): A computer-generated simulation of a three-dimensional environment that can be interacted with by a person or group of people using special hardware, such as a set of electronic goggles, gloves, or haptic devices.

Web3 or Web 3.0: The third generation of online services for websites and applications with core concepts of blockchain-based decentralization, AR/VR-based immersive technologies and AI-based semantics, all of which facilitate transparent, ubiquitous, open, vibrant virtual experiences.

WORLD BUILDING

- Augmented = digital overlay on the "real" world
    - Theme parks
    - Games like Pokemon Go
    - Social Media (think Instagram filters)
    - Robotic Surgery

- Virtual = fully digital, immersive platform
    - Haptics to produce "real" sensation in gaming systems like PS5
    - Control of avatars with body motions
    - Simulation of fully 3D environments (esp. with VR goggles)

WHAT IT MEANS TO THE "REAL" WORLD

- Like it or not, you are online. You have a digital life whether or not you ever do anything to create it.

- Biometrics increasingly replacing or supplementing passwords. Your face is in the Cloud.

- Borderless banking and transactions are a thing. Increasingly, location is irrelevant.

- Remote work means international work. Anywhere there's an Internet connection.

- Merging of AR/VR and reality: You are the data
  - Online 24/7, mobile and connected
  - Web 3.0 means constant interaction
  - No longer *need* brick & mortar institutions
    - Schools
    - Churches
    - Libraries
    - Theaters
    - Banks
    - Law Firms

ISSUES RAISED: WHOSE LAW?

- State or Federal?
  - Most intellectual property issues are Federal
  - Most corporate issues are State
  - What is "Interstate Commerce" on the Internet?

- International Law?
  - Trademarks are a geographical patchwork
  - Patents are generally enforceable worldwide
  - No such thing as an "international copyright." Rights based on publication within borders.
  - What about privacy? GDPR, state laws, otherwise ▯▓▯♀▯
  - When transactions are "borderless," who determines jurisdiction for disputes?

ISSUES RAISED: WHAT IS "PROPERTY?"

- Who "owns" the Internet?

- Who's Intellectual property rights?

- Can you "own" virtual land in the Metaverse?

- How do you "own" cryptocurrency?

- How do you "own" NFT's and other intangible "assets"?

- Can you file a UCC-1 on ANY of it?

ISSUES RAISED: PRIVACY & SECURITY

- "Europe's comprehensive privacy law, General Data Protection Regulation (GDPR), requires companies to ask for some permissions to share data and gives individuals rights to access, delete, or control the use of that data. The United States, in contrast, doesn't have a singular law that covers the privacy of all types of data. Instead, it has a mix of laws that go by acronyms like HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA, designed to target only specific types of data in special (often outdated) circumstances." Thorin Klosowski, "The State of Consumer Data Privacy Laws in the US (And Why It Matters)," New York Times, Sept. 6, 2021.

- Ownership of Personally Identifiable Information
  - Usually, data belongs to the data aggregator.
  - In limited circumstances, you can control who has access to data about you. But you don't own it.
  - "Penumbra of Rights" line of cases that follow *Griswold v. Connecticut* potentially disappearing along with *Roe v. Wade*.

WHO REGULATES THE METAVERSE?

- Difficulty of governing

- Variety of statutory schemas

- Common law

- Contracts

U.S. LAWS: FEDERAL

- **Copyrights and Patents** are enshrined in Article III of the U.S. Constitution. **Trademarks** still follow common law.

- **Defend Trade Secrets Act (DTSA)** provides a cause of action for victims of trade secret theft where a trade secret (But only if the trade secret is related to a product or service used in interstate commerce).

- **Health Insurance Portability and Accountability Act** (HIPAA) covers only *communication* between patient and medical service providers and insurers.

- **Fair Credit Reporting Act (FCRA)** regulates information in individual's credit report, how the information is obtained, and who is allowed to see it.

- **Family Educational Rights and Privacy Act (FERPA)** gives parents, students, and other schools the right to inspect individual's education records maintained by a school.

- **Gramm-Leach-Bliley Act (GLBA)** requires loan services and financial advisors to explain how they share an individual's data (but not how they use it), as well as the customer's right to opt out.

- **Electronic Communications Privacy Act (ECPA)** restricts government wiretapping, but doesn't protect against law enforcement access of data stored on servers, in the cloud, and in search queries.

- **Children's Online Privacy Protection Rule (COPPA)** imposes certain limits on a company's data collection for children under 13 years old.

- **Video Privacy Protection Act (VPPA)** prevents the disclosure of VHS rental records (but says nothing about Netflix).

- **Federal Trade Commission Act (FTC Act)** empowers the FTC to go after an app or website that violates its own privacy policy. The FTC can also investigate violations of marketing language related to privacy.

U.S. LAWS: STATES

- 48 states, the USVI and Puerto Rico adopted **Uniform Trade Secrets Act (UTSA)**

  - Defines a trade secret as something used in business that (a) is not known or readily accessible by competitors, (b) has commercial value or that provides a competitive advantage in the marketplace, and (c) the owner of the information protects from disclosure through reasonable efforts to maintain its secrecy.

- Contracts and Business Organizations

  - Potentially the best way to determine jurisdiction is to create an entity and put all of your contracts in the same jurisdiction as the entity.

  - State-by-state whether public policy will follow your choice of laws provision, depending on the nature of the contract

- Only 15 sates with Data Privacy Regulations (Source: National Conference of State Legislatures, April 26, 2022)

  - **California, Colorado, Utah, and Virginia**— have comprehensive consumer data privacy laws.

  - **California, Nevada, and Vermont** — regulate data brokers and/or establish registry.

  - **Maine, Minnesota, and Nev**ada— laws regarding individual Internet privacy rights.

  - **California and Delaware**— laws regarding children's data privacy rights.

  - **California, Connecticut, Delaware, Nevada, Pennsylvania, and Oregon** — regulate online privacy practices.

  - **Connecticut, Colorado, Delaware, Hawaii, New York, and Tennessee** — regulate employee email privacy.

FOREIGN LAWS

EUROPEAN UNION

- **General Data Protection Regulation (EU GDPR)** – dominant privacy law worldwide
- Transatlantic Data Flow
    - U.S. entities doing business in the EU (or attracting visitors from there) are subject to GDPR
    - *Data Protection Commissioner v. Facebook Ireland Ltd.* (C-311/18) (a.k.a. *Schrems II*), July 16, 2020
        - EU and the US designed a GDPR-compliant data transfer mechanism for transferring personal data from the EU to the US: The EU-US Privacy Shield Framework which mandated the use of certain Standard Contractual Clauses (SCCs) .
        - Max Schrems petitioned the DPC over Facebook's transfer of personal data from its Ireland to the US, relying on SCC's to secure the data.
        - CJEU examined the validity of the EU-US Privacy Shield and held that the corresponding provisions of U.S. laws do not satisfy requirements of GDPR and declared the EU-US Privacy Shield Framework invalid.
        - Nonetheless, upheld the use of SCC's as a data transfer mechanism.
    - Hilarity ensued? We're still scrambling to manage cross-border compliance.

FOREIGN LAWS

ASIA AND PACIFIC (Source: *Asia Pacific Privacy Guide 2020-2021*, [Deloitte](#), December 2020.)

- Emergence of data privacy legislation

    - Recent proliferation of draft legislation regarding data privacy

    - Increase in consumer awareness due to data breaches

    - Australia, Hong Kong, Japan, Myanmar, New Zealand, South Korea, and Thailand, have comprehensive data privacy laws

    - Cambodia, China, and Sri Lanka introduced privacy legislation in 2020 in order to curb unauthorized access to personally-identifiable information (China's regulatory scheme is byzantine)

- Emergence of Biometrics for Security

    - Facial recognition at New Delhi and Bengaluru airports

- Increasingly trying to comply with GDPR

    - GDPR Article 45 – Same regulation U.S. used in establishing EU-US Privacy Shield Framework

    - If a government's cross-border privacy scheme is approved under Article 45, fewer restrictions on data transfer

    - Data transfer = TRADE in the Metaverse

FOREIGN LAWS

LATIN AMERICA/CARIBBEAN

- Most legislation does not comport with GDPR, patchwork of laws
- Brazil's General Personal Data Protection Law (LGPD) was modeled after GDPR
- Columbia, Argentina, Jamaica have data privacy laws

AFRICA/MIDDLE EAST

- Early data privacy legislation
- Israel, Benin, Kenya, Nigeria, South Africa have data privacy laws

EASTERN EUROPE

- Non-existent data privacy legislation
- Home of Hackers

CORPORATE GOVERNANCE AND DOA'S

- Corporations and other traditional business entities

- Decentralized Autonomous Organizations (DAO's)
  - Distributed computing means no single jurisdiction
  - Blockchain as contract
  - Open-source coding
  - Data mining and crypto mining

CONTRACTS IN THE METAVERSE

- "Four Corners"
  - Basic contract law principles still apply
  - Who are the parties?
  - Offer/acceptance/consideration
  - Construction against the drafter means obligation to do what you say
  - Watch your boilerplate!

- Formalities
  - Writing = Blockchain
  - Signature = Consensus Mechanism
  - Witness = Distributed Ledger
  - Notary = Hash

SPECIFIC USE CASES

- Entertainment
  - Gaming
  - Audiovisual works
  - Theme parks
- Healthcare
  - Robotic surgical training
  - Limb replacement
  - Virtual surgery
- Gamification
  - Finance
  - Exercise

- Scientific research
  - Outcome prediction/modeling
  - Astrophysics
- Augmented Education
  - STEM Education
  - Military/Defense/Security
  - Transport simulation
  - Factory simulation
- Retail
  - In-app sales
  - Virtual try-on

WHO OWNS THE METAVERSE?

"Property" rights in completely intangible spaces are de facto regarded as "intellectual property." But is that all?

INTELLECTUAL PROPERTY RIGHTS

Intangible digital assets are by their very nature intellectual property

- Copyrights – "fixed in a tangible medium"

- Patents – "novelty" and "utility" require that the invention acts on the "real world." Algorithms usually don't qualify.

- Trademarks – "use in interstate commerce"

- Trade Secrets – "reasonable measures" requirement

CONTRACTUAL RIGHTS

- Licenses and Assignments
- Works made for hire
- Collaboration agreements
- Terms of Use
- Privacy Policies
- "First Sale" Doctrine
- "Shareholder" Rights
- Royalty agreements

OTHER "PROPERTY" RIGHTS

- Non-fungible Tokens (NFT's)

- Digital media copies

- "Land" in digital space

- Cryptocurrency and virtual money

COMPETITION IN THE METAVERSE

- Antitrust Issues
  - *Epic Games, Inc. v. Apple Inc.*, 4:20-cv-05640-YGR (N.D. Cal. Sep. 10, 2021)
    - Found that Apple iOS ecosystem is not monopolistic, but that Apple's anti-steering restrictions are anticompetitive. (Also said that courts are ill-suited to micromanage Apple's business operations.)

- Cross border Competition
  - Protecting patents and trade secrets
  - Protecting copyrights
  - Defending trademarks

MONEY IN THE METAVERSE

It's not just Bitcoin and other cryptocurrency. Your financial data is out there (along with everyone else's). Every time you use a credit card, or online banking, or Zelle, you move money in the Metaverse.

MOVING MONEY IN THE METAVERSE

- Real-money trading ("RMT")
  - "Gold-farming" - selling digital assets from a virtual world for cash outside the MV
  - MMPOG in-game currency more stable than local currency in some jurisdictions (like Venezuela), making RMT preferred to coin of the realm
- Virtual Assets
  - Billions spent annually on digital assets with no tangible value
    - Case to watch: ***Doe v. Roblox Corp.*, 3:21-cv-03943-WHO (N.D. Cal. May 9, 2022)** Roblox sued under California's Unfair Competition Law by minor Pt. for fraudulent business practice of selling in-game currency to spend it on virtual items for their avatars and incentivizing its users-who are mostly minors- by periodically deleting some items without warning to induce users to buy more. MTD denied May 9, 2022.
  - Non-fungible Tokens (NFT's)
    - Case to watch: ***Playboy Enters. Int'l v. www.playboyrabbitars.app*, 21 Civ. 08932 (VM) (S.D.N.Y. Nov. 13, 2021)** Playboy sued to stop the counterfeiting of its trademarks in connection with the unauthorized sale of fake Playboy Rabbitars non-fungible tokens ("NFTs") that were identical versions of the Playboy trademark and are almost identical to Playboy's actual website selling authentic Rabbitar NFT's. TRO granted.

MORE MONEY IN THE METAVERSE

- Gamified Finance
  - Robinhood (stocks and crypto trading)
  - Coinbase (cryptotrading and gamified financial education)
  - Mynt (automatic budgeting; rewards for good behavior)
  - Credit Karma (credit score tracking; gamified credit score boosting)
  - Case to watch: ***In re Jan. 2021 Short Squeeze Trading Litig.*, 21-02989-MDL-ALTONAGA/Torres (S.D. Fla. Jan. 26, 2022)**
    In January 2021, scores of retail investors rushed to purchase stocks that hedge funds and institutional investors had bet would decline in value, causing a dramatic increase in those stocks' share prices. The mass rush to purchase these "meme stocks" led to a highly volatile securities trading market, with the prices of certain stocks varying wildly by the hour. Robinhood responded to SEC demands to suspend trading, and investors sued. Robinhood's MTD granted with prejudice, appeal to follow.

DATA MINING

- **Cryptocurrency Mining** - competitive process that verifies and adds new transactions to the blockchain for a cryptocurrency. Winner is rewarded with some cryptocurrency and/or transaction fees (cash).

  - *United States v. Harmon*, 474 F. Supp. 3d 76 (D.D.C. 2020)
    District Court of D.C. classified cryptocurrency exchanges as "money transmitting businesses" under 18 U.S.C. § 1960.

- **Decentralized Computing** – enables blockchain building across platforms

- **Knowledge Discovery in Databases (KDD)** – looks for patterns in massive data

- **Data Farming** – computational experiments to "grow" data (extrapolation), which is then analyzed

- **Blockchain** is the mechanism for securing these transactions, making them something less ephemeral

CREATOR ECONOMY

"With over 50 million creators by 2021, there is tremendous demand for content from independent artists and influencers on social media platforms, and experts believe the metaverse will allow creators to saturate markets and industries through new promotion opportunities for products and services." - *Metaverse and the Future of the Creator Economy*, Identity Review, April 4, 2022

- "Content Creator" market is over $104 billion, and 41% of creators earning $69,000 annually (or more), growing year to year. Source: "Five predictions for the creator economy in 2022," *Fast Company*, Dec. 29, 2021.
- Brand marketing is increasingly Influencer marketing
- Gen-Z shops on TikTok and Instagram

VENTURE CAPITAL IN THE METAVERSE

- Metaverse industries identified by PitchBook as "emerging" VC spaces:
  - Election technology
  - Climate technology
  - Space tourism
  - Carbon capture & removal
  - Neurotechnology
  - Digital freight brokerage
  - eVTOLs and air taxis

- Investors poured a record $1.3 billion into the Content Creator space in 2021.

WHAT'S NEXT IN THE METAVERSE?

Metaverse is just "Capitalism on Decentralized Land." Alessandro Bogliari, cofounder and CEO of Influencer Marketing Factory.

- Expect more decentralization
- Expect less-traditional business deals
  - Healthcare Consultant + Game Developer + Robots + Haptics = Surgical training program
  - Production Company + Content Creator + AR/VR Developer = Augmented reality escape room
  - Game Developer + Data Miner + Blockchain = Video game where players mine crypto
- Expect more negotiation over governing law and jurisdiction
- Expect global conformity to GDPR
- Expect security concerns to continue grow

1 **ACROSS THE METAVERSE:**
   SOMETHING'S GONNA CHANGE YOUR WORLD

2 **SUZANNE D. MEEHLE, ESQ.**

Suzanne Meehle is the founder and managing shareholder of Meehle & Jay P.A. For over a decade, her practice has focused on the needs of small businesses and start-ups. She has a special affinity with technology services clients thanks to a 12-year career in the software industry before entering law school. To put it simply, she speaks geek. Her clients include app and game developers, AR/VR, biometrics, and engineering firms, and IT service providers.

3 **WHAT IS THE METAVERSE ANYWAY?**

met·a·verse

/ˈmedəˌvərs/

a virtual-reality space in which users can interact with a computer-generated environment and other users.

-Oxford English Dictionary

4 **GLOSSARY (A-C)**

Artificial Intelligence (AI): computer systems that can perform tasks that normally require human intelligence, comprehension and understanding.

Augmented Reality (AR): Technology that superimposes a computer-generated image on a user's view of the actual world, providing a composite view that often includes perceptual information.

Blockchain: A shared, immutable digital ledger that records and maintains transactions and tracks assets across a peer-to-peer business network in digital "blocks" where data is stored and encrypted.

Consensus Mechanism: A fault-tolerant process used in blockchain systems to obtain the necessary agreement on a single data value among distributed processes or multi-agent systems.

Creator Economy: A class of businesses made up of content creators, curators and community builders which enable the content producers to monetize their creations.

Cryptocurrency: A digital currency — designed to work as a medium of exchange — in which transactions are verified and records maintained by a decentralized computer network using cryptography, rather than

going through a centralized, trusted authority. Ex.: Bitcoin, Ethereum, Dogecoin

Cryptography: The computerized practice of encoding and decoding information for secure communication.

Crypto Wallet: A physical or digital device, computer application or smartphone app that stores the public and/or private keys for cryptocurrency transactions, including sending, receiving, buying, selling, swapping of cryptocurrencies and NFTs and digitally signing information.

5 ☐ **GLOSSARY (D)**

Decentralization: The transfer of control and decision-making from a centralized, trusted authority (i.e., an individual, organization, group, government, etc.) to a distributed network.

Decentralized Applications (dApps): An application that can operate autonomously using smart contracts on a peer-to-peer network of computers or a decentralized computing, blockchain system.

Decentralized Autonomous Organization (DAO): A group or entity that is represented by rules that are controlled by its members and not influenced or controlled by a central government or power — all governance is done as part of a group or collective.

Decentralized Finance (DeFi): Enables peer-to-peer financial services without reliance on intermediaries such as brokerages, exchanges or banks through the use of smart contracts on a public blockchain.

Digital Twin: A virtual or 3D digital representation that is identical to the real-time version of a physical object or process.

Distributed Ledger: A ledger or database of replicated, shared and synchronized digital data that is maintained in a decentralized form that is spread across multiple sites, countries or institutions without using a central administrator.

Distributed Ledger Technology (DLT): The technological infrastructure and protocols, also known as blockchain technology, that enables simultaneous access, validation and record updating in an immutable manner across a geographically diverse network made up of multiple entities.

6 ☐ **GLOSSARY (E-Ma)**

Extended Reality (XR): An environment or experience that combines

virtual and physical realities through the use of augmented reality (AR), mixed reality, virtual reality (VR) or any similar immersive technologies.

GameFi: An amalgam of the words gaming and decentralized finance (DeFi), GameFi refers to play-to-earn (P2E) games.

Gas: The fee that is charged for successfully conducting a transaction or executing a contract on a blockchain platform.

Haptics: technology that stimulates the senses of touch and motion, especially to reproduce in remote operation or computer simulation the sensations that would be felt by a user interacting directly with physical objects.

Hash or Hash Function: A mathematical one-way cryptographic algorithm that maps an input of arbitrary size to a unique output of a fixed length of bits.

Immersive Social: Enables users to explore and interact with 3D environments and collaborate with other users in a virtual space, all of which facilitates a richer, more compelling, personal way of sharing experiences and relating to one another.

InterPlanetary File System (IPFS): A protocol and distributed peer-to-peer network for storing and sharing data via a distributed file system.

Machine Intelligence: An umbrella term that describes the accuracy of a machine learning (ML), deep learning (DL) or classical algorithm output; also refers to artificial intelligence (AI).

Machine Learning (ML): A part of artificial intelligence; refers to algorithms that can improve automatically through experience and the use of data without human intervention.

7 GLOSSARY (Me-Pe)

Metaverse: The still-evolving concept of a 3D, virtual network with a focus on social connections. It is not Web3, but it is seen as a part of Web3, the concept of which is a hypothetical iteration of the internet as a single, unified virtual world that is accessed through VR or AR headsets.

Mixed Reality (MR): Mixed reality is the merging of physical and virtual worlds to produce new environments and visualizations, where physical and digital objects co-exist and interact in real-time; the key difference is between mixed reality and augmented reality is the user's ability to interact.

Non-Fungible Token (NFT): A non-interchangeable cryptographic unit

of data with unique identification codes and metadata that distinguishes it from another. This form of digital ledger is stored on a blockchain and can be sold and traded. NFTs are typically associated with digital files, including videos, images and audio.

Open Platform: A platform based on open standards that allows developers to build applications or services that work on the platform. Also referred to as "Open Source" development.

Permissionless: Refers to permissionless or trustless blockchains, which are open networks that allow everyone to participate in the consensus process, which itself uses blockchains to validate transactions and data.

8 GLOSSARY (Pr-Sm)

Proof of Stake (PoS): A cryptocurrency consensus mechanism used for processing transactions, creating new blocks on a blockchain, validating entries into a distributed database and keeping the database secure.

Proof of Work (PoW): A cryptographic method of verifying and tracking the creation of new cryptocurrency and transactions that occur on a blockchain by measuring the amount of a specific computational effort expended.

Private Key: A digital, cryptographic key used to decrypt messages that are received from the sender who used a public key to encrypt it.

Public-Key Cryptography: A cryptographic technique that uses a paired public and private key algorithm for secure digital communication. The sender's public key encrypts the message, and the recipient's private key decrypts a message.

Public Key: A digital, cryptographic key that can be obtained and used to encrypt messages sent to a specific recipient who uses the private key to decrypt it.

Smart Asset: Unique virtual currency tokens that may represent a tangible physical asset (such as a car) or non-tangible ownership (crypto) that can be bought, sold or traded as defined by smart contracts that are on the blockchain network.

Smart Contract: A computer program or a transaction protocol that defines the terms of an agreement, with those terms being executed as code that is running on a blockchain; enables developers to create apps that utilize blockchain security, reliability and accessibility.

9 **GLOSSARY (St-W)**

Stablecoin: Cryptocurrencies that attempt to offer stability due to the price being backed by a cryptocurrency, fiat money or exchange-traded commodities.

State: A snapshot of a blockchain system at a specific point in time, which includes multiple aspects such as the order of transactions, amount per transaction and account balances.

Token: A digital currency token or a denomination of a cryptocurrency (such as Bitcoin or Ether coin) that represents a tradable asset or utility on its own blockchain and enables the holder to use it for investment or economic purposes.

Trustless: A core element of blockchain, crypto payments and smart contracts, trustless refers to the fact that transactions don't rely on trusting a third party such as a bank or other entity.

Virtual Currency: A digital representation of currency, typically cryptocurrencies, that can only exist in electronic form, can be accepted for goods and services and can be bought, sold and traded via cryptocurrency exchanges.

Virtual Economy: An emergent economy that exists in a digital virtual world, where virtual goods are bought, sold and exchanged using virtual currency in the context of an online game.

Virtual Reality (VR): A computer-generated simulation of a three-dimensional environment that can be interacted with by a person or group of people using special hardware, such as a set of electronic goggles, gloves, or haptic devices.

Web3 or Web 3.0: The third generation of online services for websites and applications with core concepts of blockchain-based decentralization, AR/VR-based immersive technologies and AI-based semantics, all of which facilitate transparent, ubiquitous, open, vibrant virtual experiences.

10 **WORLD BUILDING**

• Augmented = digital overlay on the "real" world
  • Theme parks
  • Games like Pokemon Go
  • Social Media (think Instagram filters)
  • Robotic Surgery
•

- Virtual = fully digital, immersive platform
  - Haptics to produce "real" sensation in gaming systems like PS5
  - Control of avatars with body motions
  - Simulation of fully 3D environments (esp. with VR goggles)
-

11   WHAT IT MEANS TO THE "REAL" WORLD

- Like it or not, you are online. You have a digital life whether or not you ever do anything to create it.
- Biometrics increasingly replacing or supplementing passwords. Your face is in the Cloud.
- Borderless banking and transactions are a thing. Increasingly, location is irrelevant.
- Remote work means international work. Anywhere there's an Internet connection.
- Merging of AR/VR and reality: You are the data
  - Online 24/7, mobile and connected
  - Web 3.0 means constant interaction
  - No longer *need* brick & mortar institutions
    - Schools
    - Churches
    - Libraries
    - Theaters
    - Banks
    - Law Firms
-
-

12   ISSUES RAISED: WHOSE LAW?

- State or Federal?
  - Most intellectual property issues are Federal
  - Most corporate issues are State
  - What is "Interstate Commerce" on the Internet?

- International Law?
  - Trademarks are a geographical patchwork
  - Patents are generally enforceable worldwide

- No such thing as an "international copyright." Rights based on publication within borders.
- What about privacy? GDPR, state laws, otherwise 🤷🏻‍♀️
- When transactions are "borderless," who determines jurisdiction for disputes?
-
-

13 ☐ **ISSUES RAISED: WHAT IS "PROPERTY?"**
- Who "owns" the Internet?
-
- Who's Intellectual property rights?
-
- Can you "own" virtual land in the Metaverse?
-
- How do you "own" cryptocurrency?
-
- How do you "own" NFT's and other intangible "assets"?
-
- Can you file a UCC-1 on ANY of it?
-
-

14 ☐ **ISSUES RAISED: PRIVACY & SECURITY**
- "Europe's comprehensive privacy law, General Data Protection Regulation (GDPR), requires companies to ask for some permissions to share data and gives individuals rights to access, delete, or control the use of that data. The United States, in contrast, doesn't have a singular law that covers the privacy of all types of data. Instead, it has a mix of laws that go by acronyms like HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA, designed to target only specific types of data in special (often outdated) circumstances." Thorin Klosowski, "The State of Consumer Data Privacy Laws in the US (And Why It Matters)," New York Times, Sept. 6, 2021.
-
- Ownership of Personally Identifiable Information
  - Usually, data belongs to the data aggregator.
  - In limited circumstances, you can control who has access to data

about you. But you don't own it.
- "Penumbra of Rights" line of cases that follow *Griswold v. Connecticut* potentially disappearing along with *Roe v. Wade*.

-
-
-

15 **WHO REGULATES THE METAVERSE?**
- Difficulty of governing
-
- Variety of statutory schemas
-
- Common law
-
- Contracts

16 **U.S. LAWS: FEDERAL**
- Copyrights and Patents are enshrined in Article III of the U.S. Constitution. Trademarks still follow common law.
- Defend Trade Secrets Act (DTSA) provides a cause of action for victims of trade secret theft where a trade secret (But only if the trade secret is related to a product or service used in interstate commerce).
- Health Insurance Portability and Accountability Act (HIPAA) covers only *communication* between patient and medical service providers and insurers.
- Fair Credit Reporting Act (FCRA) regulates information in individual's credit report, how the information is obtained, and who is allowed to see it.
- Family Educational Rights and Privacy Act (FERPA) gives parents, students, and other schools the right to inspect individual's education records maintained by a school.
- Gramm-Leach-Bliley Act (GLBA) requires loan services and financial advisors to explain how they share an individual's data (but not how they use it), as well as the customer's right to opt out.
- Electronic Communications Privacy Act (ECPA) restricts government

wiretapping, but doesn't protect against law enforcement access of data stored on servers, in the cloud, and in search queries.
- Children's Online Privacy Protection Rule (COPPA) imposes certain limits on a company's data collection for children under 13 years old.
- Video Privacy Protection Act (VPPA) prevents the disclosure of VHS rental records (but says nothing about Netflix).
- Federal Trade Commission Act (FTC Act) empowers the FTC to go after an app or website that violates its own privacy policy. The FTC can also investigate violations of marketing language related to privacy.
-

17 ☐ **U.S. LAWS: STATES**
- 48 states, the USVI and Puerto Rico adopted Uniform Trade Secrets Act (UTSA)
  - Defines a trade secret as something used in business that (a) is not known or readily accessible by competitors, (b) has commercial value or that provides a competitive advantage in the marketplace, and (c) the owner of the information protects from disclosure through reasonable efforts to maintain its secrecy.
  -
- Contracts and Business Organizations
  - Potentially the best way to determine jurisdiction is to create an entity and put all of your contracts in the same jurisdiction as the entity.
  - State-by-state whether public policy will follow your choice of laws provision, depending on the nature of the contract
    -
- Only 15 sates with Data Privacy Regulations (Source: National Conference of State Legislatures, April 26, 2022)
  - California, Colorado, Utah, and Virginia— have comprehensive consumer data privacy laws.
  - California, Nevada, and Vermont — regulate data brokers and/or establish registry.
  - Maine, Minnesota, and Nevada— laws regarding individual Internet privacy rights.
  - California and Delaware— laws regarding children's data privacy rights.

- California, Connecticut, Delaware, Nevada, Pennsylvania, and Oregon — regulate online privacy practices.
- Connecticut, Colorado, Delaware, Hawaii, New York, and Tennessee — regulate employee email privacy.
-
-
-

18 ☐ **FOREIGN LAWS**

EUROPEAN UNION

- General Data Protection Regulation (EU GDPR) – dominant privacy law worldwide
- Transatlantic Data Flow
  - U.S. entities doing business in the EU (or attracting visitors from there) are subject to GDPR
  - *Data Protection Commissioner v. Facebook Ireland Ltd.* (C-311/18) (a.k.a. *Schrems II*), July 16, 2020
    - EU and the US designed a GDPR-compliant data transfer mechanism for transferring personal data from the EU to the US: The EU-US Privacy Shield Framework which mandated the use of certain Standard Contractual Clauses (SCCs) .
    - Max Schrems petitioned the DPC over Facebook's transfer of personal data from its Ireland to the US, relying on SCC's to secure the data.
    - CJEU examined the validity of the EU-US Privacy Shield and held that the corresponding provisions of U.S. laws <u>do not satisfy requirements of GDPR</u> and declared the EU-US Privacy Shield Framework invalid.
    - Nonetheless, upheld the use of SCC's as a data transfer mechanism.
  - Hilarity ensued? We're still scrambling to manage cross-border compliance.
-
-
-

19 ☐ **FOREIGN LAWS**

ASIA AND PACIFIC (Source: *Asia Pacific Privacy Guide 2020-2021*,

- Emergence of data privacy legislation
  - Recent proliferation of draft legislation regarding data privacy
  - Increase in consumer awareness due to data breaches
  - Australia, Hong Kong, Japan, Myanmar, New Zealand, South Korea, and Thailand, have comprehensive data privacy laws
  - Cambodia, China, and Sri Lanka introduced privacy legislation in 2020 in order to curb unauthorized access to personally-identifiable information (China's regulatory scheme is byzantine)

- Emergence of Biometrics for Security
  - Facial recognition at New Delhi and Bengaluru airports
  -
- Increasingly trying to comply with GDPR
  - GDPR Article 45 – Same regulation U.S. used in establishing EU-US Privacy Shield Framework
  - If a government's cross-border privacy scheme is approved under Article 45, fewer restrictions on data transfer
  - Data transfer = TRADE in the Metaverse
-
-
-

20 ☐ FOREIGN LAWS
LATIN AMERICA/CARIBBEAN
- Most legislation does not comport with GDPR, patchwork of laws
- Brazil's General Personal Data Protection Law (LGPD) was modeled after GDPR
- Columbia, Argentina, Jamaica have data privacy laws

AFRICA/MIDDLE EAST
- Early data privacy legislation
- Israel, Benin, Kenya, Nigeria, South Africa have data privacy laws
-
EASTERN EUROPE
- Non-existent data privacy legislation
- Home of Hackers

-
-

21 ☐ CORPORATE GOVERNANCE AND DOA'S

- Corporations and other traditional business entities
-
- Decentralized Autonomous Organizations (DAO's)
  - Distributed computing means no single jurisdiction
  - Blockchain as contract
  - Open-source coding
  - Data mining and crypto mining
-
-
-
-
-

22 ☐ CONTRACTS IN THE METAVERSE

- "Four Corners"
  - Basic contract law principles still apply
  - Who are the parties?
  - Offer/acceptance/consideration
  - Construction against the drafter means obligation to do what you say
  - Watch your boilerplate!
-
- Formalities
  - Writing = Blockchain
  - Signature = Consensus Mechanism
  - Witness = Distributed Ledger
  - Notary = Hash

23 ☐ SPECIFIC USE CASES

- Entertainment
  - Gaming
  - Audiovisual works

- Theme parks
- Healthcare
  - Robotic surgical training
  - Limb replacement
  - Virtual surgery
- Gamification
  - Finance
  - Exercise

-
- Scientific research
  - Outcome prediction/modeling
  - Astrophysics
- Augmented Education
  - STEM Education
  - Military/Defense/Security
  - Transport simulation
  - Factory simulation
- Retail
  - In-app sales
  - Virtual try-on
-
-

24 ☐ WHO OWNS THE METAVERSE?

"Property" rights in completely intangible spaces are de facto regarded as "intellectual property." But is that all?

25 ☐ INTELLECTUAL PROPERTY RIGHTS

Intangible digital assets are by their very nature intellectual property

-
- Copyrights – "fixed in a tangible medium"
-
- Patents – "novelty" and "utility" require that the invention acts on the "real world." Algorithms usually don't qualify.

-
- Trademarks – "use in interstate commerce"
-
- Trade Secrets – "reasonable measures" requirement
-
-
-

26 ☐ CONTRACTUAL RIGHTS
- Licenses and Assignments
- Works made for hire
- Collaboration agreements
- Terms of Use
- Privacy Policies
- "First Sale" Doctrine
- "Shareholder" Rights
- Royalty agreements
-
-
-
-

27 ☐ OTHER "PROPERTY" RIGHTS
- Non-fungible Tokens (NFT's)
-
- Digital media copies
-
- "Land" in digital space
-
- Cryptocurrency and virtual money
-
-
-
-
-

28 ☐ COMPETITION IN THE METAVERSE

- Antitrust Issues
  - *Epic Games, Inc. v. Apple Inc.*, 4:20-cv-05640-YGR (N.D. Cal. Sep. 10, 2021)
    - Found that Apple iOS ecosystem is not monopolistic, but that Apple's anti-steering restrictions are anticompetitive. (Also said that courts are ill-suited to micromanage Apple's business operations.)
  -
- Cross border Competition
  - Protecting patents and trade secrets
  - Protecting copyrights
  - Defending trademarks

-
-
-

29 ☐ **MONEY IN THE METAVERSE**

It's not just Bitcoin and other cryptocurrency. Your financial data is out there (along with everyone else's). Every time you use a credit card, or online banking, or Zelle, you move money in the Metaverse.

30 ☐ **MOVING MONEY IN THE METAVERSE**
- Real-money trading ("RMT")
  - "Gold-farming" - selling digital assets from a virtual world for cash outside the MV
  - MMPOG in-game currency more stable than local currency in some jurisdictions (like Venezuela), making RMT preferred to coin of the realm
- Virtual Assets
  - Billions spent annually on digital assets with no tangible value
    - Case to watch: *Doe v. Roblox Corp.*, 3:21-cv-03943-WHO (N.D. Cal. May 9, 2022)
      Roblox sued under California's Unfair Competition Law by minor Pt. for fraudulent business practice of selling in-game currency to spend it on virtual items for their avatars and incentivizing its users-who are mostly minors- by periodically deleting some items without warning to induce users to buy more. MTD denied

May 9, 2022.
- Non-fungible Tokens (NFT's)
  - Case to watch: *Playboy Enters. Int'l v. www.playboyrabbitars.app*, 21 Civ. 08932 (VM) (S.D.N.Y. Nov. 13, 2021)
  Playboy sued to stop the counterfeiting of its trademarks in connection with the unauthorized sale of fake Playboy Rabbitars non-fungible tokens ("NFTs") that were identical versions of the Playboy trademark and are almost identical to Playboy's actual website selling authentic Rabbitar NFT's. TRO granted.

-

31 ☐ MORE MONEY IN THE METAVERSE

- Gamified Finance
  - Robinhood (stocks and crypto trading)
  - Coinbase (cryptotrading and gamified financial education)
  - Mynt (automatic budgeting; rewards for good behavior)
  - Credit Karma (credit score tracking; gamified credit score boosting)
  - Case to watch: *In re Jan. 2021 Short Squeeze Trading Litig.*, 21-02989-MDL-ALTONAGA/Torres (S.D. Fla. Jan. 26, 2022)
  In January 2021, scores of retail investors rushed to purchase stocks that hedge funds and institutional investors had bet would decline in value, causing a dramatic increase in those stocks' share prices. The mass rush to purchase these "meme stocks" led to a highly volatile securities trading market, with the prices of certain stocks varying wildly by the hour. Robinhood responded to SEC demands to suspend trading, and investors sued. Robinhood's MTD granted with prejudice, appeal to follow.

-

32 ☐ DATA MINING

- Cryptocurrency Mining - competitive process that verifies and adds new transactions to the blockchain for a cryptocurrency. Winner is rewarded with some cryptocurrency and/or transaction fees (cash).

  - *United States v. Harmon*, 474 F. Supp. 3d 76 (D.D.C. 2020)
  District Court of D.C. classified cryptocurrency exchanges as "money transmitting businesses" under 18 U.S.C. § 1960.

- Decentralized Computing – enables blockchain building across platforms
- Knowledge Discovery in Databases (KDD) – looks for patterns in massive data
- Data Farming – computational experiments to "grow" data (extrapolation), which is then analyzed
- Blockchain is the mechanism for securing these transactions, making them something less ephemeral
-

33 ☐ CREATOR ECONOMY

"With over 50 million creators by 2021, there is tremendous demand for content from independent artists and influencers on social media platforms, and experts believe the metaverse will allow creators to saturate markets and industries through new promotion opportunities for products and services." - *Metaverse and the Future of the Creator Economy*, Identity Review, April 4, 2022

- "Content Creator" market is over $104 billion, and 41% of creators earning $69,000 annually (or more), growing year to year. Source: "Five predictions for the creator economy in 2022," Fast Company, Dec. 29, 2021.
- Brand marketing is increasingly Influencer marketing
- Gen-Z shops on TikTok and Instagram
-

34 ☐ VENTURE CAPITAL IN THE METAVERSE

-
- Metaverse industries identified by PitchBook as "emerging" VC spaces:
  - Election technology
  - Climate technology
  - Space tourism

.
- Carbon capture & removal
- Neurotechnology
- Digital freight brokerage
- eVTOLs and air taxis

- Investors poured a record $1.3 billion into the Content Creator space in 2021.
-
-
-
-

35 ☐ WHAT'S NEXT IN THE METAVERSE?

Metaverse is just "Capitalism on Decentralized Land." Alessandro Bogliari, cofounder and CEO of Influencer Marketing Factory.

- Expect more decentralization
- Expect less-traditional business deals
  - Healthcare Consultant + Game Developer + Robots + Haptics = Surgical training program
  - Production Company + Content Creator + AR/VR Developer = Augmented reality escape room
  - Game Developer + Data Miner + Blockchain = Video game where players mine crypto
- Expect more negotiation over governing law and jurisdiction
- Expect global conformity to GDPR
- Expect security concerns to continue grow

-
-
-

36 ☐ QUESTIONS?

iapp

Global Comprehensive Privacy Law Mapping Chart

Comprehensive data protection laws exist across the globe. While each law is different, there are many commonalities in terms of the rights, obligations and enforcement provisions. The Westin Research Center has created this chart mapping several comprehensive data protection laws, including the laws in the U.S., to assist our members in understanding how data protection is being approached around the world.

Our intent is to add to this chart and update it as laws are amended and other laws come into force. As always, we appreciate input from our members. If you have comments about the mapping or believe additional information should be included, please share it with Cathy Cosgrove at ccosgrove@iapp.org.

Special thanks to Perry Cruz, Amit Gadhia, Dr. Julien C. Hounkpe, Anna Johnston, Louisa Meliqsetyan, Selin Ozbek Cittone, Yechiel Steinmetz, Kezia Talbot, Daimhin Warner, and former IAPP legal externs, including Seth Azubuike, Brynne Duvall, Sean Kellogg, Eduardo Monteverde, and Cheryl Saniuk-Heinig, for their contributions.

Last updated: April 2022
Note: *This tool is for informational purposes and is not legal advice. Whether a law includes a particular provision should always be verified via official sources.*

	Argentina	Armenia	Australia	Benin Republic
	Personal Data Protection Act*	Law On Personal Data Protection	Privacy Act 1988 / Australian Privacy Principles (included in Privacy Act) / Australian Privacy Principles Guidelines	Digital Code
INDIVIDUAL RIGHTS				
Right to access	Articles 4(6) and 14	Articles 15, 18(1 and 4) and 20(1 and 2)	APP 12	Article 437
Right to correct	Article 16	Articles 6, 15(2) and 21(2)	APP 13	Article 441
Right to delete	Articles 4(5) and 16	Article 15(2)	APP Guidelines, APP 13 (related to correcting inaccuracy)	Articles 441, 443 and 444
Right to portability				Article 438
Right to opt out of all or specific processing		Articles 9(3), 11(2), 12(2) and 21(6)	APP 7	Articles 390 and 440
Right to opt in for sensitive data processing	Articles 2 and 7*	Articles 12 and 13*	APP 3	Article 394
Age-based opt-in right		Article 9(9)		Article 446
Right not to be subject to fully automated decisions				Articles 401, 415 and 439
BUSINESS OBLIGATIONS				
Notice/transparency requirements	Articles 6 and 13	Articles 9(5-8) and 10	APPs 1 and 5	Articles 384, 403, 415, 416 and 418
Legal basis for processing		Article 8		Articles 383 and 389
Purpose limitation	Article 4(3)	Articles 4(2), 16, 18(2) and 19(1)	APP 6	Articles 383(3) and 424
Data minimization	Article 4(1), (7)	Articles 5, 18(2) and 19(1)	APP 3.1–3.2	Articles 383(4) and 424
Security requirements	Article 9	Article 19 and Government Decision on Biometric Personal Data*	APP 11	Articles 383 and 426
Privacy by design			APP Guidelines, APP 1, 1.3	Article 424
Processor/service provider requirements	Article 9 (security)	Article 14		Article 386
Prohibition on discrimination				Articles 393 and 401
Record keeping	Chapter IV (Articles 21–28) (for data files, registers, banks, etc.)		APP Guidelines, APP 1, 1.5	Article 435
Risk/impact assessments			Privacy Act 1988, 33D; APP Guidelines, APP 1, 1.7; Australian Government Agencies Privacy Code*	Article 428
Data breach notification*		Article 21(3 and 4)	Privacy Act 1988, Part IIIC	Article 427
Registration with authorities	Chapter IV (Articles 21–28) (for data files, registers, banks, etc.)	Article 23		Articles 405 and 406 (reporting obligation)
Data protection officer			Australian Government Agencies Privacy Code*	Articles 430–432
International data transfer restrictions	Article 12	Articles 26 and 27	APP 8	Articles 391 and 392
SCOPE				
Exemption for employee data		Section 16 of Labour Code	Privacy Act 1988, 7B(3)	
Nonprofits covered	Articles 1 and 2	Article 1(1)	Privacy Act 1988, 6C–6E / OAIC guidance	Article 380
Sectoral law carveouts		Article 1(2)		
State-level preemption				
ENFORCEMENT				
Independent enforcement authority	Agencia de Acceso a la Información Pública	Personal Data Protection Agency	Office of the Australian Information Commissioner	Autorité de Protection des Données à caractère Personnel
	Chapter V (Articles 29 and 30)	Articles 24 and 25	Privacy Act 1988, Part IV	Articles 462–490
Rulemaking authority	Chapter V (Articles 29 and 30)	National Assembly, RA Government, Personal Data Protection Agency	Privacy Act 1988, 100	Article 483
Fining authority	Article 31	Article 24; Article 189.17, Administrative Violations Code	Privacy Act 1988, Part III, 13G; Part IIIA; Part V, 46, 65–66, etc.	Articles 452-455, 459 and 483
Criminal penalties	Articles 31 and 32	Article 145, Criminal Code (medical privacy)	Privacy Act 1988, Part V, 46, 65 and 66; Part VIA, 80Q, etc.	Articles 460 and 461
Personal liability	Articles 31 and 32		Privacy Act 1988, 99A	Article 460
Private right of action	Articles 33–39	Articles 17 and 21		Articles 449–451

*Data breach notification: *Many countries and all 50 U.S. states have separate data breach notification laws. The term in this chart refers to a provision included in a comprehensive data protection law.*

*Argentina: *Morrison Foerster's privacy library has an English version of the PDPA. The law provides no person can be compelled to provide sensitive data, subject to certain exceptions.*

*Armenia: *The Law on Personal Data Protection has different categories of personal data, including "special category" personal data, "personal life data" and "biometric personal data." Armenia also has a decision regarding biometric personal data, RA Government Decision N 1175-N dated 15 October 2015 "On Defining Requirements for Material Carriers of Biometric Personal Data and Technologies for Storage of Such Data outside of Information Systems." The Armenian Constitution includes a right to privacy in Article 31.*

*Australia: *The Australian Government Agencies Privacy Code requires Australian government agencies subject to the Privacy Act to conduct written privacy impact assessments for "high privacy risk" projects and requires the appointment of a privacy officer(s) and privacy champion.*

iapp

Global Comprehensive Privacy Law Mapping Chart

Last updated: *April 2022*

Note: *This tool is for informational purposes and is not legal advice. Whether a law includes a particular provision should always be verified via official sources.*

		Brazil	Canada	China	Colombia
		General Data Protection Law	Personal Information Protection and Electronic Documents Act	Personal Information Protection Law	Law 1581/2012*
					Law 1266/2008
INDIVIDUAL RIGHTS	Right to access	Articles 6(IV) and 18(II)	Schedule 1, Principle 9	Articles 44 and 45	Articles 8 and 18, Law 1581; Article 7, Law 1266; Article 21, Decree 1377
	Right to correct	Article 18(III)	Schedule 1, Principle 9	Article 46	Articles 8 and 18, Law 1581; Article 7, Law 1266; Article 22, Decree 1377
	Right to delete	Article 18(VI)	Schedule 1, Principle 9 (related to correcting inaccuracy)	Article 47	Articles 8 and 18, Law 1581; Article 7, Law 1266; Article 22, Decree 1377
	Right to portability	Article 18(V)		Article 45	
	Right to opt out of all or specific processing		Schedule 1, Principle 3 (4.3.8)	Articles 15 and 44	Article 8(e), Law 1581
	Right to opt in for sensitive data processing	Article 11	See OPC Guidance, Principle 3	Article 29	Articles 5 and 6, Law 1581; Article 6, Decree 1377
	Age-based opt-in right	Article 14		Article 31	Article 7, Law 1581*; Article 12, Decree 1377
	Right not to be subject to fully automated decisions	Article 20		Articles 24 and 55	
BUSINESS OBLIGATIONS	Notice/transparency requirements	Article 10, Section 2	Schedule 1, Principles 2, 3 and 8	Articles 7, 17, 23 and 30	Articles 4(e) and 12, Law 1581; Articles 14–18, Decree 1377
	Legal basis for processing	Article 7	Schedule 1, Principle 4.3 (consent required)	Article 13	Article 9, Law 1281; Article 5, Decree 1377 (consent based)
	Purpose limitation	Article 6(I)	Schedule 1, Principle 4	Article 6	Article 4(b), Law 1581
	Data minimization	Article 6(III)	Schedule 1, Principle 4	Articles 6 and 19	Articles 4 and 11, Decree 1377
	Security requirements	Articles 6(VII) and 46–49	Schedule 1, Principle 7	Articles 9, 51 and 59	Articles 4(g), 17 and 18, Law 1581; Article 19, Decree 1377
	Privacy by design				
	Processor/service provider requirements	Articles 37, 39 and 40		Article 21	Articles 8, 12, 17 and 18, Law 1581
	Prohibition on discrimination	Article 6(IX)		Article 16	
	Record keeping	Article 37	Part 1, Division 1.1, Section 10.3	Articles 54–56	Articles 8, 17 and 18, Law 1581; Articles 8 and 26, Decree 1377
	Risk/impact assessments	Article 38		Articles 55 and 56	Articles 17, 18 and 25, Law 1581
	Data breach notification*	Article 48	Part 1, Division 1.1, Sections 10.1–10.3	Article 57	Articles 17 and 18, Law 1581
	Registration with authorities			Articles 52 and 53	Article 25, Law 1581 (databases)
	Data protection officer	Article 41	Schedule 1, Principle 1	Article 52	Article 23, Decree 1377 (person or area designated to assume the function of personal data protection)
	International data transfer restrictions	Article 33		Articles 38–43	Article 26, Law 1581; Articles 24 and 25, Decree 1377
SCOPE	Exemption for employee data		Part 1, Section 4(1)(b)*		
	Nonprofits covered	Article 3	Part 1, Section 4	Article 3	Article 2, Law 1581
	Sectoral law carveouts				
	State-level preemption		See OPC Guidance		
ENFORCEMENT	Independent enforcement authority	National Data Protection Authority	Office of the Privacy Commissioner	*	Superintendency of Industry and Commerce
		Articles 55-A–55-L	Part 1, Division 2		Articles 19–24, Law 1581
	Rulemaking authority	Article 55-J	Part 1, Division 4, Section 26	Article 62	Article 21, Law 1581
	Fining authority	Articles 52–54	Part 1, Division 4, Section 28	Article 66	Articles 23 and 24, Law 1581; Title VII, Law 1266
	Criminal penalties			Article 71	
	Personal liability			Article 66	Articles 23 and 24, Law 1581; Articles 18 and 19, Law 1266
	Private right of action	Articles 42–45	Part 1, Division 2, Sections 14–17	Articles 50, 69 and 70	Article 16, Law 1266; Decree 2591

Data breach notification: *Many countries and all 50 U.S. states have separate data breach notification laws. The term in this chart refers to a provision included in a comprehensive data protection law.*

Canada: *PIPEDA applies to employee information in organizations engaged in federal works, undertakings or businesses.*

China: *Several government departments are responsible for enforcement, including the Cyberspace Administration of China, Ministry of Industry and Information Technology, and Ministry of Public Security.*

Colombia: *In addition to the data protection laws, there are decrees and other documents with relevant data protection provisions, including Decree 1377/2013 and Decree 2591/1991. Law 1581/2012 prohibits the processing of personal data of children and adolescents.*

iapp

Global Comprehensive Privacy Law Mapping Chart

Last updated: *April 2022*

Note: *This tool is for informational purposes and is not legal advice. Whether a law includes a particular provision should always be verified via official sources.*

	European Union	Hong Kong	Israel	Kenya
	General Data Protection Regulation	Personal Data Privacy Ordinance* / Data Protection Principles (PDPO Schedule 1)	Protection of Privacy Law / Privacy Protection (Data Security) Regulations	The Data Protection Act, 2019 / The Data Protection Regulations, 2021*

INDIVIDUAL RIGHTS

	European Union	Hong Kong	Israel	Kenya
Right to access	Article 15	Part 5, Division 1, Section 18; DPP 6	Article 13	Section 26(b)
Right to correct	Article 16	Part 5, Division 2, Section 22	Article 14	Sections 26(d) and 40
Right to delete	Article 17	DPP 2 (related to correcting inaccuracy)	Articles 14 (related to correcting inaccuracy) and 17F(b) (direct mailing)	Section 26(e) (if false or misleading data) and 40 (limited)
Right to portability	Article 20			Section 38
Right to opt out of all or specific processing	Articles 7 and 21	Part 6A, Division 2, Section 35G		Sections 26(c), 32, 34 and 36
Right to opt in for sensitive data processing	Article 9			*
Age-based opt-in right	Article 8			Section 33
Right not to be subject to fully automated decisions	Article 22			Section 35

BUSINESS OBLIGATIONS

	European Union	Hong Kong	Israel	Kenya
Notice/transparency requirements	Article 12	DPPs 5 and 6	Article 11	Sections 25(b), (e) and 29
Legal basis for processing	Article 6	DPP 1	Article 1	Section 30
Purpose limitation	Article 5(1)(b)	DPPs 1 and 3	Articles 2(9) and 8(b)	Section 25(c)
Data minimization	Article 5(1)(c)	DPP 1	Article 2(c), Privacy Protection (Data Security) Regulations*	Sections 25(d) and 39
Security requirements	Article 32	DPP 4	Articles 17 and 17B; Privacy Protection (Data Security) Regulations	Sections 19(2)(e), 29(f), 41 and 42
Privacy by design	Article 25			Section 41
Processor/service provider requirements	Article 28	DPPs 2(3) and 4(2)	Articles 17 and 17A; Articles 15 and 19, Privacy Protection (Data Security) Regulations	Parts III and IV; Part IV, General Regulations
Prohibition on discrimination	Recital 71			
Record keeping	Article 30	Part 5, Division 3, Section 27	Articles 6(b), 10, 11, 15(a)(2)(d), 17, 18, and 19, Privacy Protection (Data Security) Regulations	Section 43(8) (data breach); General Regulation 19
Risk/impact assessments	Article 35		Article 5(c), Privacy Protection (Data Security) Regulations	Section 31; Part VIII, General Regulations
Data breach notification*	Article 33 / Article 34		Article 11(d), Privacy Protection (Data Security) Regulations	Section 43; Part VI, General Regulations
Registration with authorities	Article 37(7)	Part 4, Section 15	Article 8(a)(1) (databases)	Sections 18-22; Registration of Data Controllers and Data Processors Regulations
Data protection officer	Article 37		Article 17B (security supervisor)*	Section 24 (optional)
International data transfer restrictions	Articles 44–50	Part 6, Section 33 (not yet in operation)	Privacy Protection (Transfer of Data to Databases Abroad) Regulations	Sections 25(h) and Part VI; Part VII, General Regulations

SCOPE

	European Union	Hong Kong	Israel	Kenya
Exemption for employee data		Part 8, Sections 53 and 54		
Nonprofits covered	Article 2	Part 1, Section 2	Article 1; Article 4 of the Interpretation Law	Section 4
Sectoral law carveouts	Article 6(2)		Article 13(c)(3)	
State-level preemption	Recital 10			

ENFORCEMENT

	European Union	Hong Kong	Israel	Kenya
Independent enforcement authority	EU national data protection authorities / Articles 51–59	Office of the Privacy Commissioner for Personal Data / Part 2, Section 5	Privacy Protection Authority / Articles 9, 10, 10A, and 12 (database registration); Articles 11(d) and 20, Privacy Protection (Data Security) Regulations	Office of the Data Protection Commissioner / Sections 5-17
Rulemaking authority	Articles 64, 65(1)(c) and 92	Part 3, Section 12	Article 36; the Privacy Protection Authority	Sections 5, 8, 9 and 74
Fining authority	Article 83	Part 7, Sections 35C, 50A, 64, etc.	Privacy Protection Authority	Sections 9(1)(f) and 63
Criminal penalties		Numerous provisions	Articles 5, 6, 16, 29A, 30, 31A and 31	Section 73
Personal liability		Director convicted under PDPO	Articles 4, 17, 17B(b), 30, 31A, 31B and 31	
Private right of action	Article 79	Part 9, Section 66	Articles 4, 15, 17F(e), 30, 31B and 31	Section 65

*Data breach notification: *Many countries and all 50 U.S. states have separate data breach notification laws. The term in this chart refers to a provision included in a comprehensive data protection law.*

*Hong Kong: *The Personal Data (Privacy) (Amendment) Ordinance 2021 focused on combating doxxing acts took effect Oct. 8, 2021.*

*Israel: *As with most countries, there are other laws in Israel that may be relevant to data privacy, including the Basic Law: Human Dignity and Liberty that provides all persons the right to privacy (Article 7) and Communications Law (Bezeq and Transmissions) (Amendment No. 72), 2018. The PPA has publications on topics like data minimization, cross-border transfers and the appointment of data protection officers.*

*Kenya: *The Data Protection Regulations include general regulations, regulations regarding complaints handling and enforcement procedures, and regulations regarding registration of data controllers and data processors. Kenya limits the grounds for processing sensitive personal data (Sections 44 and 45) and personal data relating to the health of a data subject (Section 46).*

iapp

Global Comprehensive Privacy Law Mapping Chart

Last updated: *April 2022*

Note: *This tool is for informational purposes and is not legal advice. Whether a law includes a particular provision should always be verified via official sources.*

	New Zealand	Nigeria	Philippines	Singapore
	Privacy Act 2020	Nigeria Data Protection Regulation	Data Privacy Act of 2012 (R.A. 10173)*	
	Information Privacy Principles (Part 3, Subpart 1 of the Privacy Act)	Nigeria Data Protection Regulation Implementation Framework	Implementing Rules and Regulations of the Data Privacy Act of 2012	Personal Data Protection Act
	Codes of practice			

INDIVIDUAL RIGHTS

	New Zealand	Nigeria	Philippines	Singapore
Right to access	IPP 6; Part 4, Subpart 1	Paragraph 3.1 (6) and (14)	Section 16(c); IRR, Rule VIII, Section 34(c)	Section 21
Right to correct	IPP 7; Part 4, Subpart 2	Paragraph 3.1(7)(h)	Section 16(d); IRR, Rule VIII, Section 34(d)	Section 22
Right to delete	IPP 7; Section 7(1); Part 4, Subpart 2 (related to correcting inaccuracy)	Paragraph 3.1(9)	Section 16(e); IRR, Rule VIII, Section 34(e) (certain circumstances)	Section 25 (obligation limiting retention)
Right to portability		Paragraph 3.1(14) and (15)	Section 18; IRR, Rule VIII, Section 36	Sections 26F–26J*
Right to opt out of all or specific processing		Paragraphs 2.3(c) and 3.1(11)	IRR, Rule VIII, Section 34(b)	Section 16
Right to opt in for sensitive data processing		NDPR Framework, Articles 5.3.2 and 5.4*	Section 13; IRR, Rule V, Section 22	
Age-based opt-in right		NDPR Framework, Articles 5.3.1(d), 5.4 and 5.5*	*	*
Right not to be subject to fully automated decisions		Paragraph 3.1(7)(L); NDPR Framework, Articles 3.2 (xvi) and 5.3.1(f)	Section 16(c)(6); IRR, Rule VIII, Section 34(b)	

BUSINESS OBLIGATIONS

	New Zealand	Nigeria	Philippines	Singapore
Notice/transparency requirements	IPP 3	Paragraphs 2.5, 3.1(1) and (7); NDPR Framework, Annex B (Privacy Policy Template)	Sections 11 and 16(a) and (b); IRR, Rule IV, Section 18(a) and Rule VIII, Section 34(a)	Sections 12(d) and 20
Legal basis for processing	IPPs 10 and 11 (post-collection)	Paragraph 2.2	Section 12; IRR, Rule V	Section 13 (consent required)
Purpose limitation	IPP 10	Paragraphs 2.1(1)(a) and 3.1(7)(m); NDPR Framework, Article 4.1	Sections 11 and 12; IRR, Rule IV, Sections 18 and 19.	Sections 18 and 20
Data minimization	IPPs 1 and 9 (storage limitation)	NDPR Framework, Annex A (Audit Template), No. 4.6	Sections 11(d) and (e); IRR, Rule IV, Section 19(d) and Rule VI, Section 26(e)	Section 14(2)(a)
Security requirements	IPP 5	Paragraphs 2.1(1)(d) and 2.6; NDPR Framework, Article 3.2(v)	Chapters V and VII; IRR, Rules VI and VII	Section 24
Privacy by design				
Processor/service provider requirements	IPP 5; Section 11	Paragraph 2.7; NDPR Framework, Article 3.2	Sections 14, 20(d) and 21; IRR, Rule VI, Section 26(f) and Rule X	Section 4(2)
Prohibition on discrimination				
Record keeping		NDPR Framework, Annex A (Audit Template), No. 3.1	IRR, Rule VI, Section 26(c)	Section 22A
Risk/impact assessments		Paragraph 4.1(5)-(7) (audit requirement); NDPR Framework, Articles 3.2(viii) and 4.2 (data protection impact assessment)	Section 20(c); IRR, Rule VI, Section 29; NPC Advisory No. 2017-03, Guidelines on Privacy Impact Assessments	*
Data breach notification*	Part 6, Subpart 1	NDPR Framework, Articles 3.2(ix) and 9	Section 20(f); IRR, Rule IX	Sections 26A–26E
Registration with authorities			IRR, Rule XI; NPC Circular 17-01	Section 11(5)*
Data protection officer	Section 201	Paragraph 4.1(2); NDPR Article 3.4-3.7	Section 21(b); IRR, Rule VI, Section 26(a) and Rule XII, Section 50(b)	Section 11
International data transfer restrictions	IPP 12; Part 8	Paragraphs 2.11-12 and 3.1(8); NDPR Framework, Articles 7 and 14	Section 21; IRR, Rule XII	Section 26

SCOPE

	New Zealand	Nigeria	Philippines	Singapore
Exemption for employee data			Section 4 (limited to government officers, employees and contractors)	First Schedule, Part 3 Legitimate Interests, Section 10
Nonprofits covered	Section 8	Paragraph 1.2; NDPR Framework, Article 2.1	Section 4	Section 4
Sectoral law carveouts	Sections 24 and 28		Section 4	Section 4(6)(b)
State-level preemption				

ENFORCEMENT

	New Zealand	Nigeria	Philippines	Singapore
Independent enforcement authority	Office of the Privacy Commissioner	Nigeria Data Protection Bureau*	National Privacy Commission	Personal Data Protection Commission
	Part 2	Paragraph 4.2; NDPR Framework, Article 10	Chapter II; IRR, Rule III	Sections 5–10
Rulemaking authority	Part 3, Subpart 2	Preamble to NDPR	Chapter II; IRR, Rule III	Section 65
Fining authority		Paragraph 2.10; NDPR Framework, Article 10.1.4	Sections 7(i); IRR, Rule III, Section 9(f)	Sections 48C–48F, 48J–48K, 51–52A and 56
Criminal penalties	Sections 104, 118, 197 and 212	Paragraph 2.10; NDPR Framework, Article 10.1.5	Chapter VIII; IRR, Rule XII, Section 51 and Rule XIII	Sections 48C–48F, 51–52A and 56
Personal liability	Sections 12, 27, 119, 120, and 211		Chapter VIII; IRR, Rule XII, Section 51 and Rule XIII	Sections 48C–48F, 48J–48K, 51–52A, 56 and 60
Private right of action	Section 31		Section 16(f); IRR, Rule VIII, Section 34(f) and Rule XII, Section 51	Section 48O

__Data breach notification:__ Many countries and all 50 U.S. states have separate data breach notification laws. The term in this chart refers to a provision included in a comprehensive data protection law.

__Nigeria:__ Explicit consent is required for the processing of sensitive personal data. Consent is required for the processing of the personal data of a minor. A child is defined as any person under 13. The National Information Technology Development Agency issued the NDPR and was the main regulator. In February 2022, the government of Nigeria created the NDPB to oversee implementation of the NDPR.

__Philippines:__ The NPC has issued a number of guidance documents regarding the interpretation of the DPA and the IRR that may be informative. For example, in Advisory Opinion No. 2017-49, the NPC stated "a minor cannot validly provide the consent as defined under the DPA."

__Singapore:__ Amendments to the PDPA not yet in effect will create a right of portability and increase potential financial penalties. The PDPC has issued Advisory Guidelines on various topics, including data activities related to minors and data protection impact assessments. There is no DPO registration requirement but the law does require DPO contact details be made public.

iapp

Global Comprehensive Privacy Law Mapping Chart

Last updated: *April 2022*

Note: *This tool is for informational purposes and is not legal advice. Whether a law includes a particular provision should always be verified via official sources.*

		South Africa	South Korea	Turkey
		Protection of Personal Information Act Regulations Relating to the Protection of Personal Information	Personal Information Protection Act	Law on the Protection of Personal Data
INDIVIDUAL RIGHTS	Right to access	Sections 5(b), 23 and 25*	Articles 4 and 35	Chapter 3, Article 11
	Right to correct	Sections 5(c) and 24; Regulation 3	Articles 4 and 36	Chapter 3, Article 11
	Right to delete	Sections 5(c) and 24; Regulation 3	Articles 4 and 36	Chapter 2, Article 7; Chapter 3, Article 11 (limited)
	Right to portability			
	Right to opt out of all or specific processing	Sections 5(d)-(e) and 11(3)-(4)	Articles 4 and 37	
	Right to opt in for sensitive data processing	Sections 26–33 ("special personal information")	Article 23	Chapter 2, Article 6
	Age-based opt-in right	Sections 34 and 35	Article 22(6)	
	Right not to be subject to fully automated decisions	Sections 5(g) and 71		Chapter 3, Article 11(1)(g)
BUSINESS OBLIGATIONS	Notice/transparency requirements	Sections 5(a) and 18	Articles 3, 4 and 30	Chapter 3, Article 10(1)
	Legal basis for processing	Sections 4, 9 and 11	Articles 3 and 15	Chapter 2, Articles 4–6
	Purpose limitation	Sections 13 and 15	Articles 3, 15, 18 and 19	Chapter 2, Article 4(2)(c)
	Data minimization	Sections 10, 14 and 16	Article 16(1)	Chapter 2, Article 4(2)(ç) and (d)
	Security requirements	Sections 19–21	Article 29	Chapter 3, Article 12
	Privacy by design			
	Processor/service provider requirements	Sections 20 and 21 (security)	Articles 19 and 26	Chapter 3, Article 12
	Prohibition on discrimination			
	Record keeping	Sections 14 and 17	Article 29	Chapter 4, Article 16
	Risk/impact assessments	Regulation 4(b)	Article 33	
	Data breach notification*	Section 22	Article 34	Chapter 3, Article 12(5)
	Registration with authorities	Sections 55 (for Information Officers) and 58 (certain processing); Guidance Note on Application for Prior Authorisation*	Article 32	Chapter 4, Article 16
	Data protection officer	Sections 55 and 56; Regulation 4; Guidance Note on Information Officers and Deputy Information Officers*	Article 31	
	International data transfer restrictions	Section 57(1),(d) and 72	Articles 14(2), 17(3), 39-12 and 39-13	Chapter 2, Article 9
SCOPE	Exemption for employee data	Section 32(1)(f)		
	Nonprofits covered	Section 3	Article 58	Chapter 1, Article 2
	Sectoral law carveouts		Article 6	Chapter 7, Article 28
	State-level preemption			Chapter 7, Article 28
ENFORCEMENT	Independent enforcement authority	Information Regulator Sections 39–54	Personal Information Protection Commission Article 7	Personal Data Protection Authority Chapter 6, Articles 19 and 20
	Rulemaking authority	Sections 40(1)(f), 60-68 and 112(2)	Articles 7-8 and 7-9	Chapter 6, Article 22
	Fining authority	Section 109	Articles 70–76	Chapter 5, Article 18; Chapter 6, Article 22
	Criminal penalties	Section 107	Articles 70–73	Chapter 5, Article 17
	Personal liability	Section 93(b)(ii) (Information Officers); Guidance Note on Information Officers and Deputy Information Officers*	Articles 70–76	Chapter 5, Article 18
	Private right of action	Section 99	Articles 51–57	Chapter 3, Article 11(1)(ğ)

*Data breach notification: *Many countries and all 50 U.S. states have separate data breach notification laws. The term in this chart refers to a provision included in a comprehensive data protection law.*

*South Africa: *Access to personal informatiom is further regulated by the Promotion of Access to Information Act No. 2 of 2000. Guidelines, guidance notes and notices from the Information Regulator can be found here.*

Global Comprehensive Privacy Law Mapping Chart

	United States				
	California		**Colorado**	**Utah**	**Virginia**
	California Consumer Privacy Act / California Consumer Privacy Act Regulations	California Privacy Rights Act (fully operative Jan. 1, 2023)	Colorado Privacy Act* (effective July 1, 2023)	Utah Consumer Privacy Act (effective Dec. 31, 2023)	Virginia's Consumer Data Protection Act (effective Jan. 1, 2023)
INDIVIDUAL RIGHTS					
Right to access	Section 1798.100, Section 1798.110, Section 1798.115	Section 1798.100, Section 1798.110, Section 1798.115	Section 6-1-1306(1)(b)	Section 13-61-201(1)	Section 59.1-577(A)(1)
Right to correct		Section 1798.106	Section 6-1-1306(1)(c)		Section 59.1-577(A)(2)
Right to delete	Section 1798.105	Section 1798.105	Section 6-1-1306(1)(d)	Section 13-61-201(2)	Section 59.1-577(A)(3)
Right to portability	Sections 1798.100(d) and 1798.130(a)(2)	Section 1798.130(a)(3)(B)(iii)	Section 6-1-1306(1)(e)	Section 13-61-201(3)	Section 59.1-577(A)(4)
Right to opt out of all or specific processing	Section 1798.120	Section 1798.120	Section 6-1-1306(1)(a)	Section 13-61-201(4)	Section 59.1-577(A)(5)
Right to opt in for sensitive data processing		Section 1798.121*	Section 6-1-1308(7)	Section 16-61-302(3)(a) (notice and opportunity to opt-out)	Section 59.1-578(A)(5)
Age-based opt-in right	Section 1798.120(c)	Section 1798.120(c)	Section 6-1-1308(7)	Section 13-61-302(3)(b) (process in accordance with the Children's Online Privacy Protection Act))	Section 59.1-578(A)(5) (process in accordance with the Children's Online Privacy Protection Act)
Right not to be subject to fully automated decisions		Section 1798.185(a)(16)*	Section 6-1-1306(1)(a)(I)(C)		Section 59.1-577(A)(5)
BUSINESS OBLIGATIONS					
Notice/transparency requirements	Section 1798.100(b), Sections 1798.130(a) and 1798.135	Section 1798.100(a), Section 1798.130	Section 6-1-1308(1)	Section 13-61-302(1)	Section 59.1-578(C)-(E)
Legal basis for processing					
Purpose limitation	Section 1798.100(b)	Section 1798.100(c)	Section 6-1-1308(2), (4)		Section 59.1-578(A)(2)
Data minimization		Sections 1798.100(c) and 1798.100(a)(d)	Section 6-1-1308(3)		Section 59.1-578(A)(1)
Security requirements	Section 1798.150(a)	Sections 1798.100(e) and 1798.150(a)	Section 6-1-1308(5)	Section 13-61-302(2)	Section 59.1-578(A)(3)
Privacy by design					
Processor/service provider requirements	Section 1798.140(v)	Sections 1798.100(d) and 1798.140(ag)(1)	Section 6-1-1305	Section 13-61-301	Section 59.1-579
Prohibition on discrimination	Section 1798.125	Section 1798.125	Section 6-1-1308(6)	Section 13-61-302(4)	Section 59.1-578(A)(4)
Record keeping	CCPA Regulations, Section 999.317				
Risk/impact assessments		Section 1798.185(a)(15)	Section 6-1-1309		Section 59.1-580
Data breach notification*					
Registration with authorities					
Data protection officer					
International data transfer restrictions					
SCOPE					
Exemption for employee data	Section 1798.145(m) from CPRA operative immediately until Jan. 1, 2023		Section 6-1-1304(2)(k) (employment records)*	Section 13-61-102(2)(o)*	Section 59.1-576(C)(14)*
Nonprofits covered			Section 6-1-1304		
Sectoral law carveouts	Sections 1798.145 and 1798.146	Sections 1798.145 and 1798.146	Section 6-1-1304(2)	Section 13-61-102(2)	Section 59.1-576
Preemption	Section 1798.180	Section 1798.180	Section 6-1-1312	Section 13-61-103(1)	
ENFORCEMENT					
Independent enforcement authority		California Privacy Protection Agency* Section 1798.199.10 et seq.			
Rulemaking authority	Section 1798.185	Section 1798.185	Section 6-1-1313		
Fining authority	Section 1798.155	Sections 1798.155, 1798.199.55 and 1798.199.90	Section 6-1-1311	Section 13-61-402	Section 59.1-584
Criminal penalties					
Personal liability					
Private right of action	Section 1798.150	Section 1798.150			

*Data breach notification: *Many countries and all 50 U.S. states have separate data breach notification laws. The term in this chart refers to a provision included in a comprehensive data protection law.*

*California: *The CPRA categorizes sensitive data and allows consumers to limit its use and disclosure but does not require opt-in consent for use of sensitive data. There is no explicit right against automatic decision-making but the use of automatic decision-making is within the scope of the regulations to be promulgated. The CPPA has administrative authority to implement and enforce the CPRA. The California attorney general's office retains civil enforcement authority.*

*Colorado: *The CPA is now codified in the Colorado Revised Statutes. The definition of "consumer" in Section 6-1-1303(6)(b) "does not include an individual acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context."*

*Utah: *In addition to the exemption for data processed in the employment context, the definition of "consumer" in Section 13-61-101(10)(b) "does not include an individual acting in an employment or commercial context."*

*Virginia: *The definition of "consumer" in Section 59.1-575 "does not include a natural person acting in a commercial or employment context."*