*[DRAFT]*

# BIT Supplementary Document

Version 1.0

**Editors:** Paul Knowles, John Wunderlich, Ken Klingenstein

## Contents

*[DRAFT]*

# Introduction

The Blinding Identity Taxonomy (BIT) is a fundamental resource developed by the Kantara Initiative, serving the identity and information-sharing community. It is pivotal in aiding policymakers and technologists in making informed decisions regarding applying blinding techniques to datasets containing Personally Identifiable Information (PII) attributes. The primary objective of the BIT is to provide practical guidance for professionals involved in profile and schema development. Its purpose is to mark PII attributes within datasets to enhance the protection of individual identities.

The BIT offers a systematic approach to flag specific elements that necessitate cryptographic encoding to mitigate the risk of identifying data principals. Once these elements are either encrypted or excluded, the dataset achieves a state of 'blinding,' meaning that adversaries with access to the dataset cannot discern data principals.

This supplementary document complements the BIT by providing detailed insights into its 49 categories, offering comprehensive definitions, examples, considerations, privacy implications, and special notes for each BIT class. It is an essential reference for practitioners wanting to reduce risk, meet business goals, safely handle datasets containing identifiable information, and seek to implement adequate data blinding techniques, thereby reducing the risk of privacy breaches and ensuring compliance with data protection regulations.

By offering a deeper understanding of the BIT categories and their implications, this supplementary document empowers organizations to safeguard sensitive information, bolster data privacy, and make their datasets more secure for various purposes. It encourages collaboration and knowledge sharing across distributed data ecosystems, fostering the development of profiles and schemas that facilitate the adoption of the Blinding Identity Taxonomy.

# Detailed Descriptions of Each BIT Category

This section comprehensively describes the 49 Blinding Identity Taxonomy (BIT) field categories, offering insights into the nature and significance of each. It provides definitions, practical examples, considerations, privacy implications, and special notes for every BIT category. Whether you are a policymaker, technologist, data scientist, or privacy professional, this section is a valuable reference to understand each BIT category and its role in enhancing data privacy and security. Explore these descriptions to make informed decisions about applying blinding techniques to datasets containing Personally Identifiable Information (PII) attributes.

*[DRAFT]*

## 1. Names

"Names" refers to the identifying labels given to an individual or an entity in the context of PII. This category encompasses personal names (first and last names), full names, pseudonyms, aliases, and names of entities such as businesses or organizations.

**Examples:**

- Personal Names: "John Smith", "Maria Garcia"
- Full Names: "Alexandra Elizabeth Johnson"
- Pseudonyms/Aliases: "Mark Twain" (for Samuel Clemens)
- Entity Names: "Acme Corporation", "Green Valley Nonprofit"

**Considerations:**

- Names are fundamental identifiers used in various contexts, from official documents to online platforms.
- First names alone, prevalent ones, may only constitute PII if combined with other data (e.g., address, birth date).
- Cultural variations in naming conventions should be considered in profile and schema designs, as they can affect the identification potential of a name.
- Pseudonyms are often used for protection (e.g., by activists or individuals in sensitive situations) and require special handling to avoid unintended exposure.

**Privacy Implications:**

- While names alone may not uniquely identify an individual, they can lead to privacy concerns when linked with other data elements.
- Names are vital to tracking, profiling, or locating a person, primarily when combined with other identifiers.
- Compliance with data protection regulations is essential, particularly concerning consent, storage limitation, and purpose specification.
- Handle the use and storage of full names with caution to prevent privacy breaches.
- Anonymization or pseudonymization may be necessary in contexts where individual identification is not required.

**Special Notes:**

- In some cases, names can be de-identified or used in a pseudonymized form to reduce privacy risks.
- Ensure that the storage and processing of names in profiles and schemas align with the purpose for which individuals gave consent and offered their data.

## 2. Physical Address(es)

Physical address refers to the specific geographical location of an individual or an entity, including street addresses, city, state, country, and any other information that can pinpoint a particular physical location.

**Examples:**

- Residential Address: 123 Main St, Springfield, IL, USA
- Business Address: 456 Oak Ave, Suite 100, Metropolis, NY, USA
- Postal Address: P.O. Box 789, Gotham City, NJ, USA

**Considerations:**

- Physical addresses are crucial for many services, from shipping to service provision.
- They are often used with other PII-like names to identify individuals uniquely.
- Consider international variations in address formats when processing data globally.
- Addresses may be sensitive in specific contexts, such as for protected individuals or secret locations.
- The street number/name and the postal code are particularly sensitive, while regional information like town, city, state, county, province, and country is usually less sensitive.

**Privacy Implications:**

- Physical addresses can lead to direct physical access to an individual and thus pose significant privacy and security concerns.
- Including an address in a data set can increase the risk of stalking, harassment, or unwanted contact.
- It's essential to ensure that addresses are only collected and processed when necessary and with explicit consent.
- Appropriate security measures should be in place to protect this data from unauthorized access.

**Special Notes:**

- In some contexts, the full Address may not be necessary, and using a partial address or a generalized location can be appropriate.
- Consider anonymizing or pseudonymizing addresses, especially when the exact location is unnecessary for the service or analysis.
- The storage and processing of physical addresses in profiles and schemas must align with the purpose for which individuals consented to provide their data.
- While street number/name and postal code are the most sensitive components, broader regional details can still contribute to identifying an individual when combined with other data elements.

## 3. E-mail Address(es)

E-mail addresses are unique identifiers used for electronic communication. They typically include a local part, an "@" symbol, and a domain part. E-mail addresses can uniquely identify individuals or entities and serve various purposes in personal, professional, and business contexts.

**Examples:**

- Personal Email: jane.doe@example.com
- Professional Email: johndoe@company.com
- Anonymous Email: user12345@anonymousmail.com

**Considerations:**

- E-mail addresses are pervasive in online transactions and communications.
- They often serve as user IDs for various online services and platforms.
- The format of an e-mail address can provide hints about its owner, such as their name, employer, or role.
- E-mail addresses are often linked to other personal data, making them a significant identifier in data breaches.

**Privacy Implications:**

- E-mail addresses can access an individual's online identity and activity.
- They are a primary target in phishing attacks and other forms of cybercrime.
- Consent and purpose specification are crucial when collecting and processing e-mail addresses.
- Including an email address in a dataset can expose individuals to spam, scams, or other unwanted communications.

**Special Notes:**

- Consider using email aliases or temporary e-mail addresses when long-term identification is unnecessary.
- Ensure that the collection and use of email addresses in profiles and schemas are consistent with the consent provided by the individual and the purpose of the data collection.

## 4. Telephone Number(s)

Telephone numbers serve as a direct line of communication to an individual or entity. They include landline, mobile, and VoIP numbers. Telephone numbers are unique and can be tied directly to an individual, a household, or a business.

**Examples:**

- Home Landline: +1-202-555-0173
- Mobile Phone: +44-7700-900123
- Business Line: +61-3-9876-5432

**Considerations:**

- Telephone numbers are key identifiers in communication and often serve as a contact point for personal, business, and emergency purposes.
- Profiles and schemas can actively link telephone numbers to other personal data like names and addresses.
- The format and length of telephone numbers vary internationally.

- Mobile numbers are often more sensitive than landline numbers as they are usually tied directly to an individual.

**Privacy Implications:**

- Telephone numbers can expose individuals to unsolicited calls, marketing, or scams.
- They are often used for identity verification processes, making them sensitive in case of data breaches.
- Collecting and processing telephone numbers should be done with explicit consent and for a clear purpose.
- Appropriate security measures are essential to protect this data from unauthorized access.

**Special Notes:**

- Consider alternative means of communication where telephone contact is not necessary.
- Collect and process telephone numbers in profiles and schemas to align with the individual's consent and the specific purpose for which they provided the data.
- Consider anonymizing or pseudonymizing telephone numbers in scenarios where direct contact is unnecessary.

## 5. Postal Code(s)

Postal codes refer to a series of letters, numbers, or both used by postal services to aid in the sorting and delivery of mail. They generally represent a geographic area ranging from a few buildings to an entire district.

**Examples:**

- Residential Area: 90210 (Beverly Hills, CA, USA)
- Business District: EC1A 1BB (London, UK)
- Rural Route: T0L 0Z0 (Southern Alberta, Canada)

**Considerations:**

- Postal codes are less specific than physical addresses but still provide location information.
- Often, entities use postal codes for demographic analysis, marketing purposes, and service delivery.
- The granularity of postal codes can vary significantly between countries and even within the same country.
- Postal codes can be sensitive in specific contexts, such as when associated with high-profile locations or individuals.

**Privacy Implications:**

- Postal codes can indirectly reveal demographic information about an individual, such as their general living area, socioeconomic status, or lifestyle.

- They are commonly used with other PII to enhance the accuracy of location-based services or analytics.
- Entities should avoid privacy infringements when using postal codes for profiling or targeted advertising.
- Implement data protection measures to ensure that postal code data is not misused.

**Special Notes:**

- In some scenarios, only partial postal codes might be necessary for service provision or analysis.
- Anonymizing or pseudonymizing postal code information can reduce privacy risks, especially in datasets where specific location information is not essential.
- The collection and processing of postal codes in profiles and schemas must be consistent with the purposes for which the individual has consented.

## 6. Personal Software Application Handles

Personal Software Application Handles are unique identifiers or usernames that individuals use in various software applications. These handles encompass user IDs, screen names, or nicknames utilized across online platforms, including social media, gaming platforms, and other digital forums.

**Examples:**

- Skype Handle: johndoe123
- Slack Username: @techguru
- RocketChat ID: maria_innovator
- Gaming Tag: DragonSlayer88
- Social Media Username: @naturelover

**Considerations:**

- Software application handles, being unique, often allow for tracing back to an individual's identity.
- They are used across various platforms and can link an individual's activities across different services.
- Handles can reveal personal interests, professions, or affiliations, depending on their nature and use.
- Collecting, processing, or displaying software application handles requires careful handling to prevent the unintended identification of individuals.

**Privacy Implications:**

- Handles can be a source of privacy concerns if used to track or profile individuals across platforms.
- They can lead to unwanted exposure or harassment, especially if linked with other personal information.

- Protecting the privacy of handles is crucial, particularly in platforms where users expect a degree of anonymity.
- Appropriate privacy controls should be in place for applications that use these handles, especially in contexts where users might be vulnerable.

**Special Notes:**

- Consider anonymizing or pseudonymizing handles in datasets where individual identification is not necessary.
- Ensure that the collection and processing of application handles in profiles and schemas align with the users' consent and the intended purpose of data collection.
- The application's nature and the context of handle usage significantly affect its privacy implications.

## 7. Profile Pages

Profile Pages refer to personal web pages or segments within websites, applications, or social media platforms designed to represent an individual's or entity's identity, interests, and activities. These pages often contain a combination of personal information, such as names, photos, biographical details, and other identifiers.

**Examples:**

- Social Media Profiles: Facebook profile page, LinkedIn account page.
- Professional Websites: A personal portfolio website or a professional biography page.
- Blogs and Personal Websites: A personal blog page with an 'About Me' section.

**Considerations:**

- Profile pages typically aggregate various personal information, making them rich sources of PII.
- They may contain links to other personal digital spaces or reference additional personal data.
- The visibility and accessibility of profile pages vary, with some being public and others restricted to specific networks or groups.

**Privacy Implications:**

- Profile pages can provide comprehensive insights into an individual's personal and professional life, leading to privacy concerns.
- Profiles on these pages may become targets for profiling, identity theft, or social engineering attacks.
- Managing privacy settings and the type of information shared on profile pages is crucial for protecting personal information.
- Ensure that the collection and use of information from profile pages in profiles and schemas align with the purpose consented to by the individual.

**Special Notes:**

- In some scenarios, anonymizing or limiting the amount of personal information on profile pages may be advisable to minimize privacy risks.
- It's essential to regularly review and update the privacy settings and contents of profile pages to maintain privacy and data accuracy.

## 8. Passport Numbers

Passport Numbers refer to the unique identification numbers assigned to an individual's passport document. Each passport number is globally unique and a critical international travel identifier. As authoritative issuing entities, governments provide these numbers, affirming the passport's validity.

**Examples:**

- A series of alphanumeric characters typically found on the identification page of a passport.
- Different countries have different formats, but they all serve the same purpose of uniquely identifying a passport.

**Considerations:**

- Passport numbers directly linked to an individual's identity and nationality constitute sensitive PII.
- Passport numbers are often necessary for international travel and visa applications and occasionally for identity verification in financial or official transactions.
- The format and length of passport numbers vary depending on the issuing country.

**Privacy Implications:**

- Unauthorized access to passport numbers can lead to identity fraud and other security breaches.
- They should be stored and processed with high-security standards due to their sensitivity.
- When collecting passport data, gather only the minimum necessary information and protect it against unauthorized access.

**Special Notes:**

- The handling of passport numbers must comply with international data protection and privacy regulations.
- Consider pseudonymization or anonymization in scenarios where direct identification is not necessary.
- Ensure that the collection and processing of passport numbers in profiles and schemas align with the purpose for which individuals provided their data and consented.

## 9. Social Security Numbers

Social Security Numbers (SSNs) are unique identification numbers issued by governments, primarily used for tracking individuals for social security purposes and taxation. The Social Security Administration issues SSNs in the United States.

**Examples:**

- United States SSN: 123-45-6789 (format varies by country)

**Considerations:**

- SSNs are highly sensitive and uniquely identify individuals.
- Employers, banks, and government services often require SSNs.
- In the U.S., SSNs are crucial for credit reporting and background checks.

**Privacy Implications:**

- Due to their wide usage in identity verification, identity thieves and financial fraudsters often target SSNs.
- Misuse of SSNs can lead to serious privacy breaches and financial harm.
- Limiting SSN collection and ensuring robust security measures in handling them is crucial.
- Ensure that the collection and processing of SSNs in profiles and schemas strictly align with the consent given by individuals and the intended purpose of data use.

**Special Notes:**

- Consider alternative identifiers where possible to reduce reliance on SSNs.
- Implement anonymization or pseudonymization of SSNs when their complete numbers are not essential.
- Be aware of legal restrictions and compliance requirements regarding the collection, storage, and use of SSNs.

## 10. National Insurance Numbers

National Insurance Numbers (NINs) are unique identifiers assigned to individuals in various countries for social security and taxation purposes. These numbers are crucial for government services, employment, and accessing social welfare benefits.

**Examples:**

- UK National Insurance Number: AB123456C
- Social Insurance Number in Canada: 123 456 789

**Considerations:**

- NINs vary in format and name depending on the country.
- These numbers are essential for employment, tax purposes, and accessing government services.

- NINs require confidential handling and high security due to their sensitive nature.

**Privacy Implications:**

- NINs can be used for identity verification and are highly sensitive due to their financial and personal information connection.
- Misuse of NINs can lead to identity theft, financial fraud, and unauthorized access to personal information.
- Collecting and processing NINs only for legitimate purposes and with proper consent is crucial.

**Special Notes:**

- Ensure the storage and processing of NINs in profiles and schemas align with the purpose for which individuals consented to provide their data.
- To minimize privacy risks, use anonymization or pseudonymization techniques where full NINs are unnecessary.

## 11. Driving License Numbers

Driving License Numbers are unique identifiers assigned to an individual's driver's license. A governmental body responsible for vehicle regulation and driver licensing typically issues these numbers. They are unique to each license holder and can vary in format depending on the issuing country or state.

**Examples:**

- A US driver's license number like 'S123-4567-8910'.
- A UK driving license number like 'SMITH607045SM9IJ 35'.

**Considerations:**

- Driving license numbers are often used as a form of identification in governmental and commercial contexts.
- The format and information contained in the license number can vary significantly from one jurisdiction to another.
- Detailed personal information, such as address, birth date, and sometimes even biometric data, can link to these numbers.

**Privacy Implications:**

- Driving license numbers are sensitive PII and can be targeted for identity theft and fraud.
- These numbers should be used and stored with caution, ensuring that they are only collected and retained when necessary and with proper consent.
- They should be adequately protected to prevent unauthorized access.

**Special Notes:**

- When processing driving license numbers, aligning with the purpose for which individuals have consented to provide their data is essential.

- Implement anonymization or pseudonymization techniques when the full license number is unnecessary for the intended service or analysis.

## 12. Vehicle Registration Numbers

Vehicle Registration Numbers are unique identifiers assigned to motor vehicles by government authorities. These numbers are found on vehicle registration documents and license plates, serving as an official record of a vehicle's legal registration.

**Examples:**

- License plate numbers: 'ABC 1234' or 'XYZ-5678'
- Registration numbers on documents: 'VRN123456789'

**Considerations:**

- Vehicle registration numbers can be publicly visible and potentially lead to the tracing of the vehicle owner, raising privacy concerns.
- They often serve legal purposes, including handling traffic violations, insurance claims, and verifying vehicle ownership.
- Different countries and regions have varying formats and regulations governing vehicle registration numbers.

**Privacy Implications:**

- Vehicle registration numbers can reveal the owner's identity and sometimes serve as tools for tracking or profiling.
- Protecting this data from unauthorized access and misuse is crucial, especially in vehicle sales or services that involve exchanging registration information.
- Data protection measures should ensure that vehicle registration numbers are used only for legitimate and authorized purposes.

**Special Notes:**

- To protect privacy, consider using partial or anonymized registration numbers when identifying a vehicle.
- Align the collection and processing of vehicle registration numbers in profiles and schemas with the vehicle owner's consent and the purpose of data collection.

## 13. Bank Account Numbers

Bank Account Numbers refer to the unique numerical identifiers associated with an individual's or organization's bank account. Individuals and organizations use these numbers for financial transactions, withdrawals, deposits, and other banking activities.

**Examples:**

- Personal Savings Account: 1234567890
- Business Checking Account: 9876543210

- International Bank Account Number (IBAN): GB29NWBK60161331926819

**Considerations:**

- Bank account numbers are critical in financial transactions and are frequently associated with personal or business identities.
- Handle them securely to prevent unauthorized access and fraud.
- Sometimes, you may not need the full bank account number, and you can use partial numbers or tokenization for added security.

**Privacy Implications:**

- They are directly linked to an individual's or organization's financial assets, making them susceptible.
- Mishandling of bank account numbers can lead to financial fraud, identity theft, and unauthorized access to funds.
- Strict security measures must be in place to protect this data from breaches.

**Special Notes:**

- Tokenization or partial masking of bank account numbers can be considered for enhanced security, especially when full numbers are not required.
- Compliance with financial regulations and data protection laws is essential when handling bank account numbers.
- Ensure that the collection and processing of bank account numbers align with the individual's consent and the intended financial transactions.

## 14. Financial Institution Card Numbers

Financial Institution Card Numbers encompass various card numbers issued by financial institutions, including credit and debit card numbers. They facilitate electronic financial transactions and payments.

**Examples:**

- Credit Card Number: 1234 5678 9012 3456
- Debit Card Number: 9876 5432 1098 7654

**Considerations:**

- Financial institution card numbers are essential for electronic payments and transactions.
- They are linked to an individual's or entity's financial account and may include sensitive financial information.

**Privacy Implications:**

- Financial institution card numbers constitute sensitive PII as an identifier linked to an individual's financial assets.
- Protecting these numbers from unauthorized access and fraud is crucial.

- Strict security measures are necessary when handling, storing, or processing these numbers.
- Consider using anonymization or tokenization techniques to enhance security and privacy.

**Special Notes:**

- In some cases, only partial card numbers or tokens may be required for specific transactions, enhancing security and reducing exposure to whole card numbers.

## 15. Personal Identification Numbers (PINs)

Personal Identification Numbers (PINs) are confidential numeric codes for authentication and access control. They typically consist of a series of digits and are employed to verify the identity of individuals when accessing secured accounts, electronic devices, or protected areas.

**Examples:**

- ATM PIN: A 4 to 6-digit code used to access an individual's bank account at an Automated Teller Machine (ATM).
- Smartphone PIN: A numeric code used to unlock a mobile device or access sensitive data.
- Security System PIN: A code used to arm or disarm a security system for homes or businesses.

**Considerations:**

- PINs are a critical security mechanism to protect personal or confidential information access.
- They are often used with other authentication factors, such as passwords or biometric data, to enhance security.
- The length and complexity of PINs can vary, with longer and more complex codes providing greater security.

**Privacy Implications:**

- PINs are susceptible and confidential as they grant access to secure accounts and devices.
- Unauthorized access to a PIN can lead to identity theft, financial fraud, or unauthorized use of personal information.
- Securely storing and transmitting PINs is essential to prevent data breaches and unauthorized access.

**Special Notes:**

- Individuals should use unique and secure PINs for different purposes to minimize the risk of unauthorized access.
- The storage and handling of PINs should adhere to strict security standards to protect individuals' privacy and security.

- Consider multi-factor authentication methods to enhance security when using PINs for access control.

## 16. Private Keys / Master Keys

Private Keys and Master Keys are cryptographic elements crucial in various encryption and security protocols. These keys are typically paired with public keys and are essential for securing digital communications and data.

**Examples:**

- SSL/TLS Certificates: Private keys establish secure connections between web servers and clients, ensuring the confidentiality and integrity of data transmitted over the internet.
- Email Encryption: PGP (Pretty Good Privacy) and S/MIME (Secure/Multipurpose Internet Mail Extensions) use private keys to decrypt and encrypt email messages.
- Blockchain Wallets: Cryptocurrency wallets use private keys to sign transactions and control access to digital assets.
- Secure File Storage: Some cloud storage services use private keys to encrypt files before uploading them to the cloud.

**Considerations:**

- Private keys are typically kept secret and should never be shared or exposed to unauthorized individuals.
- Loss or compromise of a private key can result in unauthorized access to sensitive data, including financial assets or personal information.
- Proper key management practices, including secure storage and backup, are critical to protect private keys from loss or theft.

**Privacy Implications:**

- Private keys are pivotal in ensuring digital communications and data confidentiality and security.
- Compromised private keys can lead to data breaches, unauthorized access, and privacy violations.
- Individuals and organizations must safeguard their private keys to prevent security incidents.

**Special Notes:**

- Cryptographic applications, including digital signatures and secure communication, use private keys.
- Master keys are used for encrypting or decrypting other keys, such as data encryption keys, adding a layer of security.
- Correctly generated and managed private keys are essential for maintaining the security and privacy of digital systems and communications.

## 17. Symmetric Keys

Symmetric Keys refer to a category of cryptographic keys used in encryption and decryption processes. They are mathematically related, with the same key used for both functions, hence the term "symmetric." Many processors widely use symmetric encryption algorithms to secure data.

**Examples:**

- Examples of symmetric encryption algorithms include:
    - Advanced Encryption Standard (AES)
    - Data Encryption Standard (DES)
    - Triple DES (3DES).

**Considerations:**

- Symmetric keys are typically faster than asymmetric keys (public-private key pairs) for encryption and decryption operations.
- The security of symmetric keys relies on keeping the key secret. If an attacker gains access to the key, they can decrypt the data.
- Key management is crucial for securely using symmetric keys, including key generation, distribution, and storage.

**Privacy Implications:**

- Compromising a symmetric key can lead to unauthorized access to encrypted data, potentially exposing sensitive information.
- Protecting symmetric keys is essential to maintain the confidentiality and integrity of data.

**Special Notes:**

- Symmetric encryption is often used for securing data in transit (e.g., during network communication) and data at rest (e.g., stored on a disk).
- Secure key exchange mechanisms are employed to transmit symmetric keys when needed for encryption and decryption.
- Careful key management practices are essential to prevent unauthorized access to symmetric keys and the data they protect.

## 18. Public Keys

Public Keys are cryptographic keys used in asymmetric encryption systems. They are part of a key pair, with the corresponding private key being the other half. Users openly share public keys, which encrypt data and require the corresponding private key for decryption.

**Examples:**

- RSA Public Key: A widely used public key algorithm.
- ECC (Elliptic Curve Cryptography) Public Key: Known for its efficiency and security.

**Considerations:**

- Users openly share public keys for distribution.
- They are vital in secure communication, digital signatures, and authentication.
- The security of the entire encryption system relies on the private key remaining confidential.

**Privacy Implications:**

- While public keys may not reveal much about an individual, their security is crucial for protecting sensitive data.
- Compromising a private key can lead to unauthorized access and data breaches.

**Special Notes:**

- Modern encryption systems rely on public keys, which find applications in various areas, including secure messaging, secure browsing (HTTPS), and digital signatures.
- Protecting the private key associated with a public key is paramount to maintaining security and privacy.

## 19. Link Secrets

Link Secrets are confidential tokens or keys to establish secure links or connections between entities in a networked environment, such as devices, applications, or users. These secrets ensure data confidentiality, integrity, and authentication during data transmission.

**Examples:**

- Authentication Tokens: Generated tokens during user login processes to verify identity.
- API Keys: Keys used by applications to authenticate and access services or resources.
- Secure Sockets Layer (SSL) Certificates: Certificates used to secure web connections.

**Considerations:**

- Link Secrets are essential for securing communications, including user authentication and data encryption.
- Losing or compromising link secrets can lead to unauthorized access and data breaches.
- Apply proper access controls and encryption techniques to protect these secrets.

**Privacy Implications:**

- Link secrets are sensitive because they enable secure access to networks and data.
- Unauthorized access to link secrets can result in data breaches and privacy violations.
- Safeguarding link secrets is crucial to maintain data security and user privacy.

**Special Notes:**

- Implement robust security practices to protect link secrets, including encryption, access controls, and regular key rotation.

- In cases of compromise or suspected compromise, revoke and replace link secrets promptly to maintain security.
- Follow industry best practices and standards for securing link secrets in different contexts, such as web applications or IoT devices.

## 20. Decentralized Identifiers (DIDs)

Decentralized Identifiers (DIDs) are unique and self-owned identifiers in decentralized networks. They represent individuals, entities, or objects and enable secure, privacy-preserving interactions without relying on central authorities. DIDs are a crucial component of decentralized identity systems.

**Examples:**

- DID: did:example:123
- DID URL: did:example:123#keys-1
- Verifiable Credential issued to a DID

**Considerations:**

- DIDs provide individuals with control over their digital identities, enhancing privacy.
- These identifiers can link to additional data, such as public keys, service endpoints, or biometric information.
- Adoption of specific DID methods and standards can vary, affecting interoperability.

**Privacy Implications:**

- DIDs empower individuals to manage their digital identifiers securely, reducing the risk of privacy breaches.
- Privacy concerns may arise when linked data, such as public keys or credentials, needs to be properly secured.
- Proper management and secure data storage are essential to mitigate privacy risks.

**Special Notes:**

- The choice of DID methods and associated specifications can impact the security and privacy of DIDs.
- Implement robust security practices for managing keys and endpoints linked to DIDs.
- When collecting and processing DIDs in profiles and schemas, ensure alignment with user consent and intended data collection purposes.

## 21. Employee Identifiers

Employee Identifiers refer to unique codes or numbers assigned to individuals within an organization to facilitate identification and management. These identifiers serve various administrative purposes, including human resources, access control, and regulatory compliance, and may also encompass identifiers from benefits providers like pension plans.

**Examples:**

- Employee ID: A unique identification number assigned to each employee within an organization.
- Professional License Numbers: Identifiers issued to employees in regulated professions, such as healthcare or law.
- Badge Number: A distinct number or code on employee badges or identification cards.
- Staff Code: A specific code assigned to staff members for identification and administrative purposes.
- Worker's Union Membership Numbers: Identification numbers assigned to employees who are members of worker's unions.
- Benefits Provider Identifiers: Identifiers from benefits providers, such as pension plans, for employee benefits and compensation management.

**Considerations:**

- Employee Identifiers are essential for efficient management of personnel within an organization.
- The nature and format of these identifiers may vary across industries and organizations.
- Privacy and security measures should be in place to protect employee identifiers from unauthorized access or misuse.
- Compliance with regulations regarding the handling of sensitive employee data is crucial.

**Privacy Implications:**

- Mishandling or exposure of employee identifiers can lead to privacy breaches and identity-related risks.
- Safeguarding these identifiers is essential to protect employees' personal information.
- Organizations should have policies and controls to ensure responsible handling of employee identifiers.

**Special Notes:**

- Consider anonymization or pseudonymization techniques when the full employee identifiers are unnecessary for specific HR or payroll functions.
- Compliance with industry-specific regulations, such as those governing healthcare or legal professions, may impose additional requirements on handling professional license numbers.

## 22. Account Identifiers

Account Identifiers refer to unique codes or numbers assigned to individuals or entities to access services, conduct transactions, or identify account holders. These identifiers, excluding Bank Account Identifiers, are used across various sectors and are crucial in managing and securing accounts.

**Examples:**

- Library Card Numbers: Library card numbers are unique identifiers assigned to library users to access library services and borrow books. Examples include "LIBCARD5678" or "LIBUSER123."
- Customer Account Numbers: Customer account numbers are used in businesses to identify individual customers and their transactions. Examples include "CUST-7890" or "ACCT-12345."

**Considerations:**

- Account identifiers are essential for managing accounts, access control, and personalized services.
- Protecting the confidentiality of account identifiers is crucial to prevent unauthorized access.
- To avoid exposure or misuse, individuals and organizations should handle account identifiers carefully, as they can lead to the identification of individuals.
- Compliance with data protection regulations is essential when collecting and processing account identifiers.

**Privacy Implications:**

- Account identifiers often linked to personal information and account activities can pose privacy concerns if mishandled.
- Unauthorized access to account identifiers can lead to identity theft or fraud.
- Proper security measures and consent should be in place to collect and use account identifiers.

## 23. Government Identifiers

Government Identifiers refer to unique identification numbers, cards, or other artifacts issued by a government to a natural person or an entity. These identifiers are primarily used for official government purposes and are often crucial proof of identity.

**Examples:**

- National ID Numbers: A unique identification number issued by a government to its citizens or residents for identification purposes. Examples include Computerised National Identity Card (CNIC) numbers in Pakistan, Aadhaar numbers in India, and NRIC numbers in Singapore.
- Voter ID Numbers: Identification numbers issued to eligible voters to authenticate their eligibility to vote in elections.
- Taxpayer Identification Numbers (TINs): Unique numbers assigned to individuals or entities for tax-related purposes, such as filing income tax returns. Examples include 'Codice fiscale' used as TINs in Italy.
- Military Service Numbers: Identifiers assigned to individuals who serve in the military to track their service records and entitlements.
- Resident Permit Numbers: Identification numbers issued to non-citizens or non-residents to regulate their stay or work within the country.

**Considerations:**

- Government identifiers are often sensitive PII as they are directly linked to an individual's identity and issued by authoritative government bodies.
- People and entities typically use them for critical purposes such as taxation, voting, social services, and national security.
- The handling and protection of government identifiers should adhere to strict security and privacy measures to prevent unauthorized access and misuse.
- Compliance with government regulations and data protection laws is essential when collecting, storing, or processing government identifiers.

**Privacy Implications:**

- If mishandled or exposed, government identifiers can be a prime target for identity theft or fraud.
- Improper use or sharing of these identifiers can lead to privacy violations and legal consequences.
- Safeguarding the privacy and security of government identifiers is crucial to protect individuals from harm.
- Special Notes:
- Due to the sensitive nature of government identifiers, relevant laws and regulations should govern their collection and use.
- Consider using anonymization or pseudonymization techniques when full government identifier information is not required.

## 24. Membership Identifiers

Membership Identifiers refer to unique codes, numbers, or IDs assigned to individuals or entities to signify their membership in specific organizations, clubs, loyalty programs, or social groups. Use these identifiers to manage memberships and grant access to associated benefits or privileges.

**Examples:**

- Member ID Numbers: These are unique identifiers assigned to individuals who are members of organizations, clubs, or associations. For instance, a professional association may issue Member ID Numbers to its members.
- Club Membership Numbers: Clubs or associations often provide Membership Numbers to their members for identification and access to club facilities or services.
- Loyalty Program IDs: Individuals receive unique IDs to track their participation and rewards in customer loyalty programs. For example, a hotel chain may issue Loyalty Program IDs to its frequent guests.
- Frequent Flyer Numbers: Airlines assign Frequent Flyer Numbers to passengers who enroll in regular flyer programs. Users use these numbers to track travel miles and rewards.

- Social Club Membership Numbers: Social clubs or societies issue Membership Numbers to their members for identification and participation in club activities and events.

**Considerations:**

- Membership Identifiers are often associated with specific organizations, clubs, or programs and can reveal an individual's affiliations and interests.
- Collect and store Membership Identifiers in alignment with the intended purpose while respecting user consent and privacy regulations.
- You may consider anonymization or pseudonymization techniques when you don't require full Membership Identifier information for a specific service or analysis.
- Securely manage Membership Identifiers to prevent unauthorized access or misuse, especially when granting access to benefits or privileges.

**Privacy Implications:**

- Membership Identifiers can link individuals to specific organizations or groups, potentially revealing sensitive affiliations.
- Careful handling of Membership Identifiers is necessary to prevent unintended exposure or the tracking of individuals' memberships across different organizations.
- Compliance with data protection regulations, consent requirements, and purpose specifications is essential when collecting and using Membership Identifiers.

**Special Notes:**

- Membership Identifiers may include digital or physical cards, unique codes, or digital tokens associated with a membership.
- Organizations should implement appropriate security measures to protect Membership Identifiers from data breaches or unauthorized access.

## 25. Institutional Identifiers

Institutional Identifiers represent unique codes, numbers, or labels that institutions assign to individuals for identification and record-keeping within their specific systems. Institutions use these identifiers to oversee and monitor individuals' interactions, services, or memberships within the organization. These identifiers span multiple categories, such as healthcare, education, and private clubs.

**Examples:**

- Unique Patient IDs: Healthcare providers or hospitals assign these identifiers to distinguish individual patients and manage their medical records. Examples include "PAT12345" or "UPID5678."
- Patient Record Numbers: Similar to Unique Patient IDs, healthcare facilities assign specific numbers to patient records. They help healthcare professionals access and manage patient information efficiently.

- Student ID Numbers: Educational institutions issue these numbers to students for identification, enrollment, attendance tracking, and accessing educational resources. Examples include "SID7890" or "STU-4567."

**Considerations:**

- Institutional Identifiers are institution-specific and may not have meaning outside the organization that assigns them.
- These identifiers are often used for administrative and record-keeping purposes, allowing institutions to manage interactions with individuals efficiently.

**Privacy Implications:**

- Institutional Identifiers can be sensitive because they link individuals to specific institutions or organizations.
- Protecting the privacy and security of these identifiers is essential to prevent unauthorized access or misuse.
- Compliance with privacy regulations and ensuring user consent is crucial when collecting and processing institutional identifiers.

**Special Notes:**

- Institutional Identifiers are not typically intended for public use and are specific to the institution that assigns them.
- Proper data security measures should be in place to safeguard institutional identifiers and the associated data.
- Institutions should only collect and retain these identifiers for legitimate and necessary purposes aligned with their services.

## 26. Case Identifiers

Case Identifiers encompass unique codes or numbers assigned to individual cases, instances, or occurrences within various contexts, including legal, medical, or benefit-related scenarios. These identifiers facilitate managing, tracking, and organizing specific cases and their associated information.

**Examples:**

- Case ID Numbers: Unique alphanumeric codes assigned to individual legal cases or incidents, such as "CASE12345."
- Benefit Plan Participation Identifiers: Identifiers for tracking an individual's participation in benefit plans or programs, often associated with employee benefits, health insurance, or government assistance.
- Medical Case Numbers: Numeric or alphanumeric codes used in healthcare settings to identify and manage specific medical cases or patient episodes.
- Insurance Claim Reference Numbers: Unique identifiers assigned to insurance claims for tracking and processing.

- Legal Case Dockets: Docket numbers or codes used by courts and legal systems to manage and track individual legal cases.

**Considerations:**

- Case Identifiers are essential for effective case management, record-keeping, and tracking of specific incidents or occurrences.
- They are often associated with sensitive and confidential information, making their protection crucial to safeguarding individual privacy.
- Proper handling of Case Identifiers is essential to prevent unauthorized access, disclosure, or misuse of case-related data.
- Compliance with legal and regulatory requirements, such as HIPAA in healthcare or GDPR in the European Union, is critical when dealing with Case Identifiers.

**Privacy Implications:**

- Case Identifiers are linked to specific incidents or cases, making them potentially sensitive and prone to privacy risks if mishandled.
- Unauthorized access or disclosure of case-related information can lead to privacy breaches and legal consequences.
- Privacy controls and data protection measures must be in place to secure Case Identifiers, especially in legal, medical, or benefit-related contexts.

**Special Notes:**

- When handling Case Identifiers, institutions, and organizations should adhere to relevant data protection laws and regulations to ensure the privacy and security of individuals involved in specific cases.
- Anonymization or pseudonymization techniques protect privacy when sharing case-related data for research or analysis while maintaining data integrity.

## 27. User Identifiers

User Identifiers encompass unique codes, names, or labels assigned to individuals for user account creation and access to various systems, services, or platforms. These identifiers are fundamental to user authentication, interaction, and personalization across digital platforms.

**Examples:**

- User IDs: Alphanumeric or numeric codes assigned to users during account creation, often used for login purposes.
- Usernames: Users choose distinctive names for identification within online communities, social media, or web-based applications.
- Email Addresses: Unique email addresses are identifiers for accessing email services and other online platforms.
- Login Credentials: Combinations of usernames, passwords, and other authentication factors used to verify a user's identity.

- Profile URLs: Customized web addresses associated with user profiles on websites, blogs, or social networking platforms.

**Considerations:**

- User Identifiers are essential for user account management, authentication, and personalization of digital services.
- The security and privacy of User Identifiers are critical to prevent unauthorized access to user accounts and the associated personal information.
- Protection of login credentials and passwords is crucial to avoid security breaches and data leaks.
- User consent and data protection regulations, such as GDPR and CCPA, must be adhered to when handling User Identifiers.

**Privacy Implications:**

- User Identifiers are directly linked to individual user accounts and can expose personal information and online activities if compromised.
- Unauthorized access to User Identifiers can lead to identity theft, account hijacking, and privacy breaches.
- Stringent security measures, such as strong password policies and multi-factor authentication, are necessary to protect User Identifiers and user accounts.

**Special Notes:**

- Organizations should implement robust security practices, including encryption and access controls, to safeguard User Identifiers from unauthorized access or data breaches.
- User education and awareness regarding safe online practices, such as avoiding password sharing and using unique login credentials for different platforms, can enhance User Identifier security.
- In cases where organizations use User Identifiers for personalization or targeted advertising, they must prioritize transparency and obtain user consent to respect privacy preferences and comply with data protection regulations.

## 28. Passwords

Passwords are confidential character strings that authenticate and secure access to digital accounts, systems, or devices. They serve as a crucial layer of protection for sensitive information.

**Examples:**

- Login Passwords: Individuals use secret codes to access their online accounts, email, or computer systems.
- Passphrases: Longer and more complex password phrases that enhance security.
- One-Time Passwords (OTPs): Temporary codes sent via SMS or generated by apps for single-use authentication.

**Considerations:**

- Passwords are a primary means of access control and identity verification in digital environments.
- Complex and unique passwords are essential to deter unauthorized access.
- Encourage users to employ multi-factor authentication (MFA) for added security.
- Implement password policies to enforce strong password creation and periodic changes.
- Store passwords securely using encryption techniques.

**Privacy Implications:**

- Weak passwords can lead to unauthorized access and data breaches.
- The compromise of passwords can result in identity theft and financial loss.
- Protecting stored passwords is crucial to prevent data leaks.
- Promote password hygiene and educate users on the importance of strong, unique passwords.

**Special Notes:**

- Password managers can assist in generating and securely storing complex passwords.
- OTPs offer additional security but require careful handling to prevent interception or unauthorized access.

## 29. Signatures

Signatures are unique marks, symbols, or representations made by individuals in analog or digital form to authenticate documents, transactions, or digital communications. They serve as a means of verifying identity and consent.

**Examples:**

- Analog Signatures: Handwritten signatures on paper documents, contracts, or letters.
- Digital Signatures: Electronic representations of a person's signature validate the authenticity and integrity of digital documents or messages.
- Electronic Signatures: A broad category encompassing various methods, including typed names, checkboxes, or graphical images representing consent.

**Considerations:**

- Analog signatures provide a tangible and traditional form of authentication.
- Digital signatures use cryptographic techniques to ensure the integrity and authenticity of digital content.
- Electronic signatures offer convenience and speed in the digital age.
- Countries and regions may have varying regulations regarding the legality and acceptance of electronic signatures.

**Privacy Implications:**

- Analog signatures may expose an individual's handwriting style, which potential adversaries could use for analysis or forgery.
- Digital signatures can link an individual's digital identity to specific transactions or documents.
- Protecting the security of digital signature keys is essential to prevent unauthorized use.
- Privacy regulations may govern the collection and storage of signature data.

**Special Notes:**

- Digital signatures are crucial in ensuring the integrity and authenticity of digital documents and communications.
- Organizations should implement secure methods for generating and storing digital signature keys.
- Compliance with regional and industry-specific regulations is vital when using electronic signatures for legal purposes.

## 30. Digital Certificates

Digital Certificates are cryptographic credentials that are issued to individuals or entities to confirm their identity in the digital realm. People often use them online to ensure secure communication, control access, and create digital signatures. A trusted Certificate Authority (CA) signs them, and they comprise a public key and information about the certificate holder.

**Examples:**

- SSL/TLS Certificates: Used to secure web communications by encrypting data transmitted between a web server and a client's browser.
- Code Signing Certificates: Applied to software programs and scripts to confirm their authenticity and integrity.
- Email Certificates: Used to encrypt and digitally sign email messages to ensure privacy and verify the sender's identity.
- Document Signing Certificates: Employed to sign documents, making them tamper-evident and verifiable digitally.
- Authentication Certificates: Utilized for user authentication in various online services and systems.

**Considerations:**

- Digital Certificates are often used for authentication and data security, making them critical in many online interactions.
- Commonly used to manage and verify Digital Certificates, public key infrastructure (PKI) plays a key role.
- The loss or compromise of a private key associated with a Digital Certificate can lead to identity theft or unauthorized access.
- Revocation mechanisms exist to invalidate Digital Certificates in case of loss or misuse.

**Privacy Implications:**

- Digital Certificates can be associated with specific individuals or entities, potentially revealing their online activities.
- Failure to properly secure the private key linked to a Digital Certificate can expose it to exploitation by malicious actors.
- It is essential to inform users about the implications of Digital Certificates and their role in online privacy and security.

**Special Notes:**

- Protecting the private key associated with a Digital Certificate is essential to prevent unauthorized use.
- Revocation lists and mechanisms should be in place to address compromised or lost Digital Certificates.

## 31. Photos

Photos, often referred to as images or pictures, can reveal various aspects of an individual's identity and life. This category includes analog (printed) and digital images captured through multiple means, such as cameras, smartphones, scanners, or other imaging devices.

**Examples:**

- Photographs: Personal photos of individuals, including portraits, group photos, and candid shots.
- Identification Photos: Official identification photos found on documents like passports, driver's licenses, and employee badges.
- Family Photos: Images featuring family members, including spouses, children, and relatives.
- Vacation Photos: Pictures taken during vacations or trips can reveal travel destinations and habits.
- Event Photos: Images from weddings, birthdays, and parties showcasing personal connections and social activities.

**Considerations:**

- Visual Information: Photos provide information about a person's appearance, relationships, hobbies, and interests.
- Context Matters: The context in which a photo is shared or used can influence privacy implications. A photo shared on a social media profile may have different consequences than one used for official identification.
- Metadata: Digital photos often contain metadata, including geolocation, date, and time, which can reveal additional details.

**Privacy Implications:**

- Identity Disclosure: Photos can directly reveal an individual's identity, making them a high-impact PII category.

- Sensitive Context: Depending on the content, photos may expose sensitive information about relationships, lifestyle, and activities.
- Public Sharing: Sharing photos on social media or platforms may lead to unintended exposure.

**Special Notes:**

- When handling photos as PII, it's crucial to consider the context, obtain appropriate consent, and implement security measures to protect them from unauthorized access or distribution.

## 32. Videos

Videos encompass visual recordings captured through various means, such as cameras, smartphones, camcorders, or other recording devices. Videos can reveal significant information about individuals and their surroundings.

**Examples:**

- Personal Videos: Videos recorded in private settings, including home videos, family gatherings, or casual moments.
- Workplace Videos: Videos taken in a workplace or professional context, such as office meetings, conferences, or training sessions.
- Security Camera Footage: Surveillance videos from security cameras installed in public or private areas.
- Social Media Videos: Videos shared on social media platforms can include various content, from vlogs to event recordings.
- Educational Videos: Video lectures, tutorials, or educational content that individuals may create or participate in.

**Considerations:**

- Visual Information: Videos provide information about individuals, their activities, surroundings, and interactions.
- Context Matters: The context in which a video is recorded or shared can significantly impact privacy implications. A video captured at a private gathering may have different consequences than one recorded in a public space.
- Duration and Content: Longer videos may reveal more information, and the content within the video can range from personal to professional.

**Privacy Implications:**

- Identity Disclosure: Videos can directly reveal an individual's identity, making them a high-impact PII category.
- Sensitive Context: Depending on the content, videos may expose sensitive information about individuals' lives, relationships, and activities.
- Surveillance Videos: Security camera footage and videos require careful handling due to potential privacy violations and legal considerations.

- Public Sharing: To avoid unintended exposure, consider privacy settings when sharing videos on public platforms.

**Special Notes:**

- When handling videos as PII, it's essential to consider the context, obtain appropriate consent, and implement security measures to protect them from unauthorized access or distribution.
- In cases where video files are encrypted, assessing whether the video file name should also be encrypted is advisable to enhance privacy protection.

## 33. Images

Images encompass a wide range of visual content beyond traditional photographs. This category includes various forms of visual data, such as diagrams, illustrations, screenshots, drawings, and scanned documents, that can potentially contain personally identifiable information (PII) or sensitive content. Images are a standard part of digital communication, documents, presentations, and web content, making considering their potential privacy implications important.

**Examples:**

- Diagrams and Charts: Technical diagrams, flowcharts, and graphs used in presentations or documents may inadvertently reveal sensitive information if not appropriately redacted.
- Illustrations and Artwork: Artistic or graphic illustrations, logos, or design elements can contain PII, mainly if they include names, contact information, or identifiable features.
- Screenshots: Captured images of computer or mobile device screens may expose personal data, such as messages, emails, or social media posts.
- Drawings and Sketches: Hand-drawn sketches or digital doodles can reveal information about the creator or their surroundings.
- Scanned Documents: Scanned versions of physical documents, like identification cards, contracts, or handwritten notes, can include sensitive details if not appropriately sanitized.

**Considerations:**

- Image metadata, including geolocation and timestamps, may disclose additional information.
- Optical Character Recognition (OCR) technology can extract text from images, making it necessary to redact sensitive information before sharing.
- Proper image redaction techniques should be applied to obscure PII or sensitive content, ensuring the information is not easily recoverable.

**Privacy Implications:**

- Inadvertently sharing images containing PII can result in privacy breaches.

- Careless handling of images in professional or personal contexts can lead to the exposure of confidential information.
- Compliance with data protection regulations, such as GDPR, HIPAA, or CCPA, is essential when dealing with images containing personal data.

**Special Notes:**

- Use image editing software or tools to redact sensitive information effectively.
- Follow organization-specific privacy and data protection protocols when sharing images, especially in professional or healthcare settings.

## 34. Vocal Sound Bites

Vocal sound bites are short audio recordings or clips that capture spoken words or sounds. These audio snippets can vary in content, ranging from casual conversations and voice messages to recorded phone calls and interviews. While not as common as text-based communication, vocal sound bites can contain personally identifiable information (PII) or sensitive content that must be protected and handled carefully.

**Examples:**

- Voice Messages: Voice messages exchanged via messaging apps or voicemail systems can contain personal greetings, contact details, or sensitive information.
- Phone Call Recordings: Recorded phone conversations, whether for legal, business, or personal purposes, may include confidential discussions and PII.
- Interview Recordings: Recorded job interviews, research interviews, or media interviews can contain personal details, opinions, or sensitive topics.
- Audio Notes: Personal audio notes or reminders that individuals record on their devices may include PII or sensitive content.
- Conference Call Recordings: Recorded conference calls in a business context can contain discussions about financial data, strategies, or other sensitive information.

**Considerations:**

- PII or sensitive content in vocal sound bites can be spoken names, addresses, phone numbers, email addresses, or other personal details.
- Considering the recording's context and obtaining consent from all parties involved are essential factors to address.
- Secure storage and sharing mechanisms should be in place to prevent unauthorized access.

**Privacy Implications:**

- Mishandling or unauthorized sharing of vocal sound bites can result in privacy breaches and legal consequences.
- Compliance with data protection regulations, such as GDPR or HIPAA, is crucial when dealing with audio recordings containing personal data.

**Special Notes:**

- Ensure that you obtain individuals' consent when recording their voices, especially in contexts where privacy and consent are essential.
- Implement encryption and access controls to protect sensitive vocal sound bites from unauthorized access.
- Organizations should have policies and procedures to secure handling and retention of recorded audio content.

## 35. Dates and timestamps

Dates and timestamps refer to specific points in time, including calendar dates and precise times. These can include various timestamps, such as creation dates, modification dates, and event timestamps. This category contains a wide range of temporal data, from significant life events like birthdates to when individuals or systems last accessed a digital file.

**Examples:**

- Date of Birth (DOB): e.g., "January 15, 1985"
- Transaction Dates: e.g., "March 10, 2022"
- Event Timestamps: e.g., "2023-05-25 14:30:00"
- Document Creation Date: e.g., "2023-11-01 09:15:45"
- Expiry Dates: e.g., "Expiration Date: 12/25"

**Considerations:**

- While not all dates and timestamps directly reveal an individual's identity, they can provide definitive clues when combined with other information.
- Birthdates, in particular, are considered sensitive and can be used for identity theft or fraud if not adequately protected.
- Depending on the context, capturing only partial dates (e.g., month or month/year of birth) may reduce the risk of privacy breaches while still serving the intended purpose.
- Precise timestamps can disclose patterns of behavior and activities, potentially impacting an individual's privacy.

**Privacy Implications:**

- People should handle full birthdates carefully to prevent misuse, as they are considered personally identifiable information (PII).
- Accurate timestamps can reveal an individual's routine, location, and activities, posing privacy risks if shared without consent.
- Compliance with data protection regulations is crucial when collecting and storing dates and timestamps to ensure individuals' privacy rights are respected.

**Special Notes:**

- Consider alternatives like partial dates or age ranges to reduce privacy risks when capturing birthdates.

- Implement data retention policies to limit the storage of timestamp data when it's no longer necessary for its intended purpose.
- Employ encryption and access controls for sensitive timestamps to prevent unauthorized access.
- Ensure user consent and transparency in cases where capturing timestamp data might impact an individual's privacy.

## 36. Genetic Identifiers

Genetic Identifiers refer to specific information about an individual's genetic makeup, including chromosomal, deoxyribonucleic acid (DNA), and ribonucleic acid (RNA) data. This category is crucial as it involves susceptible and unique biological information.

**Examples:**

- DNA Sequences: The unique genetic code of an individual.
- Chromosomal Information: Details about an individual's chromosomal structure.
- RNA Data: Information related to ribonucleic acid plays a vital role in gene expression.
- Genetic Test Results: Findings from genetic testing that reveal susceptibility to certain conditions or diseases.
- Genomic Data: Comprehensive genetic information, including coding and non-coding regions.

**Considerations:**

- Privacy Concerns: Genetic data is deeply personal, and its misuse can have severe privacy implications.
- Informed Consent: Collecting and using genetic data should always involve informed consent from the individual.
- Legal and Ethical Aspects: Compliance with legal and ethical standards is essential when dealing with Genetic Identifiers.

**Privacy Implications:**

- Unwanted Genetic Profiling: Discrimination based on genetic predispositions may occur against individuals.
- Privacy Breaches: Improper handling of genetic data can result in data breaches with significant consequences.

**Special Notes:**

- Given the sensitivity of Genetic Identifiers, strict regulations and ethical guidelines govern their collection, storage, and use. Researchers, healthcare professionals, and institutions must adhere to these regulations to protect individuals' privacy and ensure responsible use of genetic data. Additionally, anonymization and encryption techniques are often employed to safeguard this type of PII.

*[DRAFT]*

## 37. Biometric Identifiers

Individuals' unique physiological or behavioral characteristics, biometric identifiers, can be used for identification or authentication. These identifiers are typically intrinsic to a person and include various types of biometric data, such as fingerprint scans, facial images, iris scans, voiceprints, and more. People often use biometric data in security systems, access control, and identity verification processes.

**Examples:**

- Fingerprint Scans: Unique patterns of ridges and valleys on a person's fingertips that can be scanned and stored for authentication purposes.
- Facial Images: Measurements and features of a person's face, often used for facial recognition systems.
- Iris Scans: Scanning the unique patterns in a person's iris to verify their identity.
- Voiceprints: Analyzing the distinct characteristics of an individual's voice, including pitch and tone, for voice recognition.
- Hand Geometry: Measurements of the size and shape of a person's hand, often used for access control.
- Gait Recognition: Analyzing an individual's walking style or gait pattern for identification purposes.
- Hidden Biometrics (Brain Prints): This method involves exploring the unique structural features of an individual's brain for biometric identification.

**Considerations:**

- People consider biometric identifiers highly sensitive because they are unique to individuals and cannot be easily changed.
- Proper storage and biometric data encryption are crucial to prevent unauthorized access or misuse.
- Collect biometric data with the individual's informed consent and adhere to privacy regulations.
- Biometric data may raise privacy concerns if used for surveillance without individuals' knowledge or consent.

**Privacy Implications:**

- Biometric data, if compromised, can have severe privacy consequences, as it is difficult to change once exposed.
- Regulations and safeguards are necessary to protect biometric data and uphold individuals' privacy rights.

**Special Notes:**

- Two-factor authentication (2FA) systems often use biometric identifiers to enhance security.
- Careful consideration of the ethical and legal aspects of biometric data collection and use is essential to maintain trust and privacy.

## 38. Internet Protocol (IP) Addresses

IP addresses are numerical labels assigned to devices in a computer network, allowing them to communicate with each other. While IP addresses may not always directly identify individuals, organizations consider them a part of PII data because they can trace them back to specific users when combined with other information.

**Examples:**

- IPv4 Address: 192.168.1.1
- IPv6 Address: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

**Considerations:**

- IP addresses can reveal an individual's approximate geographic location.
- Websites, service providers, and online platforms often log IP addresses for security and analytical purposes.
- The combination of IP addresses with user activity logs can lead to the identification of specific individuals.

**Privacy Implications:**

- Even though IP addresses alone may not constitute direct PII, their combination with other data can result in privacy concerns.
- Misusing or tracking internet users' IP addresses without consent or linking them to personally identifiable information can compromise privacy.
- Compliance with data protection regulations is essential when collecting and processing IP addresses.

**Special Notes:**

- Some individuals use virtual private networks (VPNs) or proxy servers to mask their IP addresses to enhance privacy.
- Data controllers should inform users about IP address tracking and its purpose to ensure transparency and compliance with privacy regulations.

## 39. Media Access Control (MAC) Addresses

MAC Addresses are unique alphanumeric hardware codes assigned to network interfaces, such as Wi-Fi or Ethernet cards, on devices like computers, smartphones, and routers. They serve as unique identifiers for these devices on a network.

**Examples:**

- Ethernet MAC Address: 00:1A:2B:3C:4D:5E
- Wi-Fi MAC Address: 01:23:45:67:89:AB

**Considerations:**

- Uniqueness: MAC Addresses are typically unique to each network interface, and no two devices should have the same MAC Address.
- Network Identification: They play a crucial role in identifying devices on a network, allowing for data routing and communication.
- Stability: MAC Addresses usually remain constant for a device unless the hardware is changed or deliberately spoofed.

**Privacy Implications:**

- Device Identification: While MAC Addresses do not directly reveal personal information, individuals and organizations can use them to track and identify devices. When combined with other data, they may indirectly lead to user identification.
- Location Tracking: In some cases, MAC Addresses can be used for location tracking, potentially raising privacy concerns.

**Special Notes:**

- Spoofing: Some individuals or organizations may intentionally change or spoof MAC Addresses to protect their privacy or for other reasons.
- Legal Considerations: The collection and use of MAC Addresses may be subject to privacy regulations, and organizations should ensure compliance.
- Usage: People primarily use MAC Addresses for network-related functions, including data routing, device management, and network security.
- Protection: To protect privacy, organizations, and individuals can employ techniques like MAC Address randomization, which periodically changes the MAC Address to reduce tracking possibilities.

## 40. Service Set Identifiers (SSID)

Service Set Identifiers (SSIDs) are unique names for wireless networks, including local WiFi networks. They serve as labels to identify and distinguish different wireless networks.

**Examples:**

- "SmithFamilyWiFi" - An SSID for a home WiFi network.
- "XYZCorpGuest" - An SSID for a guest network in a corporate environment.
- "Joe'sCafeWiFi" - An SSID for a cafe's public WiFi.

**Considerations:**

- SSIDs are used for network identification and are prevalent in connecting devices to WiFi networks.
- They are not inherently sensitive but are part of the network environment.
- SSIDs provide hints about the network's owner or location.

**Privacy Implications:**

- While SSIDs do not usually contain direct personal information, the data transmitted over a network can be sensitive.

- Properly securing networks, including choosing strong passwords and enabling encryption, is crucial for protecting user data.

**Special Notes:**
- Users should be cautious when connecting to open or public networks, as they may lack security measures.
- SSIDs are essential for the functioning of wireless networks and are not typically considered highly sensitive, but network security is paramount to safeguard user privacy.

## 41. Bluetooth Device Addresses (BD_ADDR)

Bluetooth Device Addresses (BD_ADDR) are unique identifiers assigned to Bluetooth devices, such as smartphones, headphones, or IoT devices. These addresses enable communication and identification within Bluetooth networks.

**Examples:**
- The BD_ADDR of a smartphone used for wireless communication.
- The BD_ADDR of a pair of Bluetooth headphones.
- The BD_ADDR of a Bluetooth-enabled smart thermostat.

**Considerations:**
- BD_ADDRs play a crucial role in establishing connections between Bluetooth devices.
- They are not inherently sensitive but can be used to track device locations and interactions within Bluetooth networks.

**Privacy Implications:**
- While BD_ADDRs do not contain personal information, continuously broadcasting these addresses in public spaces can lead to device tracking.
- Protecting user privacy involves implementing measures to prevent unauthorized access to Bluetooth devices.

**Special Notes:**
- Device manufacturers and developers should consider the privacy implications of BD_ADDR tracking and implement security measures to mitigate potential risks.
- While BD_ADDRs are essential for Bluetooth functionality, users should be cautious when using Bluetooth devices in public settings to avoid unwanted tracking or connections.

## 42. Locational Information

Locational information refers to data that specifies the geographical location of individuals, devices, or entities, typically using methods like Global Positioning System (GPS) coordinates, 3-word addresses, or other location-based identifiers.

**Examples:**

- GPS Coordinates (e.g., latitude and longitude)
- 3-Word Addresses (e.g., "apple.banana.orange")
- Land Lot Numbers (e.g., Parcel ID for tax purposes)
- Indoor Positioning System Data (e.g., room or floor numbers in a building)

**Considerations:**

- The level of precision in locational information can vary, from pinpointing a specific address to broader geographic areas.
- The sensitivity of locational data depends on context; it may reveal home addresses, travel routes, or visited places.
- Combining locational information with other data can increase security and privacy risks.

**Privacy Implications:**

- Locational data can expose individuals' daily routines, habits, and frequently visited places.
- Unauthorized access to or misuse of locational information can compromise user privacy and safety.
- Protecting locational data is crucial, especially in applications involving personal navigation, mapping, or location-based services.

**Special Notes:**

- When handling locational information, it's essential to consider user consent and privacy regulations.
- One may employ anonymization or aggregation techniques to mitigate privacy risks when sharing or analyzing locational data.

## 43. Cookie Browser Identifiers

Cookie Browser Identifiers refer to unique identifiers stored in web browsers as cookies. Websites and online services often use these identifiers to track user behavior, preferences, and authentication status.

**Examples:**

- Session Cookies: Temporary cookies maintain a user's session on a website, enabling them to navigate different pages without needing re-authentication.
- Persistent Cookies: These cookies are stored for an extended period and can be used to remember user preferences, such as language settings or login information.
- Third-party Cookies: Websites set these cookies from domains different from those currently being visited by users, primarily for cross-site tracking and advertising purposes.
- Secure Cookies: Used for secure transactions and require an encrypted connection between the browser and the server.

**Considerations:**

- Websites use Cookie Browser Identifiers for various purposes, including personalization, analytics, and advertising.
- Users should be able to manage and delete cookies to protect their privacy.
- Cookie policies and practices should comply with data protection regulations.

**Privacy Implications:**

- Cookie Browser Identifiers can reveal user preferences, browsing habits, and potentially sensitive information.
- Websites can use third-party cookies to track users across other websites, raising privacy concerns.

**Special Notes:**

- Privacy-conscious users may use browser extensions or settings to limit or block cookies.
- Website operators are often required to inform users about their use of cookies and provide options to accept or reject them.

## 44. Radio Frequency Identifiers

Radio Frequency Identifiers (RFID) are electronic devices that use radio waves to transmit data. They consist of small tags or labels that can be attached to objects or individuals.

**Examples:**

- RFID tags on products for inventory management.
- RFID badges for access control in buildings.
- RFID implants in pets for identification.

**Considerations:**

- Businesses widely use RFID technology in supply chain management, access control, and identification systems.
- RFID tags can be passive (powered by the reader's signal) or active (containing their power source).
- Privacy concerns arise when RFID tags are used without individuals' consent or are not adequately secured.

**Privacy Implications:**

- RFID tags can track the movement and location of objects or individuals.
- Improper use of RFID technology can lead to privacy breaches, as it may enable unauthorized tracking and data collection.

**Special Notes:**

- Proper security measures should be in place to protect RFID data from unauthorized access.

- Organizations should inform individuals and obtain their consent when using RFID technology for tracking or identification.

## 45. IoT Identifiers (incl. Smart meter data)

IoT Identifiers, which include data from Internet of Things (IoT) devices and smart meters, refer to unique codes, numbers, or data associated with devices connected to the Internet. IoT ecosystems use these identifiers for identification and tracking purposes.

**Examples:**

- Device Serial Numbers: Unique numbers assigned to individual IoT devices for identification.
- Smart Meter Data: Information collected by smart meters, such as energy consumption data, can be linked to specific households or individuals.
- Device UUIDs: Universally Unique Identifiers assigned to IoT devices for differentiation.

**Considerations:**

- IoT Identifiers are essential for the functioning of IoT systems, enabling communication and control of devices.
- Smart meter data can reveal behavior and usage patterns, potentially compromising privacy when not handled properly.
- Security measures are critical to protect IoT Identifiers from unauthorized access and misuse.

**Privacy Implications:**

- IoT Identifiers can pose privacy risks when not handled with care. Smart meter data, in particular, can provide insights into individuals' daily routines and habits, making it essential to safeguard this information to prevent unauthorized access or misuse.

**Special Notes:**

- Employ proper encryption and data anonymization techniques to protect the privacy of individuals connected to IoT devices. Compliance with data protection regulations is also crucial when collecting and processing IoT Identifier data.

## 46. International Mobile Equipment Identity (IMEI)

The International Mobile Equipment Identity (IMEI) is a unique mobile phone and smartphone identification number. It is a distinctive serial number per device and fulfills various purposes, including tracking, device authentication, and maintenance.

**Examples:**

- You can commonly find IMEI numbers on a mobile device's packaging, underneath the battery, or in the device's settings.

- Service providers and law enforcement agencies may use IMEI numbers to track lost or stolen phones.
- Mobile manufacturers use IMEI numbers for warranty and repair purposes.

**Considerations:**

- IMEI numbers are essential for identifying and managing mobile devices within cellular networks.
- While they are not typically considered sensitive PII, individuals can use them to track device usage and location when combined with other information.

**Privacy Implications:**

- While IMEI numbers do not directly reveal personal information, their misuse or unauthorized access can compromise individuals' privacy.
- Linking IMEI numbers with other data, such as location information or user profiles, creates privacy risks.

**Special Notes:**

- Protecting the confidentiality of IMEI numbers is essential to prevent unauthorized tracking and potential misuse of mobile devices.
- International standards regulate IMEI numbers and are crucial for network operators to manage and secure mobile devices.

## 47. International Mobile Subscriber Identity (IMSI)

The International Mobile Subscriber Identity (IMSI) is a unique identifier associated with a mobile network subscriber. Mobile networks use it to identify and authenticate subscribers. IMSI is stored on a SIM card and transmitted to the network when a user's device connects.

**Examples:**

- When a mobile device connects to a cellular network, it sends its IMSI to the network for authentication.
- IMSI numbers are stored on SIM cards and are essential for enabling voice and data services on mobile devices.
- Mobile network operators use IMSI for billing and network management to ensure that only authorized devices can access their networks.

**Considerations:**

- Mobile networks rely on IMSI numbers for various network management and security purposes.
- Although IMSI numbers may not disclose extensive subscriber information, they are deemed sensitive due to their association with a person's mobile device and usage.
- Protecting the privacy of IMSI numbers is essential to prevent unauthorized access to mobile networks and to safeguard user information.

**Privacy Implications:**

- If IMSI numbers are intercepted or accessed by unauthorized parties, it could lead to unauthorized access to a subscriber's mobile network account and potentially compromise their communications and data.
- Misusing IMSI numbers for tracking or profiling individuals without consent can raise privacy concerns.

**Special Notes:**

- IMSI numbers are typically 15 digits long and consist of three parts: the Mobile Country Code (MCC), Mobile Network Code (MNC), and Mobile Subscriber Identification Number (MSIN).
- IMSI numbers differ from IMEI (International Mobile Equipment Identity) numbers. IMSI identifies the subscriber, while IMEI identifies the device itself.

## 48. Social media posts and comments

Social media posts and comments refer to textual or multimedia content shared by individuals on social networking platforms, along with the responses and comments made by others on these posts. This category includes text, images, videos, links, and other forms of content shared on social media platforms.

**Examples:**

- Textual posts and comments on platforms like Facebook, Twitter, Instagram, and LinkedIn.
- Multimedia content, including photos and videos, posted on social media.
- Responses and comments made by users in reply to posts and comments.
- Links shared in posts or comments that lead to external websites.

**Considerations:**

- The content shared on social media can vary widely, from personal thoughts and updates to discussions on various topics.
- Social media posts and comments often contain user-generated content, and individuals may share personal experiences, opinions, or even sensitive information.
- The context of a post or comment is essential to understanding its potential privacy implications, as some content may be more sensitive or revealing than others.
- Privacy settings on social media platforms can affect who can view and interact with a user's posts and comments. Publicly accessible posts may have broader privacy implications.

**Privacy Implications:**

- Social media posts and comments can reveal personal information about individuals, including their thoughts, preferences, activities, and even locations.
- Users may inadvertently share sensitive information on social media, such as their home address, phone number, or personal experiences.

- Publicly accessible social media content can be crawled and indexed by search engines, making it discoverable even if users change their privacy settings later.
- Analysts and researchers can apply data analysis and profiling techniques to social media content to derive insights about individuals, which can potentially lead to privacy risks.

**Special Notes:**

- Privacy considerations on social media platforms extend beyond individual posts and comments. Users should be aware of their online presence and manage privacy settings accordingly.
- When handling social media data for research or analysis, following ethical guidelines and obtaining consent, if necessary, to protect user privacy is essential.
- Some jurisdictions have specific regulations regarding using social media data for research, marketing, or other purposes, so compliance with relevant laws is crucial.

## 49. Free-form Text Fields / Unstructured Data

Free-form Text Fields, also known as Unstructured Data, refer to text data that does not have a specific structure or format. This category includes any textual information entered in a non-standardized manner and lacks a predefined structure.

**Examples:**

- Comments and notes fields in databases and applications.
- Textual content in emails, chat messages, and instant messaging platforms.
- User-generated content on websites and social media.
- Individuals provide descriptions, reviews, and feedback.
- Include any text-based input fields that accept user-generated content.

**Considerations:**

- Unstructured data can contain a wide range of information, from personal thoughts and opinions to sensitive details.
- The lack of structure in free-form text fields makes automatically identifying and protecting sensitive information challenging.
- Organizations should apply privacy measures such as data encryption, tokenization, and anonymization to safeguard unstructured data.
- Contextual understanding may be required to determine the privacy implications of unstructured text.

**Privacy Implications:**

- Unstructured data, such as names, addresses, phone numbers, etc., can contain personally identifiable information (PII).
- Inappropriate handling of unstructured data can lead to privacy breaches and data leaks.
- Analyzing unstructured text for insights can inadvertently reveal sensitive information about individuals.

- Compliance with data protection regulations is essential when processing unstructured data to uphold individual privacy rights.

**Special Notes:**

- Proper data handling and protection mechanisms are crucial for unstructured data due to its diversity and potential for containing sensitive information.
- Organizations should implement policies and procedures for securely managing unstructured data to mitigate privacy risks and maintain compliance with data protection laws.

# Guidance for Profile and Schema Designers

Well-structured profile and schema design are essential to implementing the Blinding Identity Taxonomy (BIT) to protect Personally Identifiable Information (PII) while ensuring data utility. This section guides profile and schema designers on leveraging the BIT for enhanced privacy and security.

## 1. Identifying PII Information

### Utilize the BIT Categories

Start by thoroughly reviewing the 49 BIT categories provided in this document. These categories are a comprehensive reference for identifying potential PII information within datasets. BIT categories cover a wide range of data elements, from biometric identifiers to locational information, enabling you to identify sensitive information effectively.

### Conduct a Data Audit

Perform a data audit to map dataset fields to relevant BIT categories. This audit helps you identify potential PII attributes that require blinding. Consider collaborating with data owners and subject matter experts to ensure a comprehensive understanding of your data.

## 2. Marking and Handling PII Fields and Attributes

### Encryption and Blinding

Follow best practices for blinding PII fields and attributes based on the BIT categories. Use cryptographic techniques such as format-preserving encryption to ensure that sensitive information is adequately protected. Apply the appropriate blinding process according to the nature of the data and ensure that the resulting dataset no longer contains readable PII.

### Profile and Schema Development

Develop profiles and schemas that define which data fields should be blinded, specifying field types and characteristics. Profiles should also recommend the type of encryption to be applied. By automating the blinding process through profiles and schemas, you can efficiently generate multiple blinded datasets tailored to specific use cases.

## 3. Maintaining Compliance with Regulations

### Data Privacy Regulations

Stay informed about data privacy regulations that apply to your organization and industry. Ensure that your blinding techniques and data handling practices align with these regulations. The BIT provides a practical framework for complying with privacy requirements by safeguarding PII.

### Security Controls

Incorporate additional security controls as needed to enhance data protection. While the BIT offers valuable guidance on data blinding, organizations may require other measures such as access controls, audit trails, and secure data storage to maintain data security.

### Collaboration and Knowledge Sharing

Engage with the broader community of practitioners to share experiences and identify common profiles and schemas that facilitate BIT adoption. Collaboration fosters the development of best practices and ensures continuous improvement in data protection techniques.

By following these guidelines, profile and schema designers can harness the power of the BIT to enhance data privacy, minimize privacy risks, and contribute to the responsible handling of PII attributes within their organizations. The BIT is a valuable resource supporting compliance with data protection regulations while enabling data-driven insights and decision-making.

# Conclusion

In conclusion, the Blinding Identity Taxonomy (BIT) Supplementary document is a vital companion to the BIT, offering essential guidance to profile and schema designers. Its primary purpose is to empower practitioners to effectively identify, mark, and handle Personally Identifiable Information (PII) attributes while maintaining data privacy and security. We encourage all practitioners, whether policymakers, technologists, data scientists, or privacy professionals, to use this supplementary document in conjunction with the BIT to understand each BIT category's nature and significance comprehensively.

By following the guidance provided in this document, you can:

- **Identify PII Information:** Utilize the 49 BIT categories as a comprehensive reference to identify potential PII attributes within datasets. Conduct data audits to map fields to relevant BIT categories for a thorough understanding of your data.

- **Mark and Handle PII Fields:** Implement best practices for blinding PII fields and attributes based on the BIT categories. Develop profiles and schemas that automate the blinding process, ensuring that sensitive information is protected adequately.

- **Maintain Compliance:** Stay informed about data privacy regulations applicable to your organization and industry. Align blinding techniques and data handling practices with these regulations. Incorporate additional security controls as needed to enhance data protection.

Collaborate with the broader community of practitioners to share experiences and identify common profiles and schemas that facilitate BIT adoption. Together, we can enhance data privacy, minimize privacy risks, and contribute to the responsible handling of PII attributes within our organizations.

The BIT and this supplementary document provide valuable resources for achieving these goals. We encourage you to leverage these tools to safeguard sensitive information, meet compliance requirements, and enable data-driven insights and decision-making in a privacy-conscious manner.

# References and Other Useful Links

| **Document/Reference** | **Short URL Link** |
|---|---|
| *Blinding Identity Taxonomy 1.0* | https://bitly.ws/35J2a |
| *ISO/IEC 20889 Privacy enhancing data de-identification terminology and classification of techniques* | https://bit.ly/3cEk0T2 |
| *ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary* | https://bit.ly/2ZbArT4 |

| | |
|---|---|
| *ISO/IEC 29100 Information technology – Security techniques – Privacy framework* | https://bit.ly/364mqb7 |
| *International Statistical Classification of Diseases and Related Health Problems* | https://bit.ly/2X6BRLG |

*Table 1 References and Useful Links*