Karlsgate

Privacy-by-Design Data Collaboration

Emerging technology for the Protected Data Age

Data sharing without exposing consumer identity

Consumer privacy protection and data security are issues that keep you up at night. Organizations have been sharing, posting and transmitting data for decades with little regard for disclosure risks. Public awareness and legislative agendas threaten to impede progress toward more beneficial applications of consumer information.

A new data sharing approach is needed. The primary design consideration for this new approach must be protecting consumer privacy. Personal data rights are a rapidly evolving field with both moral and legal implications. For technology to keep pace with these dynamics, new mechanisms need to be designed, developed and implemented to support a new social contract regarding personal data protection.

Karlsgate created Cryptoidentity™ to protect consumer privacy while enabling the free flow of consumer information between companies.

What's inside:

- Understanding the true cost of trust
- Recognizing the limitations of current data sharing methods
- Cryptoidentity: A new mechanism for a new era
- The future of sharing consumer data
- A re-imagined consumer privacy framework
- Protection empowers freedom to share data

Understanding the true cost of trust

Current modes of sharing consumer data require transferring Personal Data identifiers, like an email address, between two companies to match data sets. These data-sharing arrangements rely on trust that each organization will treat Personal Data securely and with integrity. Far too often, this trust is misplaced.

Consumer privacy protection is lost

Whether using clear text IDs or hashed IDs, sharing data like this represents personal information disclosure and promotes the discovery of individuals. Data owners lack control over what happens to Personal Data after transferring it to another company. Once Personal Data is copied, it can be copied perpetually. Not only that, once information is copied, it can be used as a persistent identifier that can link activity back to a single person forever.

Data security lapses are costly

Data owners are under moral and regulatory obligation to protect consumer privacy and data entrusted to them. The risks of not doing so are both financially and reputationally damaging.

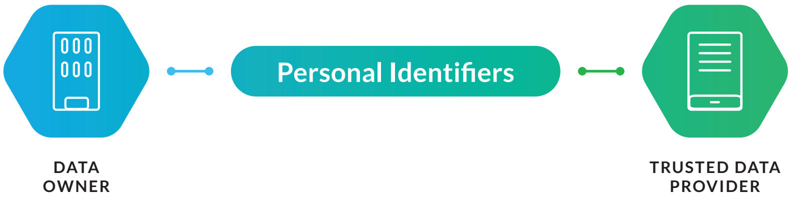
- **Data breaches** – $3.86 million average cost per data breach in 2020[1]
- **Brand reputation** – 9% decrease in global annual sales from a data privacy crisis event[2]
- **Privacy regulations** – €332 million GDPR fines for information security deficiencies in 2019[3]

Recognizing the limitations of current data-sharing methods

Email addresses are a common identifier used to connect data sets across the marketing and advertising ecosystem. Unfortunately, two of the most widely used methods for sharing ID for matching, clear text and hashing, are open to significant consumer privacy and data control risks.

Here is a comparison of some of the current approaches for exchanging identities to the Karlsgate Identity Exchange™:

Clear text email addresses transmitted to a trusted data provider



Characteristics

- Human-readable identifier used for matching purposes
- Data trading partners gain full exposure to all identifiers
- One party lacks all control over the mapping rules and security of the data transmitted
- Trust is needed, since identifying data can be leaked

Effects On Privacy

X Full disclosure of Personal Data

X Explicit consent required to transfer Personal Data in some jurisdictions

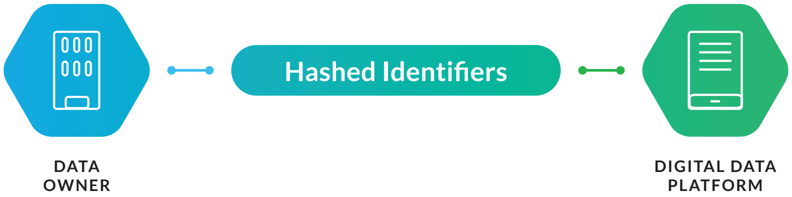
X A data breach at either party risks direct exposure to Personal Data

X Inequitable control over mapping process between sender and receiver

Security Matrix

Personal data	To the data trading partner
Are unknown identities exposed?	Yes. The entire audience is transmitted.
Can identities be re-identified?	Yes. Personal Data is openly shared.

Hashed email addresses transmitted to a digital data platform



Characteristics

- Persistent and reusable hashed identifier used for matching purposes
- Data trading partners gain access to all hashed identifiers
- One party lacks all control over the mapping rules and security of the data transmitted
- Trust is needed, since identifying data can be leaked

Effects On Privacy

√ Underlying identifiers are obfuscated

X Re-identification risk to all identities since hashed identifiers can be mapped to external databases

X Hashes serve as pseudonymous identifiers and may be classified as personal data transfers

X Inequitable control over mapping process between sender and receiver

Security Matrix

Personal data	To the data trading partner
Are unknown identities exposed?	Yes. The entire audience is transmitted.
Can identities be re-identified?	Yes. Stable hash values can be accumulated for later matching.

Cryptoidentity: A new mechanism for a new era

Karlsgate developed Cryptoidentity to address the current weaknesses in data sharing. This patent-pending technology significantly increases the privacy protection of identifying information over current methodologies of sharing data.

Using Cryptoidentity, identities in one data set can be linked or "mapped" to the matching identities within another data set without exposing Personal Data. Cryptoidentity operates on any two data sets that contain a common unique identifier, including email address, IP address, mobile advertising ID or government-issued identifiers.

Cryptoidentity uses advanced cryptography and information security best practices to enable privacy-compliant data sharing, including:

Single-Use Pseudonymization
Re-hashing all identifying data mixed with random noise for each activity to ensure pseudonyms cannot be leveraged for re-identification.

Differential Privacy
Adding noise to data elements to obscure individual details while maintaining aggregated metrics.

Blind Facilitation
Enlisting a neutral party to determine matches without any computational insight into the de-identification process. This gatekeeper approach blocks the flow of any unmatched data.

Anonymization
Completely remove all identifying attributes before working with personal data whenever insights can be gained at an aggregate level.

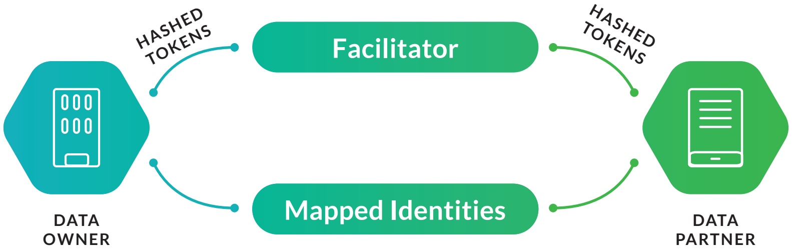
The entirety of this protocol protects against both obvious disclosure and subtle attempts to re-identify the underlying identities. None of the three transaction participants can acquire a new identity that they didn't already have direct reference to. In addition, all participants are blind to all identifying information when sharing data.

The future of sharing consumer data: Zero-trust

Cryptoidentity is the secure data matching foundation of the Karlsgate Identity Exchange. Karlsgate Identity Exchange enables data owners to trade their data assets without exposing personal data in a zero-trust environment.

Email addresses mapped using Karlsgate Identity Exchange

Cryptoidentity™



Characteristics

- Non-reusable hashed identifiers used for matching
- Data trading partners can only see their own identifiers
- Mapping rules are obvious to all parties
- Hashed tokens have no identifying value to the facilitator
- No trust is required to ensure protection

Effects On Privacy

- √ Underlying identifiers are obfuscated
- √ Re-identification is inhibited by blinding the involved parties to the requisite components of the hash algorithm
- √ Hashed tokens cannot serve as pseudonymous identifiers since others cannot recompute the token
- √ Equitable control over mapping process with enhanced transparency

Security Matrix

Personal data	To the data trading partner	To the Karlsgate facilitator
Are unknown identities exposed?	No. The facilitator only forwards signals to the trading partner upon a successful match. This prevents disclosure of any new identities to the trading partner.	No. Since each participant contributes a random component to the salt value, retention of hash value has no re-identifying capacity.
Can identities be re-identified?	No. The facilitator only forwards signals to the trading partner upon a successful match. This prevents disclosure of any new identities to the trading partner.	No. Since each participant contributes a random component to the salt value, retention of hash value has no re-identifying capacity.

Implementing privacy-by-design data sharing

Karlsgate Identity Exchange solves the biggest issues with sharing insights about people. It eliminates the need to use unprotected personal identifiers to conduct commerce. This reduces many of the risks that negatively affect personal privacy rights protection without inhibiting the use cases for data sharing.

Utilizing Karlsgate Identity Exchange supports organizations' plan to build protections directly into their data-sharing practices. It is a privacy-by-design data-sharing approach that eliminates transferring or disclosing any Personal Data. Using Cryptoidentity to map identities eliminates the need for trust in data-sharing partnerships.

No Capacity for Identity Discovery
Cryptoidentity does not permit the acquisition of additional insight or data points regarding any identity not previously present in a participant's data set.

No Personal Revelation
Triple-sourced random initialization vectors and one-way cryptographic hashing techniques create a one-way function, in which the input of the function cannot be inferred or deduced from the output of the function.

No Residual Constancy
Hash values are seeded against later reuse or inference. Single-use, random values mixed into the identifier ensures that no single participant can derive a stable or predictable output from the resultant hash values.

No Identifying Granularity
Individual identities are protected using limiters. Successful identifier mapping is based on a minimum threshold negotiated between the parties prior to uploading hashes with an absolute minimum value of 30.

Karlsgate

As we at Karlsgate embrace what we call the "Protected Data Age," we're changing the game. Gone are the days of lengthy and complicated data exchanges and vulnerable consumer information. Designed to take on the real-world complexity of today's data landscape, Karlsgate's easy-to-implement, Privacy-by-Design data processing and connectivity tools accelerate and simplify data collaboration while ensuring security and privacy.

Learn more about us at karlsgate.com or get in touch at contact@karlsgate.com.

1 IBM Security: Cost of a Data Breach Report, 2020.

2 Data Privacy study: 500 companies share their insights, 2020, Data Privacy Manager. 3 GDPR enforcement tracker.