Personal Data & Identity: Key Terms To Support Business Strategy For 2023 and Beyond

Michael J. Becker

12/31/22

Table of Contents

About the Author

Michael Becker is a strategic advisor, author, speaker, and educator. Michael is the founder and CEO of Identity Praxis, and a Director of Ctrl-Shift, both personal data & identity (PD&I) strategic consultancies. Michael offers product development, market development, business development, and marketing services to Fortune 500s, startups, and non-profits worldwide. He helps them envision the future and works with them to achieve their goals. Michael is also the Mobile Ecosystem Forum (MEF) PD&I working group Chairperson and the MEF's PD&I events, content, and research programming lead. He is the author of several books, including the soon to be released—"The Personal Data and Identity Meeting of the Waters: When Two Approaches of Personal Data and Identity Management Converge" and the "5Cs of Knowledge Management: A Guide to Unleashing Your Creative Potential and Contribution." He is the author and co-author of "Mobile Marketing Essentials," "Mobile Marketing for Dummies," "Web Marketing for Dummies," and several other books, journals (e.g., The International Journal of Mobile Marketing), articles, and videos related to personal data & identity management, business strategy, personal knowledge management, mobile and digital marketing, and The Identity Nexus™. He also maintains a YouTube channel, the 5Cs of Knowledge Management. Michael is an adjunct professor at California State Polytechnic University, Pomona, National University, and the Association of National Advertisers. Formerly, Michael was the co-founder of mCordis & The Connected Marketer, and iLoop Mobile, one of the first U.S. commercial mobile marketing platform SaaS solutions. He was also a founding member and on the board of the Mobile Marketing Association for nearly a decade and was its North American Managing Director for three years. Michael received one U.S. patent and has earned several personal and corporate awards, including the Marketing EDGE Education Leadership Award 2014.

Contact Details

Michael J. Becker

CEO, Identity Praxis, Inc.

Director, Ctrl-Shift

MEF Personal Data & Identity Working Group Chairperson

https://www.linkedin.com/in/privacyshaman/

Introduction

Those who know me know I spend a copious amount of time thinking about personal data, i.e., the data produced by and about individual people or by and about their things. Why? Because we've entered a new age with many names: the fifth industrial revolution, the self-sovereign identity movement, authentic data management, Web 3.0 or Web 5.0, the personal information economy, and more. These terms and others are all rooted in one central idea: we need to empower individuals with digital agency and self-determination so that individuals, communities, societies, and economies can and will sustainably thrive. To give people control of their personal data, we need to establish new governance systems, build technical systemic trust into products, services, an systems and create new trusted personal data-centric value chain ecosystems.

Knowledge is Power

Sir Francis Bacon.[1] nailed it, "knowledge is power," and there is nothing more demonstrably powerful than the knowledge generated from personal data.

With intimate personal data-infused knowledge, individuals, businesses, and governments can make logical decisions and take well-informed actions. Sensible decisions and well-informed actions can significantly increase an individual's chance of achieving their goals. .

For instance,

- **individuals** can achieve their goals of happiness, staying physically and mentally healthy, being educated, creating a difference, showing compassion, ensuring equality and sustainability, etc., not to mention transactional goals (a.k.a. jobs to be done).[2,3] like going out with friends, beginning new business ventures, dependably completing projects, passing a course, traveling, paying bills on time, saving and establishing a retirement account, etc. (desired goals and outcomes can significantly vary between individuals and beyond an individual's life).
- **organizations** can deliver value to those they serve, innovate, increase revenues, reduce costs, and mitigate risks.
- **governments** can deliver services, protect their citizens, improve market fairness and competition, increasing revenues (i.e., gross monistic product).

The vast majority of people–you, me, everyone–and organizations, however, are unable to harness the power of personal data because they genuinely don't

understand the nature of personal data, its velocity, volume, value, variety, and veracity, and are unable to access it and manage it easily. And, if they could do all this, there are other hurdles they face. Specifically, they lack access to the tools, experience, or training to protect their personal data and to turn their raw personal data into knowledge that can create insight to drive informed actions.

Break Down the Silos to Release the Power

People's data are scattered throughout the datasphere. Their data is held by them and is in control of others.[4], most notably governments and large private enterprises. Just look at Facebook. In 2016, Facebook reportedly held over 52,000 attributes, i.e., individual pieces of data, on the average Facebook user (today, seven years later, imagine how much they have on their users).[5] Facebook has and is using the data collected to produce knowledge. This knowledge gives it power, power to generate wealth and influence. It influences everyone, given that 39.9% of the global population uses Facebook, as do 82% of North Americas and 77.8% of Europeans.[6] There are several big tech companies and categories of companies that wield similar power. For example, Google, Amazon, TikTok, Tencent, and Apple, Mozilla, Acxiom, intermediation services, search engines, social media services, data brokers, to name just a few. The EU regulators refer to these companies and the companies in these categories as gatekeepers.[7,8]

Market forces—business, opinion, legal, and technology—are pushing hard against what has become the status quo, the centralization of personal data-infused market power into a handful of private enterprises. Governments are shaping and reshaping their regulation to redistribute power, to ensure that their markets remain open and accessible and that individuals are protected and can maintain agency and self-determination. For instance, the European Union, other democratic lending regions, and individual countries are instituting new regulations. For instance, the EU has recently published the EU Data Governance Act.[9], EU Digital Markets Act.[10], EU and Digital Services Act.[11], to name a few (I've been tracking well over 100 regulations). By 2024 75% of the world's population will fall under one of these regulations.[12] Individuals are expressing their desire to preserve their privacy and to be in control of their data, but given that they don't know how to do this, they continue with their lives and live within the status quo. Technologists have been working on new standards, protocols, infrastructure, and more to empower people and put them in control of their data. And businesses, for the most part, have been looking to thread the needle, to find a way to serve their customers and

comply with regulations, all while turning a profit. We can dig into these market forces later.

Key Terms Underpinning our Future

As I look to 2023, I can't help but think about the future of personal data and how complicated it is to understand and manage. There are many conceptual, legal, commercial, operational, social, and technical terms swirling around personal data. In alphabetical, non-prioritized order, I've listed 64 key terms that underpin the future of personal data. It is hard to keep track of all these terms, let alone understand them and successfully execute based on this understanding. But to understand them and execute we must. As current and future business leaders, we must keep track of the evolution of these terms. We must learn them, understand them and their relationship to each other, and operationalize them to steer our businesses, guide our industries, and support our economies in the coming months and years.

Key Terms Underpinning of the Future of Personal Data

Term	Description
Agency	**Agency** refers to an individual's sense that they have control over their own actions and their life's circumstances.
Attribute	**Attribute** is a characteristic, quality, or feature that is inherently part of someone or is something.
Authentic Data Management	**Authentic Data Management** is the process of verifying the provenance, accuracy, and truthfulness of data (i.e., verifying an attribute) and the claims asserted about the data, e.g., the individual is over 21, has the license to teach, graduated from a particular institution on a given date, or this thing is owned by that individual, etc.
Centralized Identity Management	**Centralized Identity Management** is an identity management approach. Under this approach, an organization takes it upon itself to self-issue and manage the identity credentials issued to individuals or things, e.g., an employee ID card or a username and password. Once an individual or thing has received an identity credential from an organization, they can use it to access the physical or digital products and services they've signed up for, licensed or purchased from the organization. Organizations may be required, due to internal policies or regulatory requirements (e.g., banks must follow know your customer (KYC) or anti-money laundering regulations), to verify the legal identity of an individual before issuing an identity credential to the individual.
Consent	**Consent** refers to the permissions individuals give an organization to process their personal data. Consent must be obtained at the time of data collection, when the

	data is to be used for purposes other than the original purpose, or when processing sensitive data (e.g., kids, criminal records, have received parental consent) (see GDPR article 9(1) and 8(1)), transfer data to third-party (see GDPR article 13(3)).
Consent-Based Sharing	**Consent-Based Sharing** see consent and permission-based data sharing.
Credential	**Credential** is a document or data set proving an individual's identity, right to use or access a product or service, or their qualifications.
Cryptology	**Cryptology** is the process of converting human-readable plain text into unintelligible text and visa-versa (a.k.a. encryption process).
Customer Journey	**Customer Journey** refers to an analysis of the path of interactions and physical and digital (inc. cognitive, emotional, and sensorial) experiences an individual will have with a business (a.k.a. brand), product, or experience. A customer journey is typically divided into the following stages: unaware, aware, consideration, transaction, adoption, loyalty, advocacy, and retirement (these labels will vary by each business and culture). Support and communications will be a common thread throughout every customer journey stage. For the purpose of convenience, the customer journey steps are often viewed linearly, but in reality, an individual will interact with a brand, product, or service in a recursive nonlinear fashion. The customer journey analysis process is often combined with individual empathy mapping, personal mapping, and BMAT.[13] (Behavior, Motivation, Ability, Trigger) mapping.
Data	**Data** are qualities and characteristics that are related to someone or something, data is used as a basis for reference, reasoning, analysis, and calculation.
Data Exchange	**Data Exchange** see data sharing.
Data Gifting	**Data Gifting** refers to the typical model of data sharing, when people share data they're really gifting it to organizations since the individual rarely receive explicit and measurable value in return for the data.
Data Sharing	**Data Sharing**
Data Subject	**Data Subject** is a legal term referring to an individual related to the data in question.
Decentralized Identifier	**Decentralized Identifier (DID)** is a standardized identifier used in the self-sovereign identity and authentic data approach to personal data and identity management. The DIDs specification is maintained by the World Wide Web Consortium ("Decentralized Identifiers (DIDs) V1.0," 2021).[14]
Decentralized Identity Management	**Decentralized Identity Management** is a privacy-preserving identity management approach. Under this approach, cryptographically secure identity credentials, e.g., FIDO Passkeys or verified credentials, are issued to individuals by an issuer and managed by individuals. Individuals manage their credentials in a secure web service or mobile app, e.g., personal data store or digital wallet. The credential is issued with a private encryption key that only the individual knows or holds; therefore, the individual and only the individual can use their decentralized identity credentials to assert claims about their identity or about data about them.
Digital ID	**Digital ID** refers to information used to identify an individual. A Digital ID can be as

	simple as a username and password combination or as complex as a verified credential.
Digital Identity	**Digital Identity** is a collection of information used to affirm the identity of an individual, application or device. Once an identity is verified the replying party can then determine what the individual, application, or device is allowed to do.
Ecosystem	**Ecosystem** refers to all the players operating within a value chain, a.k.a. business ecosystem. The term "business ecosystem" was first defined by James Moore.[15] as "an economic community supported by a foundation of interacting organizations and individuals—the organisms of the business world. The economic community produces goods and services of value to customers, who are themselves members of the ecosystem. The member organisms also include suppliers, lead producers, competitors, and other stakeholders. Over time, they coevolve their capabilities and roles, and tend to align themselves with the directions set by one or more central companies. Those companies holding leadership roles may change over time, but the function of an ecosystem leader is valued by the community because it enables members to move toward shared visions to align their investments and to find mutually supportive roles." Today, the consumer's, i.e., the individual's role is evolving. The individual is no longer a passive recipient of value within the ecosystem, but rather a central producer of value, i.e., of personal data. It is, for this reason, we will see a significant change in the industry in the months and years to come.
Empowered Data Sharing	**Empowered Data Sharing** refers to the process of an individual managing the sharing and exchange of personal data via technology and services (e.g., personal data store or personal data information system), technology that puts the data under the individual's direct and explicit control. The process is systemically trusted via technology and governance structures and gives the individual the ability to audit the flows of their data. At their discretion, the individual can share their data, exchange it, track it, and revoke access to it.
Federated Identity Management	**Federated Identity Management** is an identity management approach. Under this approach, an individual's digital identities and attributes are centrally managed by an organization and linked across multiple distinct identity management systems. Under this approach, like in the centralized approach, the organization managing the primary identity that is linked to other identity management systems, may be required to validate the individual's legal identity.
Fifth industrial revolution	**Fifth industrial revolution** refers to the harmonizing of human–machine collaborations, with a specific focus on the well-being of the multiple stakeholders (i.e., society, companies, employees, and individuals).
Five Domains of Data	**Five Domains of Data**
Gatekeeper	**Gatekeeper** is a large tech company, e.g., Google, Facebook, Amazon, etc., or one that falls into a specific category, and plays a systemic and multi-sided role in connecting businesses and consumers to digital services. The EU digital markets act recognizes 10 core platform services as gatekeepers: online intermediation services, online search engines, online social networking services, video-sharing platform services, number-independent interpersonal communication services, and

	operating systems. cloud computing services, advertising services, web browsers, and virtual assistants.[16]
Governance	**Governance** refers to the effort of providing oversight on the alignment and execution of all processes and actions necessary for adhering to the organization's industry, or government regulatory compliance requirements and the delivery of services. It ensures that organizations and the ecosystem as a whole are responsible and ethical and are following the legal, technical, commercial, and social rules and norms set by the ruling government, industry, and organization governance and related trust frameworks, principles, and codes-of-conduct.
Holder	**Holder** is the individual who is issued a verifiable credential and has the authority to use it by virtue of being in control of it. Individuals control their verified credentials via a smart wallet (a.k.a. digital wallet, SSI digital wallet) or via other web services.
Identifiable Natural Person	**Identifiable Natural Person** , according to **Article 4, point (1), of Regulation (EU) 2016/679** (also known as the General Data Protection Regulation, or GDPR),"is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.".[17]
Identifier	**Identifier** are data elements associated with an individual. Common identifiers include usernames and passwords (e.g. credentials), one-time passcodes, biometrics (fingerprint, face scan, heartbeat[18]), pseudonyms, or the possession of a physical device. Combinations of personal data can also be used as an identifier, for example, a birth date, mother's maiden name, physical address, etc. The key to successful identity management is to ensure that no two individuals have the same set of identifiers, that way you have a high level of assurance they are who they say they are (see Authentication Methods for more details).
Identity	**Identity** is the attribute or set of attributes that uniquely distinguishes an individual or thing (a person, enterprise, state, instigation, device) from another. Identity is resolved by the analysis and interpretation of data that is or can be related to an individual.
Identity Assurance	**Identity Assurance** is an identity resolution confidence measure. Ranging from zero to one hundred percent, it measures the level of an actor's confidence that the individual asserting a claim is who they say they are. The higher the assurance level, the more certain, i.e. confidence, an organization has that the individual and the claims they are marketing are authentic, i.e., true. According to the National Institute of Standards and Technology, there are 4 levels of identity assurance.[19] Also, see **Identity Proofing** .
Identity Managment	**Identity Managment**
Individual	**Individual** is any legally recognized entity, including natural persons, a public or private organization (regardless of its structure or tax status—LLC, B-Corp, C-Port, 501C3, etc.), or a government. In the context of the personal, it is also referred to as "the data subject." It is important to remember that there are many surrogate terms for the individual, including—the data subject, natural person, citizen, constituent, resident, renter, employee, consumer, buyer, shopper, prospect, patient, voter,

	investor, member, client, and more. All these terms are made up, mostly by marketers, to reflect the people they serve at different stages along the individual's journey (i.e., customer journey). When it comes to personal data, it is important that the individual, at some point in their life at different stages of the customer journey, different stages along the customer journey.
Intermediary	**Intermediary** is an organization that offers network infrastructure, e.g., internet access, domain name registration, hosting, or data collection and sharing and exchange services (i.e.,, online platforms).[20] An "intermediary service is essential for a safe, predictable and trustworthy online environment and for allowing .[European] Union citizens and other persons to exercise their fundamental rights".[21] The term data infomediary, i.e., intermediary, first arose in 1997.[22,23] as a general concept for a new class of organization would emerge to help represent the personal data interest of an individual to industry at scale. Since then, the term has fragmented and taken on several nuanced meanings and implementation approaches, such as: Information Fiduciaries.[24], Data Commons.[25], Personal Data Spaces.[26,27,28], Information Banks .[29,30,31], Personal Data Cooperatives .[32], Data Custodian.[33], Data Cooperative.[34,35], Data Steward .[36], Data Safe Haven.[37], Account Aggregator.[38], Public Data Intermediary .[39], Private For-Profit Data Intermediary .[40], Non-Profit Data Intermediary .[41], Digital Fiduciary.[42], Data Facilitator.
Interoperability	**Interoperability** refers to a product, service, or system being made to work with other products, services, and systems, e.g., making it possible for them to share user access, share data, business, logic, and service experiences. Interoperability is possible through three lenses: standards, permission, and adversarial.[43] Standards interoperability relies on the industry establishing agreed-upon standards on how products, services, or systems will work together. HTML, the standard for the web, web pages, and web browsers, are a great example of this. Web pages that use standard HTML will work in standards-compliant web browsers. Permission-based interoperability relies on a company giving permission to other companies to interoperate with their products, services, or systems; this often requires the company to share technical specifications, processes, and approvals with whoever is opening their systems up. Apple or Google Play mobile app stores are good examples of permission-based interoperability. They share their technical specs and processes to connect their systems. Adversarial interoperability occurs when a product, service, or system plugs into another without permission. A good example of this is third-party printer ink.
Issuer	**Issuer** is the party that produces and certifies that the information represented in a Verifiable Credential is authentic and accurate.
Issuer	**Issuer** is the party that produces and certifies that the information represented in a Verifiable Credential is authentic and accurate.
Lawful Basis	**Lawful Basis** under various regulatory frameworks, organizations must have a legal basis for collecting and processing personal data and identity. For instance, the **GDPR** spells out 6: 1) consent, 2) contract, 3) necessary for a legal obligation, 4) necessary for vital interests, 5) necessary for public tasks, 6) necessary for legitimate interests for the controller of a third-party. The U.K. Information Commissioner's Office hosts a "**Lawful basis intuitive guidance tool**" that can help you determine the lawful basis that might apply to your processing of personal data. Consider the

	fact that a single basis of processing will not apply to each piece of data collected.
Lawful Basis	**Lawful Basis** under various regulatory frameworks, organizations must have a legal basis for collecting and processing personal data and identity. For instance, the **GDPR** spells out 6: 1) consent, 2) contract, 3) necessary for a legal obligation, 4) necessary for vital interests, 5) necessary for public tasks, 6) necessary for legitimate interests for the controller of a third-party. The U.K. Information Commissioner's Office hosts a "**Lawful basis intuitive guidance tool**" that can help you determine the lawful basis that might apply to your processing of personal data. Consider the fact that a single basis of processing will not apply to each piece of data collected.
Metadata	**Metadata** is data about data. It is data that helps explain the properties of other types of data. There are six types of metadata: structural (data that establishes the relationship between objects), descriptive (data that defines resources associated with the data, i.e., the who, what, when, and where), preservative (data that helps preserve the data, e.g., rights management), administrate (data that helps manage the data, e.g., governance frameworks, access controls, license agreements, etc.), provenance (data that helps establish the origin of the data, its source), and definitional (references that help establish a common vocabulary for the data).
Multi-factor Authentication	**Multi-factor Authentication (MFA)** is a process for verifying an identity assertion or claim. It relies on the use of one or more factors (knowledge, possession, inheritance, location, and behavior) to authenticate an individual's identity claim. The most common factors are a one-time code sent via SMS, a mobile authenticator app-generated code, or a biometric like FaceID or a fingerprint.
Non-Personal Information	**Non-Personal Information** is data produced through interactions with an individual and an individual's capital assets and applications but can not be used on its own to trace or identify an individual. There are three categories of non-personal data: public, community, and private.
Permission-based Data Sharing	**Permission-based Data Sharing** is the process of providing permission for something to happen, e.g., an individual can provide another entity consent to use their personal data for a specific purpose over a specific period of time.
Personal Data	**Personal Data** according to **Article 4, point (1), of Regulation (EU) 2016/679** (also known as the General Data Protection Regulation, or GDPR), "personal data' means any information relating to an identified or identifiable natural person ('data subject')".[44] Extending this definition, personal data may relate to any data (attributes, attribute sets) produced by or about an individual or by and about the individual's things, their capital assets (i.e., smart things, e.g., home, car, appliances, connected devices, etc.).
Personal Data Sharing	**Personal Data Sharing** refers to an individual giving permission to an organization (or intermediary) to use the individual's data for joint or individual use. Data sharing may occur under open or commercial licensing agreements and may be subject to a fee or be free of charge.[45]
Personal Data Store	**Personal Data Store** is a service to let an individual store, manage and deploy their personal data and manage their identity in a highly secure and structured way. PDSs sit at the core of a PIMS.[46,47,48,49]
Personal Information	**Personal Information Management System** is a system to help individuals have control over their personal data, to allow them to manage their personal data in

Management System	secure, local, or online storage systems and share them when and with whom they choose.[50] A PIMS may interface with a wide range of related products, services, systems, and business structures, including personal analytics services, data generation, and tools services, permission management services, privacy awareness tools, and services, gatekeeping services, transparency services, data access, and deletions services, profile and persona management services, data sharing tools and services, privacy-preserving technologies.
Personally Identifiable Information	**Personally Identifiable Information** is personal data that can be directly or indirectly attributed to an individual. See personal data.
Phygital	**Phygital** refers to the idea that people are no longer simply physical beings but also digital beings; it is the merger of the constructs of physical and digital. The Australian agency Momentum, which claimed the copyright for the word in 2013, is attributed to be the creator of the term. The term was part of its motto "An agency for the Phygital World".[51]
Primary Purpose	**Primary Purpose** refers to the agreed update terms and intended uses of personal data at the time consent was given and it was shared. Regulations stipulate commercial agreements that personal data should only be used for the primary purposes and that new consent should be obtained if personal data is to be used for any other purpose other than the primary purpose (i.e., a secondary purpose).
Privacy	**Privacy** is a process related to an individual being in control of both their physical self (person, wards, or property—house, cards, connected devices, etc.) and digital self (i.e., their personal data).[52] An individual can be a human, an enterprise, or a governmental institution. For an individual to have and maintain privacy, they must be in a position to manage all five elements of privacy, the "5 Ws", the who, what, when, where, and why. "Who" refers to the entity (e.g., another individual, enterprise, government, or machine) seeking to gain access to the individual. "What" refers to what an entity is looking to access, i.e., aspects of the individual's physical or digital self. "When" refers to the timing of the access—in other words, when and for how long the entity will have physical or digital access to elements of the individual. "Where" refers to the location where the interaction, physical connection, or personal data exchange will take place. This could be in the real world, via mobile, in the cloud, locally on an individual's device, etc. "Why" refers to requesting an entity's intention and purpose for wanting access, for example, what they are going to do with the individual's data (and, to maintain trust, if they will ensure there are no unauthorized secondary uses of the data). Adrienne Meisels at myPlanit, as does Liz Brandt at Ctrl-Shift, roles up the 5Ws into one word "context"[53,54] The context of a situation will determine how an individual manages the flow of their information. It is important to consider that context changes, which is one of the reasons why privacy is so difficult to manage. Privacy is a process, and like any process, it is fluid, and the outcomes can change with the change of inputs and context.[55] In addition to the individual view of privacy noted above, there are other nuances to the definition of privacy to consider. For instance, there is the legal view, the security

	and technologist view, the cultural view, the economic view, and the political view of privacy. See: **file:///Applications/Spark.app/Contents/Resources/smx-composer.bundle/smx-plain-composer.html**
Provenance	**Provenance** refers to the place of origin, the earliest known history of something, e.g., and identity credential or data attribute.
Regulation	**Regulation** is a rule or directive made and maintained by an authority, e.g., a government, industry trade body, or community.
Relying Party	**Relying Party** see verifier.
Secondary Purpose	**Secondary Purpose** refers to uses of persons data other than the primary purpose.
Self-Sovereign Identity	**Self-Sovereign Identity (SSI)** is a technologically-grounded approach for establishing trustworthy digital connections and relationships between parties engaging through and with Internet-powered services (i.e., via computers and mobile devices, in both online and offline situations) so that they can engage in trusted transactions. At all times, each party maintains and has granular control over their personal data and identity. SSI, with cryptographic certainty, ensures that each party knows who they're dealing with through the "Trust Triangle." The Verifier can be assured that the data or identity assertion (i.e., verifiable credential, aka authentic data) being presented by the Holder is authentic since the information (aka Verifiable Credential) being presented has been verified by the Issuer. It is worthy to note, also, that our things can also bestowed with SSI. In the context of SSI Max Thake points calls this "self-sovereign machine identity (SSMI).[56]
Sensitive Data	**Sensitive Data** refers to people's emotional sentiment and the legal classification for specific data types. Data sensitivity tends to be classified as low, medium, or high sensitivity. Common sensitivity data includes attributes like a person's name or email address. Medium sensitive data includes things like browser history. And high sensitive data includes data like government IDs, identifiers, and financial records. Data-sensitive is personal and varies by individual, and specific regulators, markets, regions, or governments will often classify what is considered sensitive or not. The distinction is that sensitive data is treated with more excellent care, including instituting data encryption and security measures.
Smart Wallet	**Smart Wallet** also known as a digital wallet or SSI digital wallet, is a mobile or web application that stores verified credentials or otherwise cryptographically signed records, and is used by a holder to assert claims about their identity or data.
Systemic Trust	**Systemic Trust** refers to trust being established through the use of technology, e.g., the encryption of personal data and the use of decentralized identity management and related solutions. Individuals can trust because there is no way for their data to be used without their explicit consent.
Trust	**Trust** refers to your ability to be vulnerable with another, your faith in the honesty of another (an individual, system, service, or process), and your belief in another's intention to meet their social, commercial, and civic commitments and obligations that they've made to you.[57,58]
Trust	**Trust Diamond** is the Trust Triangle with an additional point, the Governing

Diamond	Authority, the authority that sets rules and technology for verified credentials and specifies who is allowed to issue, hold, and verify them[59] See: **https://cpb-us-e1.wpmucdn.com/wordpressua.uark.edu/dist/5/444/files/2018/01/BCoE2022SS1FINAL.pdf**
Trust Framework	**Trust Framework** is a collection of best practices, principles, technologies, rules, regulations, standards, etc., that are established by a body of appointed or volunteer ecosystem leaders to oversee the governance of a service or systems approach or an ecosystem.
Trust Triangle	**Trust Triangle** represents the three parties—the Issuer, the Holder, and the Verifier—in a self-sovereign identity (SSI) organized relationship. The Issuer issues a Verifiable Credential. It provides the private key to the Holder and places a public key in the public register. When the Holder wants to assert their identity or present some information, the Holder will present all or a portion of their credential to the Verifier. The Verifier can then verify the authenticity of the assertion against the public registry. All of this is managed using state-of-the-art decentralized data storage and data cryptology. Note: An individual or enterprise can play dual roles. For instance, in the case of airlines, the airline issues a ticket to a Holder. The airline will also act as the Verifier when the Holder is checking in. When the Holder is going through airport security, the airline will still act as the Issuer, but the security authority will be the Verifier.
Verified Attribute	**Verified Attribute** is an attribute whose authenticity can be determined to be valid and accurate. This determination is made by a third-party assertion or by through a cryptographic process, like presentation and verification of a verified credential.
Verified Credential	**Verified Credential** is a privacy persevering open digital identity and authentic data management standard.[60] for representing information that can be verified as having been created by an issuer? The information is a collection of attributes associated with an item or person, like all the information on a driver's license, passport, or information about a person or a person's things. A holder presents verified credentials, typically with a smart wallet (but not always) to a verifying party. The verifying party can confirm the credential's authenticity by checking a distributed ledger, or the credential can self-verify. A credential is privacy-preserving because the holder can present the credential and assert claims about themselves and their data without the issuer's knowledge and without having to disclose their identity. As of this writing, there are several accepted standards for constructing a verified credential: JSON - JWT, JSON-LOS with LD Signature, ZKP-CL, and JSON-LD ZKP with BBS+.[61,62]
Verifier	**Verifier** is the party, also known as a relying party, that has been presented with a verified credential. The verifying party can confirm the credential's authenticity by checking a distributed ledger, or the credential can self-verify.
Web 3	**Web 3** coined by Gavin Wood in 2014, Web3 refers to a decentralized online ecosystem based on the blockchain.[63]
Web 5	**Web 5** a marketing term coined by Jack Dorsey to refer to the adding a new layer to the Internet to empower individuals to have control of their data, i.e., it is Web 2.0 + Web 3.0 with the added twist that individuals should have control of their data. This

	concept is not new. There is a decades-long history of trying to make this vision happen. Common historical terms include self-sovereign identity, digital ID, and authentic data.
Zero Knowledge Proof	**Zero Knowledge Proof** is a concept developed by three MID researchers in 1985.[64] is a process that enables an individual, i.e., a Holder, to authenticate themselves or assert their control over data (think authentic data) and for a verifier to verify the individual's identity or data claim without the individual having to reveal their private data—e.g., a password, PIN code, or credit card. The individual's private data never leaves their possession. The ZKP process assesses the probability that the claim is valid; it performs the operation enough times for the probability to be a near certainty. There are a number of ways to execute ZKP authentication, including proof of knowledge, pairing public and private encryption keys, witness-indistinguishable proof (WIP), multi-party computation, and ring signature. For example, the verifier can send an encrypted public key challenge request to the Holder. If the Holder is who they say they are, they will be in possession of the only encrypted private key that can respond to the challenge. The individual will receive their private key from the Issuer, e.g., a government, who initially validates the individual's identity and related data.

Let's Connect and Work Together

It is out of the scope of this article to discuss the interdependence of all these terms or what an organization needs to do to understand and operate them. For now, I'll leave you to meditate on them. The key is to remember that these terms are not not independent but interdependent; no one concept or term will negate the other, they wall work together. For instance, I reference numerous approaches to identity management in the above list of terms. All these approaches will coexist in the market for years, possibly decades, and not months.

I am confident of two things to head into 2023 and the future.

First, the idea of individual personal data empowerment is a worthy one to strive for; I want this for myself, my kids, family, friends, colleagues, all of us. We must find a way to give people the will, knowledge, and tools they need to make their voices effectively heard and to control how their personal data is produced, collected, protected, and used wherever it resides. Likewise, we must empower enterprises (B2C, B2B, B2B2C, etc.) and governments alike with the appropriate suite of products, services, tools, processes, business models, frameworks, and policies, to hear the people's voice and to innovate, engage, serve, and act responsibly and in accordance with individuals' preferences and consents.

Second, to achieve the first, it will be tough, if not impossible, to go it alone. Today's world is just too complex to tackle alone. What's needed are collaborative, trusted ecosystems (see the definition above) and environments where we all come together, including individuals, to make the idea of individual empowerment real while also recognizing that this can be profitably achieved. Doing good, and treating people with respect, are not mutually exclusive concepts.

In 2023, I hope to lead, join, and follow. I am excited to serve, collaborate, and make a difference. I hope to hear from you and to hear your vision, aspirations, and programs for the future; I'd also like to have the opportunity to share mine with you. Hopefully, we can find a way to work together and make a difference.

Notes

1. *Meditationes sacrae*.
2. Christensen et al., "Know Your Customers' 'Jobs to Be Done'."
3. Klement, "Know the Two Very Different Interpretations of Jobs to Be Done."
4. Berners-Lee, "I Invented the Web. Here Are Three Things We Need to Change to Save It | Tim Berners-Lee | Technology | The Guardian."
5. Angwin, Mattu, and Parris, "Facebook Doesn't Tell Users Everything It Really Knows About Them."
6. Internet World Stats and Facebook, "Facebook."
7. Union, "Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA Relevance)."
8. European Commission, "Digital Markets Act."
9. European Union, "Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA Relevance)."
10. Union, "Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital

Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA Relevance)."

11. Union, "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance)."
12. Gartner, "Gartner Identifies Top Five Trends in Privacy Through 2024."
13. Fogg, "Behavior Model."
14. "Decentralized Identifiers (DIDs) V1.0."
15. "Predators and Prey"; *The Death of Competition*.
16. European Commission, "Digital Markets Act."
17. Intersoft Consulting, "Art. 4 GDPR Definitions."
18. Intagliata, "Biometric Identifies You in a Heartbeat."
19. Grassi et al., "NIST Special Publication 800-63A Digital Identity Guidelines Enrollment and Identity Proofing Requirements."
20. European Union, "Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA Relevance)."
21. Union, "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance)."
22. Hagel and Rayport, "The Coming Battle for Customer Information."
23. Hagel and Singer, "Unbundling the Corporation."
24. Balkin, "Information Fiduciaries and the First Amendment."
25. Mills, "Who Owns the Future?"
26. European Commission, "General Data Protection Regulation One Year On."

27. Commission, “Data Sharing in the EU Common European Data Spaces (New Rules).”
28. Commission, “Data Governance Act Explained | Shaping Europe’s Digital Future.”
29. Hemmi, “Japan’s ’Information Banks’ to Let Users Cash in on Personal Data.”
30. Japan, “Release of the Guidelines of Certification Schemes Concerning Functions of Information Trust Ver. 1.0.”
31. Suokas, “Japanese Information Banks.”
32. Hafen, “Personal Data Cooperatives A New Data Governance Framework for Data Donations and Precision Health.”
33. Cramer, “6 Key Responsibilities of the Invaluable Data Steward.”
34. Flanagan, “Advancing Digital Agency.”
35. Hafen, “Personal Data Cooperatives A New Data Governance Framework for Data Donations and Precision Health.”
36. Cramer, “6 Key Responsibilities of the Invaluable Data Steward.”
37. Arenas et al., “Design Choices for Productive, Secure, Data-Intensive Research at Scale in the Cloud.”
38. Manohar, Ramesh, and Kapoor, “Understanding Data Stewardship.”
39. Flanagan, “Advancing Digital Agency.”
40. Flanagan.
41. Flanagan.
42. Flanagan.
43. Doctorow, “Adversarial Interoperability.”
44. Intersoft Consulting, “Art. 4 GDPR Definitions.”
45. European Union, “Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending

Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA Relevance)."

46. Dataswift, "How It Works."
47. Montjoye et al., "openPDS."
48. Mun et al., "Personal Data Vaults."
49. "Unlocking the Value of Personal Data."
50. "European Data Protection Supervisor."
51. Borgne, "In a Phygital World... - Awabot -."
52. Westin, *Privacy and Freedom.*
53. Meisells, "PD&I Market Assessment Interview with Adreinne Meisells at myPlanit."
54. Brandt, "PD&I Market Assessment Interview with Liz Brandt at Cntrl-Shfit."
55. Petronio, "Communication Boundary Management."
56. Thake, "Self-Sovereign Identity for Machines."
57. Gefen, "Reflections on the Dimensions of Trust and Trustworthiness Among Online Consumers."
58. Sitkin, "A Research Conversation."
59. Lacity and Carmel, "Implementing Self-Sovereign Identity (SSI) for a Digital Staff Passport at UK NHS."
60. W3C, "Verifiable Credentials Data Model 1.0."
61. Goldwasser, Micali, and Rackoff, "The Knowledge Complexity of Interactive Proof-Systems."
62. Camenisch and Lysyanskaya, "An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation."
63. Edelman, "2021 Edelman Trust Barometer."
64. Goldwasser, Micali, and Rackoff, "The Knowledge Complexity of Interactive Proof-Systems."

References

Angwin, Julia, Surya Mattu, and Terry Parris. “Facebook Doesn’t Tell Users Everything It Really Knows About Them.” *ProPublica*, December 2016.

Arenas, Diego, Jon Atkins, Claire Austin, David Beavan, Alvaro Cabrejas Egea, Steven Carlysle-Davies, Ian Carter, et al. “Design Choices for Productive, Secure, Data-Intensive Research at Scale in the Cloud.” arXiv, September 2019. **https://doi.org/10.48550/arXiv.1908.08737**.

Bacon, Francis. *Meditationes sacrae*. Londini.: Excusum impensis Humfredi Hooper, 1597.

Balkin, Jack. “Information Fiduciaries and the First Amendment.” *UC Davis Law Review* 49, no. 4 (April 2016): 1185–1221.

Berners-Lee, Tim. “I Invented the Web. Here Are Three Things We Need to Change to Save It | Tim Berners-Lee | Technology | The Guardian.” https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet, March 2017.

Borgne, Marine Le. “In a Phygital World... - Awabot -.” *Awabot*, May 2018.

Brandt, Liz. “PD&I Market Assessment Interview with Liz Brandt at Cntrl-Shfit,” September 2021.

Camenisch, Jan, and Anna Lysyanskaya. “An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation.” In *Advances in Cryptology EUROCRYPT 2001*, edited by Birgit Pfitzmann, 93–118. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2001. **https://doi.org/10.1007/3-540-44987-6_7**.

Christensen, Clayton M., Taddy Hall, Karen Dillon, and David S. Duncan. “Know Your Customers’ ‘Jobs to Be Done’.” *Harvard Business Review*, September 2016.

Commission, European. “Data Governance Act Explained | Shaping Europe’s Digital Future,” June 2022.

———. “Data Sharing in the EU Common European Data Spaces (New Rules).” *Have Your Say*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Data-sharing-in-the-EU-common-European-data-spaces-new-rules-_en, July 2020.

Cramer, Jonathan James. “6 Key Responsibilities of the Invaluable Data Steward,” March 2019.

Dataswift. “How It Works.” *Dataswift Docs*. https://docs.dataswift.io/, January 2022.

“Decentralized Identifiers (DIDs) V1.0.” *W3C*. https://www.w3.org/TR/did-core/, March 2021.

Doctorow, Cory. “Adversarial Interoperability.” *Electronic Frontier Foundation*, October 2019.

Edelman. “2021 Edelman Trust Barometer.” https://www.edelman.com/trust/2021-trust-barometer, January 2021.

European Commission. “Digital Markets Act: Ensuring Fair and Open Digital Markets.” Text. *European Commission - European Commission*, October 2022.

———. “General Data Protection Regulation One Year On.” Text. *European Commission - European Commission*, June 2019.

“European Data Protection Supervisor.” *European Data Protection Supervisor*. https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_en, 2017.

European Union. “Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA Relevance),” May 2022.

Flanagan, Anne Josephine. “Advancing Digital Agency: The Power of Data Intermediaries.” Geneva, Switzerland: World Economic Forum, February 2022.

Fogg, BJ. “Behavior Model.” *Fogg Behavior Model*. https://behaviormodel.org/, October 2021.

Gartner. “Gartner Identifies Top Five Trends in Privacy Through 2024.” Newsroom. *Gartner*, May 2022.

Gefen, David. “Reflections on the Dimensions of Trust and Trustworthiness Among Online Consumers.” *Database for Advances in Information Systems* 33, no. 3 (2002): 38–53.

Goldwasser, S, S Micali, and C Rackoff. “The Knowledge Complexity of Interactive Proof-Systems.” In *Proceedings of the Seventeenth Annual ACM Symposium on*

Theory of Computing, 291–304. STOC '85. New York, NY, USA: Association for Computing Machinery, 1985. **https://doi.org/10.1145/22145.22178**.

Grassi, Paul A., James L. Fenton, Naomi B. Lefkovitz, Jamie M. Danker, Yee-Yin Choong, Kristen K. Greene, and Mary F. Theofanos. "NIST Special Publication 800-63A Digital Identity Guidelines Enrollment and Identity Proofing Requirements." Washington, D.C.: National Institute of Standards and Technology, March 2020.

Hafen, Ernst. "Personal Data Cooperatives A New Data Governance Framework for Data Donations and Precision Health." In *The Ethics of Medical Data Donation*, edited by Jenny Krutzinna and Luciano Floridi, 141–49. Philosophical Studies Series. Cham: Springer International Publishing, 2019. **https://doi.org/10.1007/978-3-030-04363-6_9**.

Hagel, John, and Jeffery Rayport. "The Coming Battle for Customer Information." *Harvard Business Review*, 1997/January-February.

Hagel, John, and Marc Singer. "Unbundling the Corporation." *Harvard Business Review*, March 1999.

Hemmi, Junya. "Japan's 'Information Banks' to Let Users Cash in on Personal Data." *Nikkei Asia*, May 2019.

Intagliata, Christopher. "Biometric Identifies You in a Heartbeat." *Scientific American*, October 2017.

Internet World Stats, and Facebook. "Facebook: Global Penetration by Region 2022." *Statista*, May 2022.

Intersoft Consulting. "Art. 4 GDPR Definitions." *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/art-4-gdpr/, August 2016.

Japan, MIC. "Release of the Guidelines of Certification Schemes Concerning Functions of Information Trust Ver. 1.0." *Ministry of Internal Affairs and Communication Japan*. https://www.meti.go.jp/english/press/2018/0626_002.html, June 2018.

Klement, Alan. "Know the Two Very Different Interpretations of Jobs to Be Done." *Medium*. https://jtbd.info/know-the-two-very-different-interpretations-of-jobs-to-be-done-5a18b748bd89#:~:text=The%20two%20versions%20of%20Job,his%20patented%20Outcome%20Driven%20Innovation, February 2020.

Lacity, Mary, and Erran Carmel. “Implementing Self-Sovereign Identity (SSI) for a Digital Staff Passport at UK NHS,” 2022, 27.

Manohar, Siddharth, Aditi Ramesh, and Astha Kapoor. “Understanding Data Stewardship: Taxonomy and Use Cases.” The Data Economy Lab, June 2020.

Meisells, Adrienne. “PD&I Market Assessment Interview with Adreinne Meisells at myPlanit,” December 2021.

Mills, Stuart. “Who Owns the Future? Data Trusts, Data Commons, and the Future of Data Ownership.” {{SSRN Scholarly Paper}}. Rochester, NY: Social Science Research Network, September 2019. **https://doi.org/10.2139/ssrn.3437936**.

Montjoye, Yves-Alexandre de, Erez Shmueli, Samuel S. Wang, and Alex Sandy Pentland. “openPDS: Protecting the Privacy of Metadata Through SafeAnswers.” *PLOS ONE* 9, no. 7 (July 2014): e98790. **https://doi.org/10.1371/journal.pone.0098790**.

Moore, James F. “Predators and Prey: A New Ecology of Competition.” *Harvard Business Review*, May 1993.

———. *The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems*. Reprint edition. New York: Harper Paperbacks, 1997.

Mun, Min, Shuai Hao, Nilesh Mishra, Katie Shilton, Jeff Burke, Deborah Estrin, Mark Hansen, and Ramesh Govindan. “Personal Data Vaults: A Locus of Control for Personal Data Streams.” In *6th International Conference, CoNEXT*, 1–12. Philadelphia, 2010.

Petronio, Sandra. “Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples.” *Communication Theory* 1, no. 4 (November 1991): 311–35. **https://doi.org/10.1111/j.1468-2885.1991.tb00023.x**.

Sitkin, Sim. “A Research Conversation: Trust, Courage, Privacy and Personal Data,” January 2022.

Suokas, Jyrki. “Japanese Information Banks.” *MyData 2019*, September 2019.

Thake, Max. “Self-Sovereign Identity for Machines.” *Peaq*, February 2022.

Union, European. “Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital

Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA Relevance),” September 2022.

———. “Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance),” October 2022.

“Unlocking the Value of Personal Data: From Collection to Usage.” World Economic Forum, February 2013.

W3C. “Verifiable Credentials Data Model 1.0.” https://www.w3.org/TR/vc-data-model/, May 2021.

Westin, Alan F. *Privacy and Freedom.* New York: Atheneum, 1967.