Decentralized Authentication and Biometrics

November 4, 2022

withersworldwide

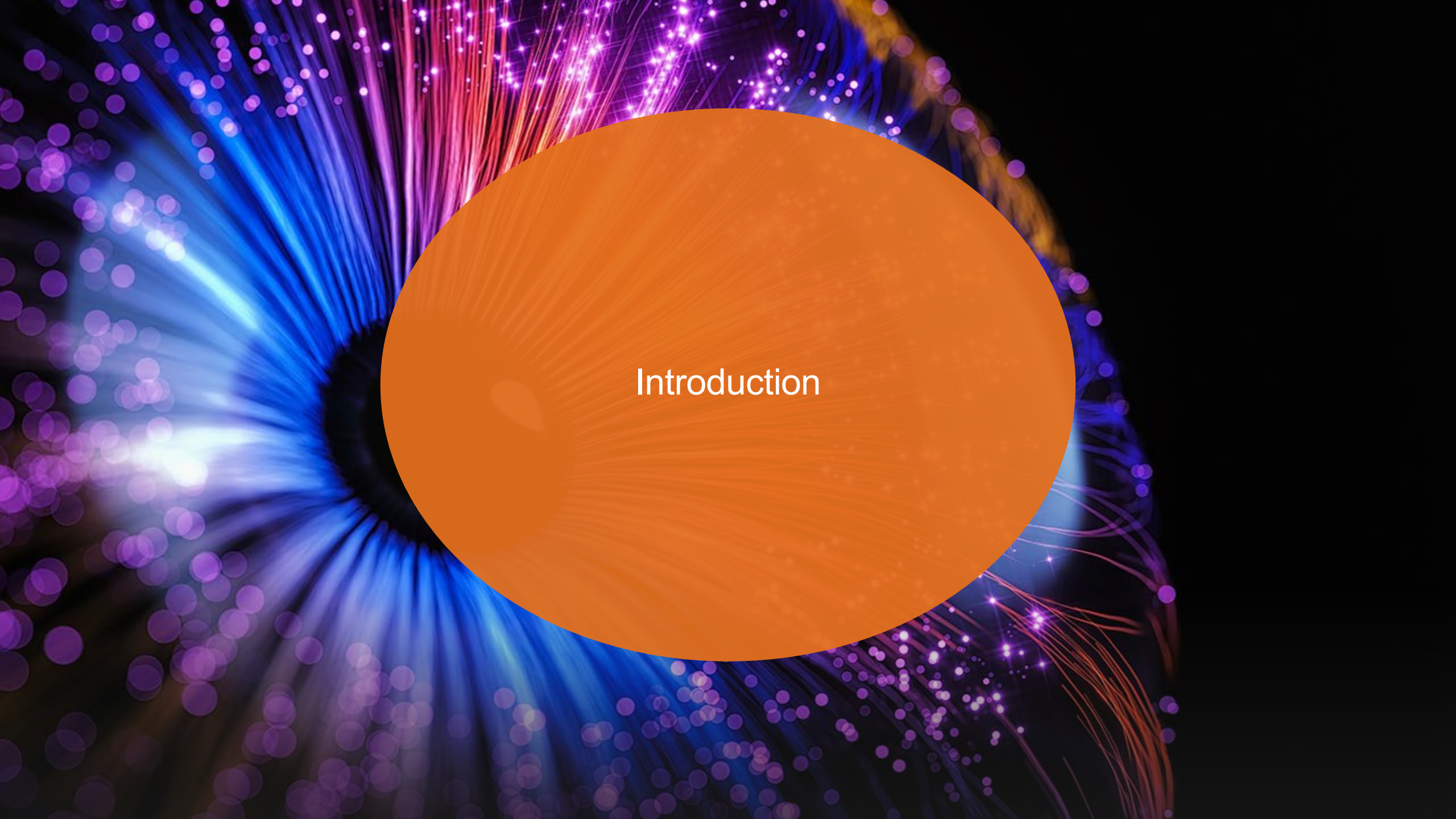
Speakers

Doron Goldstein
Partner, Americas Data Protection Lead
Withersworldwide

Frances Zelazny
CEO
Anonybit

Overview

- Introduction
- Identity Management Challenges and Privacy Tradeoffs
- Privacy and Data Protection Laws – Key Concepts for Biometric Authentication
- New Frameworks for Biometric Data Protection
- How Decentralized Authentication Aligns with Privacy and Data Protection Laws
- Looking Forward on Technology Developments, Regulatory Requirements, and Industry Guidance


Introduction

Authentication and Identity Verification Concepts

Key Concepts and Definitions (from NIST SP 1800-17) :

"Authentication" Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

"Identity" An attribute or set of attributes that uniquely describe a subject within a given context.

"Identity Assurance Level" A category that conveys the degree of confidence that the applicant's claimed identity is their real identity.

"Authenticator Assurance Level" A category describing the strength of the authentication process.

"Verifier" An entity that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.

"Authenticator" Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity.

Anonybit Withersworldwide

Biometric Data

"**Biometric data**" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is ***used to identify a specific individual***. "**Biometric data**" does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

Virginia (VCDPA)

"Biometric Information" means an Individual's physiological, blologlcal or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that ***Is used or intended to be used, singly or in combination with each other or with other identifying data, to establish individual Identit***y. Biometric Information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprlnt, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain Identifying Information.

California (CPRA)

"Biometric Information", meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity;

NY SHIELD Act

"**Biometric data**" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are ***used to identify a specific individua***l.

"**Biometric data**" does not include (A) a digital or physical photograph, (B) an audio or video recording, or (C) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

Connecticut (SB6)

"Biometric Information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or precdures excluded under the definition of biometric identifiers.

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.*

"Biometric identifier" does not include:
[…]

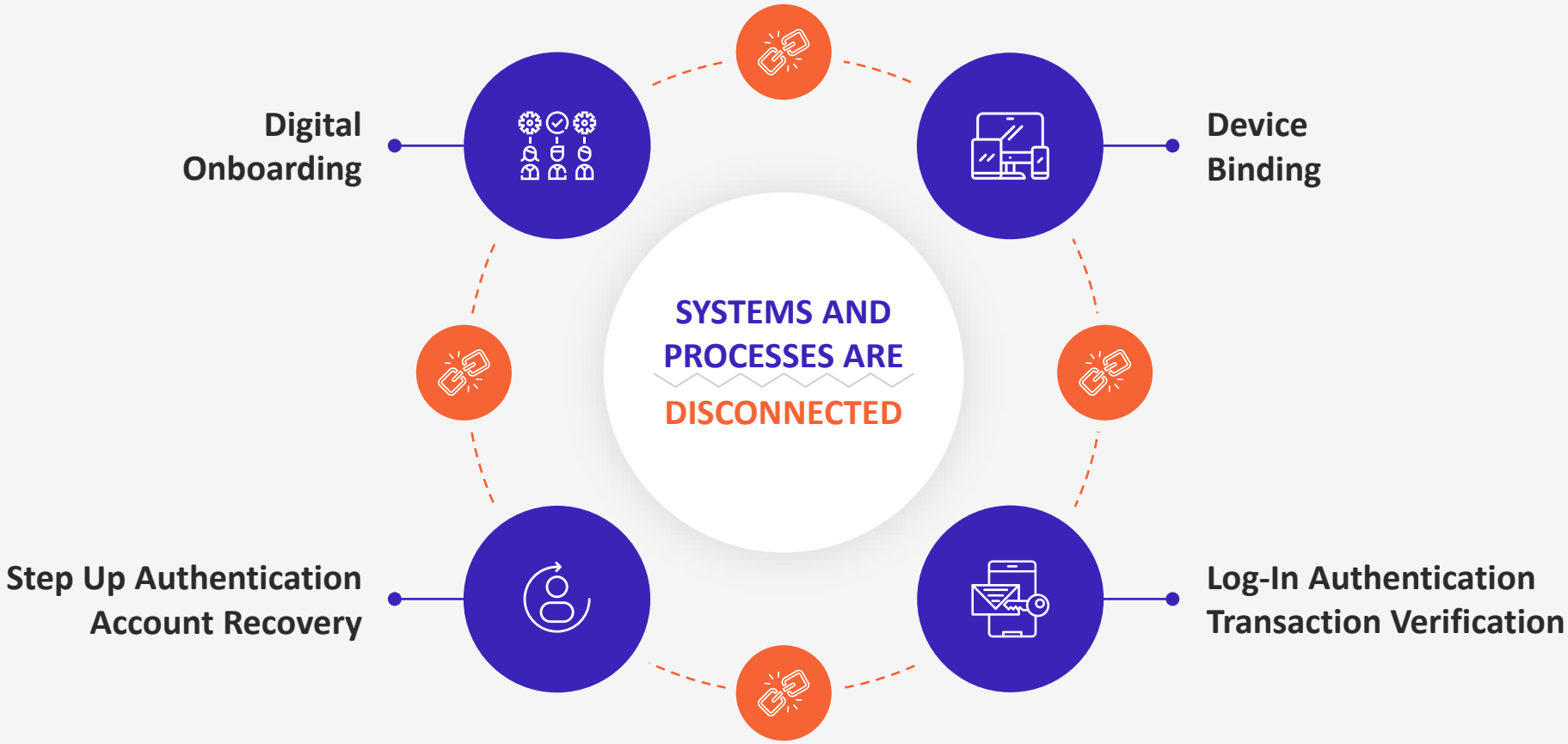
Illinois (BIPA)

'**biometric data**' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, **which allow or confirm the unique identification of that natural person**, such as facial images or dactyloscopic data;

EU (GDPR)


Identity Verification/
Authentication process and
data collection

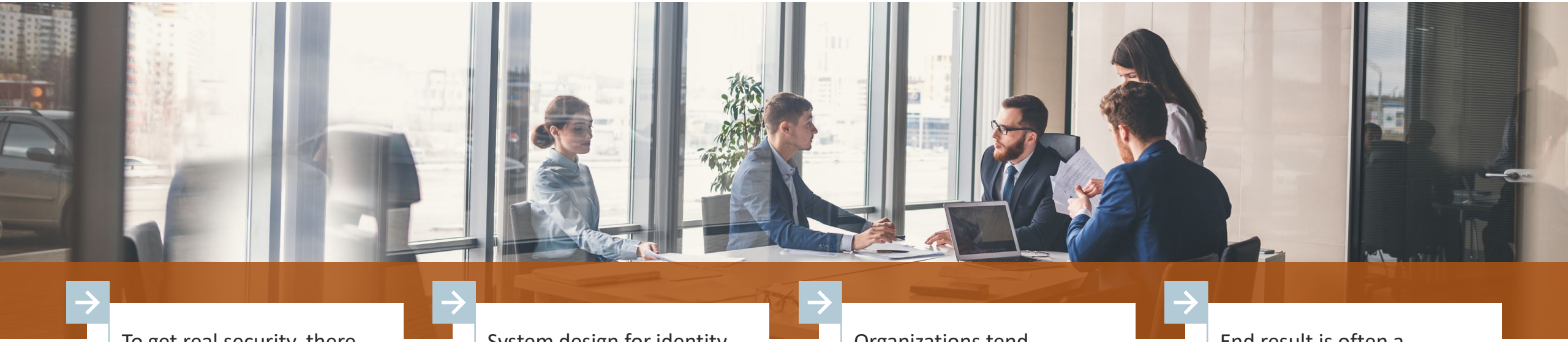
The Circle of Identity



Anonybit

Withersworldwide

Identity Management Challenges



To get real security, there is high friction and enormous cost

System design for identity management is complicated and risky from data standpoint

Organizations tend to be siloed and make individual purchase decisions

End result is often a tradeoff at the expense of privacy and security

Anonybit Withersworldwide

Privacy and Security Tradeoffs

PRIVACY-FRIENDLY DEVICE BIOMETRICS		SECURITY-ORIENTED CENTRAL HONEYPOTS
STANDALONE AUTHENTICATION NOT BOUND TO ROOTED IDENTITY		CLOSED LOOP SYSTEMS TIED TO ROOTED IDENTITY
USE OF PASSCODE FALLBACK, EASILY CIRCUMVENTED	VS	ALWAYS-ON BIOMETRICS WITH STRONG EXCEPTION HANDLING
EASILY AVAILABLE AND INTEROPERABLE		SUPPORT ISSUING AUTHORITY'S USE CASES AND APPLICATIONS

*Note, this is also typically the case even with the issuance of verifiable credentials

10

A Note about FIDO and PassKeys

- Good – Able to leverage a single FIDO credential across multiple devices. Big win for usability and convenience. Reduces burden on organizations having to manage FIDO tokens.
- Potential issues – Storage of FIDO keys in centralized clouds (Google, Microsoft, Apple) security around those, and potential lock-in as it is not clear how to migrate keys across cloud providers.
- Furthermore, unless the FIDO credentials are tied to the original onboarding via user biometrics and device binding, PassKeys will not address the issue of strong authentication (i.e., knowing *who* is behind the device).

Privacy and Data Protection Laws - Key Concepts for Biometric Authentication

Authentication and Data Protection

- There is a tension between identity verification/authentication and data protection
- More unique and difficult to change authenticators/factors are more sensitive
- Requires ongoing storage – often centralized - of [often-sensitive] personal information

Sensitive/Special Category Data

Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms

GDPR Recital 51

"Sensitive data" means a category of personal data that includes: […]
2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person; […]
4. Precise geolocation data.

A controller shall: […]
5. Not process sensitive data concerning a consumer without obtaining the consumer's consent […]

VCDPA § 59.1-575 & § 59.1-578

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

   the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,[…]

GDPR Art. 9

A business […] shall, at or before the point of collection, inform consumers of the following:
[…]

(2) If the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section.

CPRA 1798.100

Sensitive/Special Category Data: Biometric Data

b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative

Illinois BIPA

A person may not capture a biometric identifier of an individual for a commercial purpose unless the person:(1) informs the individual before capturing the biometric identifier; and
(2) receives the individual's consent to capture the biometric identifier.

Texas Biometric Privacy Law

"Enroll" means to capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual.

(1) A person may not enroll a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose.
(2) Notice is a disclosure, that is not considered affirmative consent, that is given through a procedure reasonably designed to be readily available to affected individuals. The exact notice and type of consent required to achieve compliance with subsection (1) of this section is context-dependent.
[…]
(6) The limitations on disclosure and retention of biometric identifiers provided in this section do not apply to disclosure or retention of biometric identifiers that have been unenrolled.
(7) Nothing in this section requires an entity to provide notice and obtain consent to collect, capture, or enroll a biometric identifier and store it in a biometric system, or otherwise, in furtherance of a security purpose.

Washington RCW 19.375.010 & 19.375.020

Data Localization

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. [2]All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

GDPR Art. 44

Before communicating personal information outside Québec, a person carrying on an enterprise must conduct a privacy impact assessment. The person must, in particular, take into account
(1) the sensitivity of the information;
(2) the purposes for which it is to be used;
(3) the protection measures, including those that are contractual, that would apply to it; and
(4) the legal framework applicable in the State in which the information would be communicated, including the personal information protection principles applicable in that State.
The information may be communicated if the assessment establishes that it would receive adequate protection, in particular in light of generally recognized principles regarding the protection of personal information..
The same applies where the person carrying on an enterprise entrusts a person or body outside Québec with the task of collecting, using, communicating or keeping such information on his behalf.

Quebec Bill 64

A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless—
(a) the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that—
effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and
includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;
(b) the data subject consents to the transfer; […]

South Africa – POPI Act

Anonymization

Process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party.

ISO 29100:2011

"Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:
(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
(2) Has implemented business processes that specifically prohibit reidentification of the information.
(3) Has implemented business processes to prevent inadvertent release of deidentified information.
(4) Makes no attempt to reidentify the information.

CPRA

[…] The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

GDPR Recital 26

Pseudonymization

"Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

VCDPA

…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

GDPR

“Pseudonymize” or “Pseudonymization” means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

CPRA

Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.

GDPR Recital 26

Data Minimization/Retention Limitation

"Personal data shall be:

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation') […]

(e)kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; […] ('storage limitation');

GDPR Art. 5(1)

(4) A person who knowingly possesses a biometric identifier of an individual that has been enrolled for a commercial purpose: […] (b) May retain the biometric identifier no longer than is reasonably necessary to:
(i) Comply with a court order, statute, or public records retention schedule specified under federal, state, or local law;
(ii) Protect against or prevent actual or potential fraud, criminal activity, claims, security threats, or liability; and
(iii) Provide the services for which the biometric identifier was enrolled.

Washington RCW 19.375.020

A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.

A business […] shall, at or before the point of collection, inform consumers of the following: […]
(3) The length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.

CPRA 1798.100

A controller shall:
1. Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer;

2. Except as otherwise provided in this chapter, not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;

VCDPA § 59.1-578

Security

A. A controller shall:
;
3. Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue;

VCDPA § 59.1-578

(4) A person who knowingly possesses a biometric identifier of an individual that has been enrolled for a commercial purpose:
(a) Must take reasonable care to guard against unauthorized access to and acquisition of biometric identifiers that are in the possession or under the control of the person;

Washington RCW 19.375.020

A private entity in possession of a biometric identifier or biometric information shall:

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

BIPA Section 15

Personal data shall be:

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

GDPR

Security

(a) any person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data.
(b) a person or business shall be deemed to be in compliance with Paragraph (a) of this subdivision if it […]
(ii) implements a data security program that includes the following:

(a) reasonable administrative safeguards such as the following, in which the person or business:
(1) designates one or more employees to coordinate the security program;
(2) identifies reasonably foreseeable internal and external risks;
(3) assesses the sufficiency of safeguards in place to control the identified risks;
(4) trains and manages employees in the security program practices and procedures;
(5) selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and
(6) adjusts the security program in light of business changes or new circumstances; and

(b) reasonable technical safeguards such as the following, in which the person or business:
(1) assesses risks in network and software design;
(2) assesses risks in information processing, transmission and storage;
(3) detects, prevents and responds to attacks or system failures; and
(4) regularly tests and monitors the effectiveness of key controls, systems and procedures; and

(c) reasonable physical safeguards such as the following, in which the person or business:
(1) assesses risks of information storage and disposal;
(2) detects, prevents and responds to intrusions;
(3) protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and
(4) disposes of private information within a reasonable amount of time sfter it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

NY SHIELD Act

New Frameworks for Biometric Data Protection

Homomorphic Encryption

Allows **computations to take place within encrypted data sets**. Able to scale and handle structured and unstructured data sets. Allows data sharing across organizations in encrypted formats.

Data remains **centralized** and **encryption keys need to be managed.** Note that if the encryption keys are compromised, the data set is at risk. Up to 35%-60% of data breaches occur from insider threats and misuse of privileged access credentials.

Anonybit Withersworldwide

Tokenization

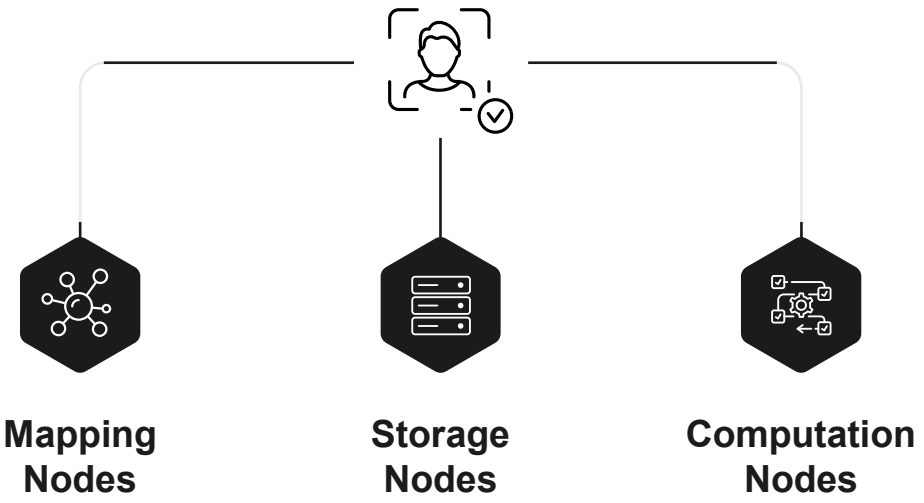
Creates a **one-way hash to make data unusable to an attacker** by randomly generating a token value for any data set and stores the mapping in a database.

*Can be distributed hosted servers or user mobile devices

The original data set will never leave the organization. However, **tokens need to be managed**, which require their own processes. This makes it very difficult to scale and validate data across organizations.

Anonybit Withersworldwide

Decentralization



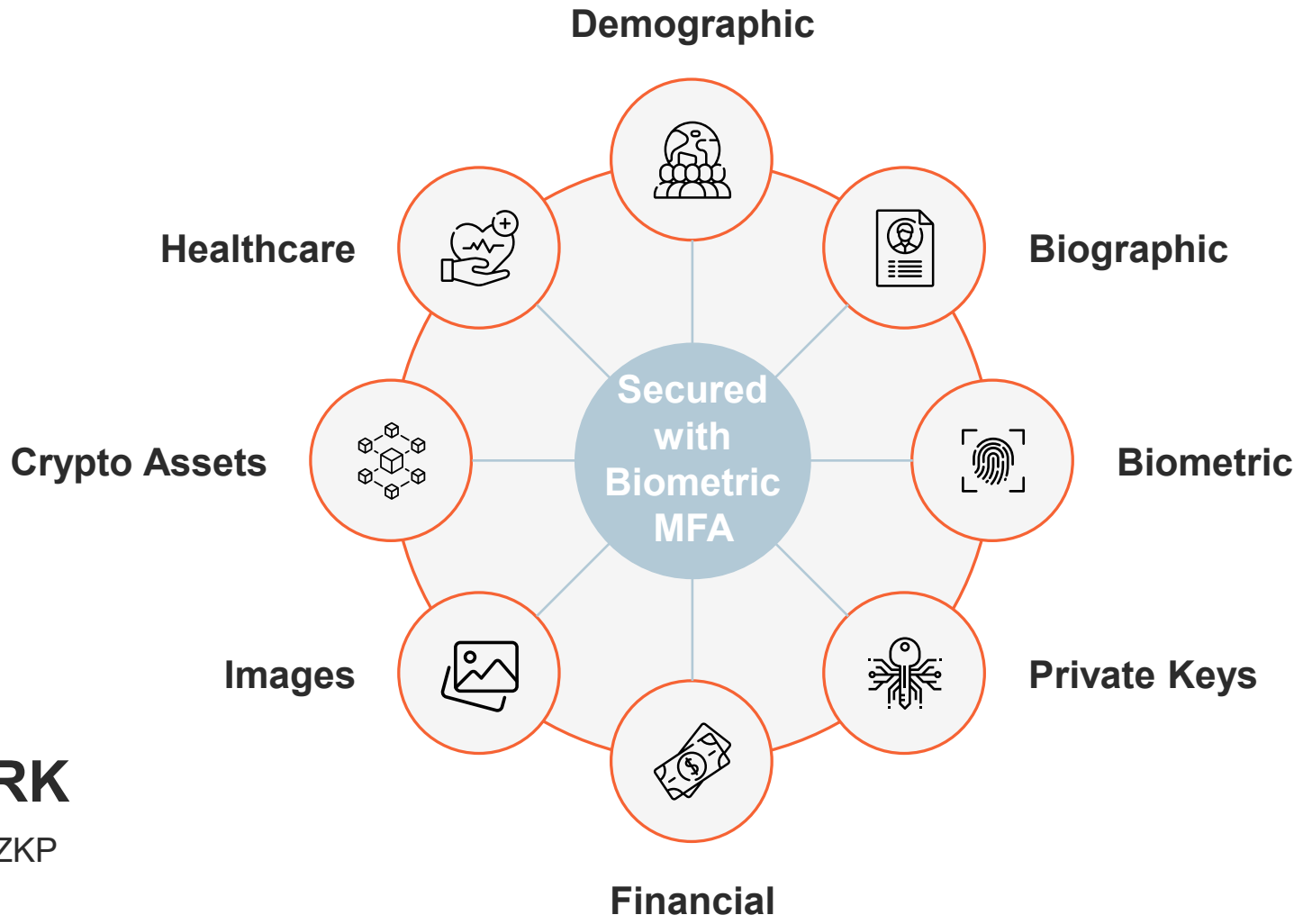
Leveraging multi-party computing (MPC) and zero knowledge proofs, **personal data is broken up and distributed** over a peer-to-peer network of nodes.

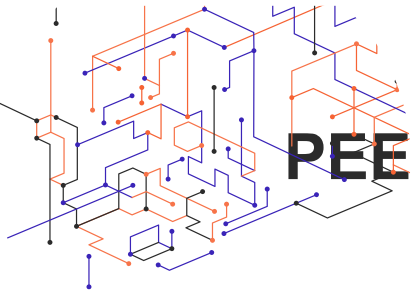
*Can be distributed hosted servers or user mobile devices

With biometrics, **the data is never retrieved and never compiled together again**, even for matching, eliminating the risk of a data breach. Can run **1:1 and 1:N** queries on the MPC network.

Anonybit Withersworldwide

Data Decentralized Beyond Biometrics





PEER TO PEER NETWORK

MPC+ZKP

Anonybit

Withersworldwide

Security vs Privacy
New Frameworks Allow Us to Have Both

Closed Circle of Identity

Connects digital onboarding to downstream authentication to close the gaps exploited by hackers.

Privacy-by-Design

Personal data is not held in any central honeypot. Maintain principles of FIDO and GDPR.

Multiple Use Cases

Supports all biometric modalities and third party-algorithms for different identity management needs across the enterprise.

Device Independent

Works across devices. Not susceptible to insider threats or device takeover, phishing and other attacks.

Anonybit Withersworldwide

How Decentralized Authentication Aligns with Privacy and Data Protection Laws

Decentralization: Pseudonymization

The consumer rights contained in subdivisions A 1 through 4 of § 59.1-577 and § 59.1-578 shall not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

VCDPA

To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

GDPR Recital 26

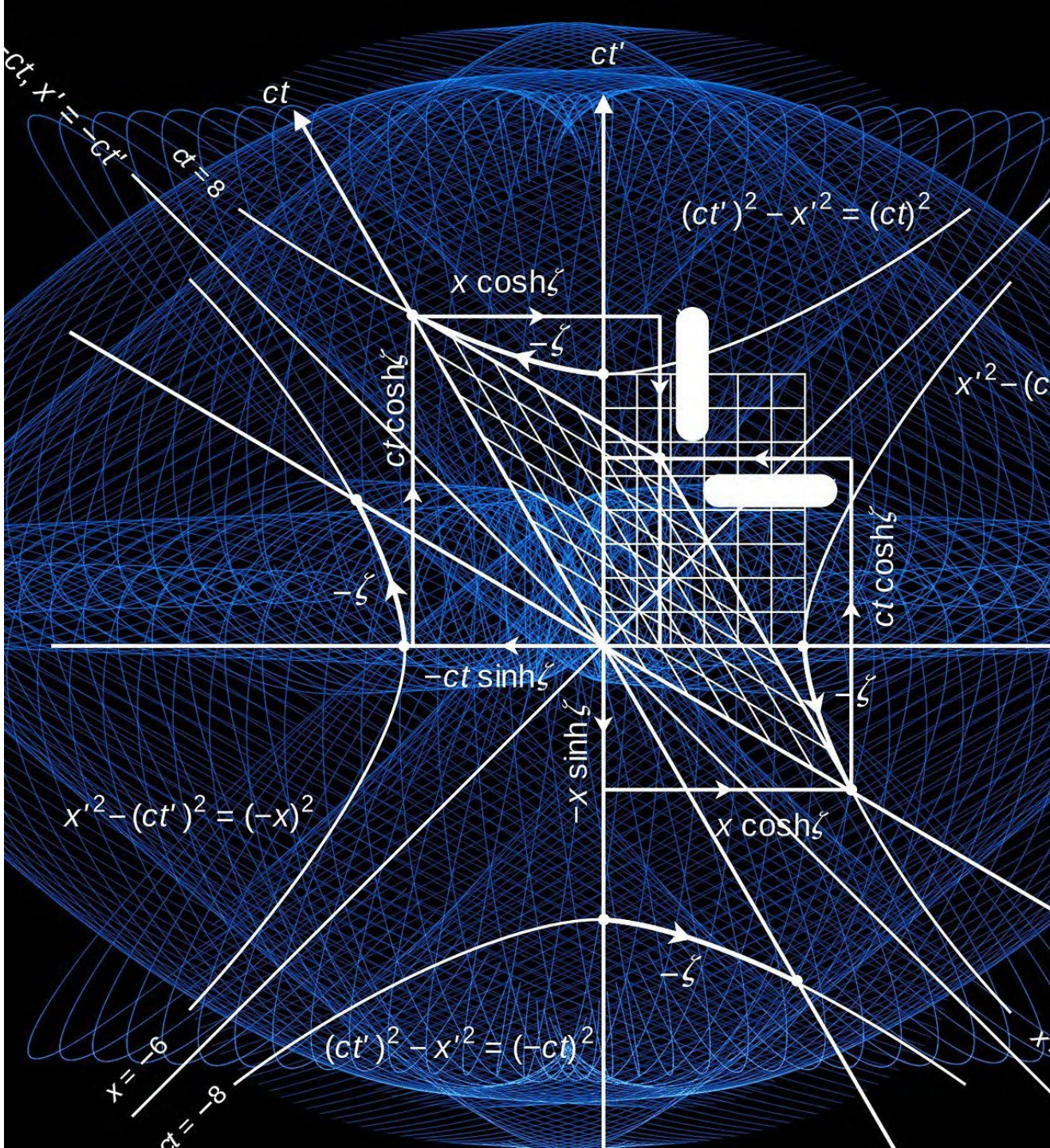
Decentralization: Risk of Harm

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

GDPR Art 35

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

GDPR Art 33



Anonybit

Withersworldwide

Decentralization/Encryption: Security

Personal data shall be : (f) processed in a manner that ensures appropriate security of the personal data , including protection against unauthorised or unlawful processing and against accidental loss , destruction or damage , using appropriate technical or organisational measures (' integrity and confidentiality ')

GDPR Art .5 (1)

Personal Information:

(A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: […]

California Data Breach Notification Law

Looking Forward on Technology Developments, Regulatory Requirements, and Industry Guidance


Questions?

Thank you!

Withers Bergman LLP – 430 Park Avenue, 10th Floor, New York, NY 10022, +1 212 848 9800

Global office locations

London | Cambridge | Geneva | Milan | Padua | Hong Kong | Singapore | Tokyo | British Virgin Islands

New York | Boston | Greenwich | New Haven | Texas | San Francisco | Los Angeles | San Diego

withersworldwide