Karlsgate

Embracing the Protected Data Age

Zero-trust framework for data sharing without exposing consumer identities

The Protected Data Age

The data economy is broken because it exposes people to data privacy threats including theft, re-identification and persistency. As brands adopt data-driven experiences, they'll have to find ways to protect consumer privacy. The current practice of trading consumer privacy for business performance is unsustainable.

This paper explores the current shortcomings of data sharing in the Information Age and proposes a new data-sharing paradigm. We're entering the Protected Data Age: Customer identity protection is no longer derived from the assurances of trading partners, but is inherent in the process of data sharing. This zero-trust environment can be realized using cryptographic technology that makes identity matching completely anonymous to the parties sharing data.

What's inside:

Marketing success depends on consumer data

Let's face it—our appetite for consumer data is limitless. There are more connected personal digital devices being served by a widening array of data-hungry services and apps. The value of delivering personalized customer experiences and the ability to monetize digital audiences are driving up demand for more consumer data and more data sharing.

Personalization fuels the demand for consumer data

Brands and media companies are racing to improve their customers' experience with greater levels of personalization. Insight into personal and household demographics, lifestyles, life events, behaviors, preferences and attitudes is critical for organizations to differentiate and build brand loyalty. Personalization is a winning strategy.

Greater personalization boosts retail customers' spending and brand satisfaction more than ever before

110%
more likely to buy items than planned[1]

40%
more likely to spend more than planned[1]

20%
more likely to recommend the brand[1]

Addressable digital advertising depends on audience identifiers

Digital ad spending is estimated to reach $526 billion globally by 2024, representing 62.6% of total ad spending.[2] Digital advertising is accelerating as more video content is available via OTT streaming services and Advanced Advertising grows for cable system operators. At the same time, the deprecation of third-party ad cookies will become a reality when Google joins Apple, Mozilla and Microsoft in adding cookie-blocking technology to its browser in 2022.

These trends are putting pressure on brands, publishers, data providers and ad tech firms to replace their dependence on third-party cookies with first-party data matching capabilities for audience activation and measurement.

Consumer digital identities

Proprietary ID based on first-party data
Identity created by the consumer-relationship owner for their own use or to match with partners.

Common ID
Identity based on first-party data match to a third-party, Personal Data-based reference data set.

Common identity token
Identity to facilitate enhanced recognition across trading ecosystems.

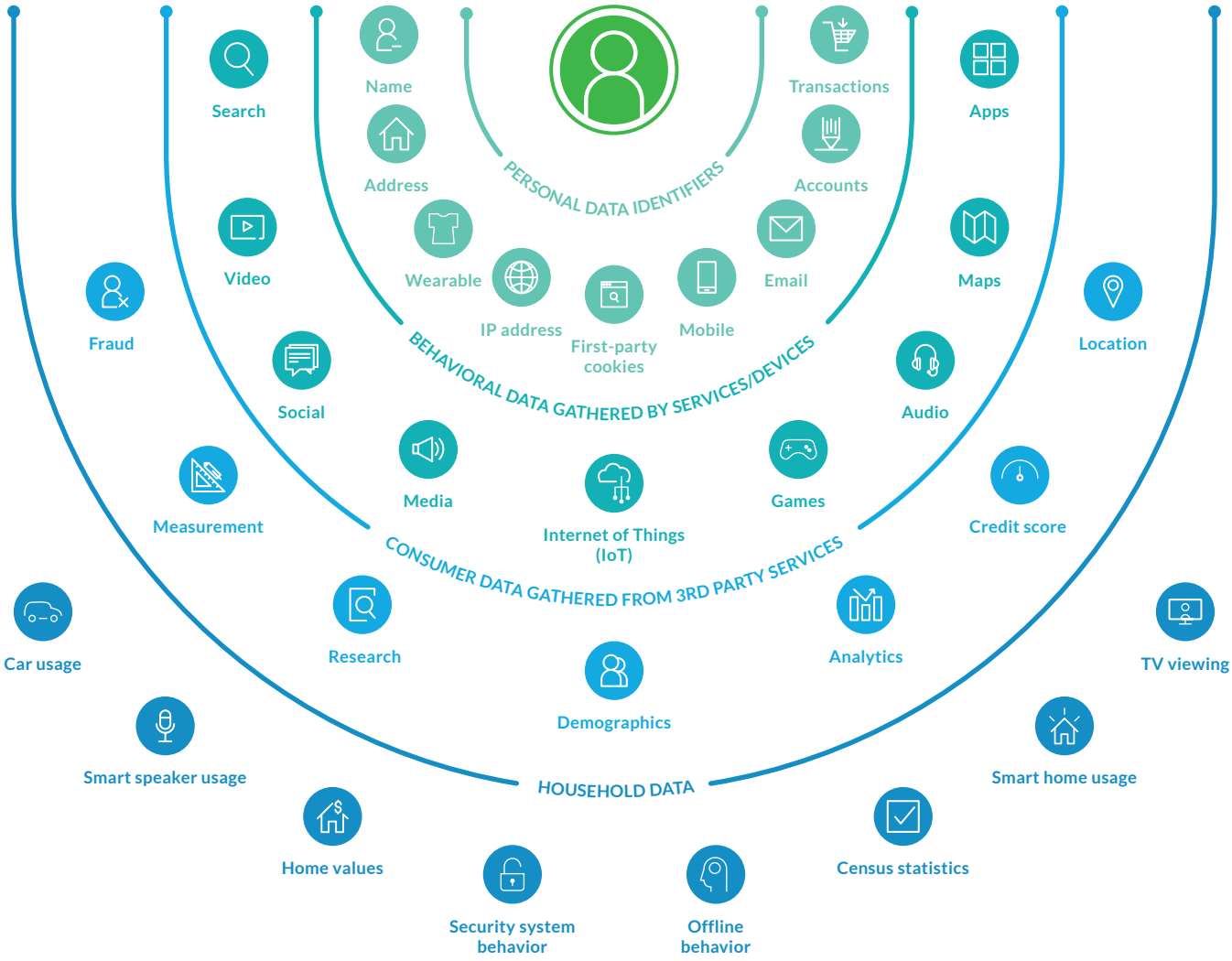
Household ID
Identity based on IP address and physical address.

First-party data graph increases the need for data sharing

A first-party data graph, a profile of a customer with whom a brand has a relationship, combines all of the customer's identity information with their account information and transaction history. Brands gather this information from their own physical locations, call centers, websites and apps. First-party data is critical not only for marketers, but it's also a way for publishers to recover the value of their audience by making it easier to target ads.

Enriching the first-party data graph with third-party data provides brands the ability to truly understand and anticipate the needs of their customers. This consumer data comes from data bureaus, media companies, service providers, social media, smart devices and analytics companies. The technology investments to support the consumer big data ecosystem are forecasted to reach $93 billion by 2030.[3]

The personal data universe



The data economy is broken

The data economy underwent a complete transformation in the last 20 years. The introduction of smartphones, apps, social networks and video streaming services made consumer behavior tracking possible. Coinciding with breakthroughs in big data processing, companies now monetize consumer data as a primary revenue stream. The resulting conflict between honoring consumer privacy and driving company revenue has broken the data economy.

Consumer behavior data gold rush

The "old" data economy was made up of brands with direct customer relationships managing customer databases and a handful of data bureaus providing consumer data enhancement services. In this environment, credit data was regulated and marketing data self-regulated. Consumer insight was research based and aggregated by demographics and geography.

However, today's data economy is a gold rush for consumer-behavior data. The consumer is the commodity and data the currency. Consumer data collection drives the entire marketing and advertising ecosystem. Mining consumer data is often an end in itself. Connecting digital consumer identifiers with online behavior and offline data to create a complete and persistent view of a consumer is the mother lode.

Data economy built on broad consumer behavior collection

The result is an explosion of companies that are trying to build comprehensive consumer data repositories.

Brands
Gather data from their customers directly at each touchpoint.

Digital publishers
Gather data from users and third-party cookies to track consumers across the web.

Ad networks
Gather data via third-party and mobile IDs to enable real-time ad targeting.

Social media companies
Gather first-party data in a "walled garden" they control.

Mobile app developers
Gather real-time data from smartphones to understand users' location and behavior.

Technology companies
Gather user behavior to enable ad targeting, measurement and analytics.

Data companies
Gather online and offline data to support data integration, customer analysis and audience building.

Telecommunications companies
Gather user behavior via user accounts to enable real-time ad targeting.

Consumer privacy and identity data at risk

Given the value of consumer data, it's not surprising how difficult it is to protect. While companies struggle to secure consumer data they store, the digital economy based on sharing data between companies has also fallen short. This leaves consumers' privacy at risk and their data open to cybercrime.

50%

of Americans in 2019 had their data compromised[4]

9x

growth in US breach incidents since 2005, doubled in the last 5 years[4]

60%

of cases resulting in identity theft, indicating a global problem[4]

Inadequate techniques to protect identities

There's no standard for protecting consumer identity data as it's shared across the digital ecosystem. A number of data-matching techniques using varying levels of protection are in use today, but none offer the protection of complete anonymity.

- **Clear text** – No protection: Personal Data in its original format is shared for matching
- **Hashed/pseudonymized identifiers** – Limited protection: Personal Data is scrambled using a standard mathematical formula that is applied by each party for matching
- **Clean rooms** – Limited protection: Personal Data custody is transferred to a third party who matches datasets using a probabilistic statistical model

The privacy protection spectrum

< Protective practices — Permissive practices >

Anonymous data

- No disclosure of identifiers
- No re-identification
- No individual-level utility

Pseudonymized identifiers
(hashing/encryption)

- No disclosure of identifiers
- Re-identification possible
- Individual-level matching

Personal data
(clear text/hashing)

- Full disclosure of identifiers
- Re-identification possible
- Individual-level matching

The current data sharing model is unsustainable

Self-regulation has failed

Unfortunately, once consumer data became the currency of the data economy, consumer privacy became an inconvenience and self-regulation impossible. Governments and regulators across the globe recognize that the digital data economy is a threat to consumer privacy.

Rigorous consumer privacy regulation started with the 2018 General Data Protection Regulation (GDPR) in the European Union and the 2019 California Consumer Privacy Act (CCPA). GDPR set the standard for legislative models, and more than 22 countries have implemented or are considering similar laws to protect consumer data.

The data economy needs a new model for safely sharing consumer insights

With no standard for securing identity data and an increasingly aggressive regulatory environment, the data economy needs a new model for sharing data while protecting Personal Data rights. For technology to keep pace, new mechanisms need to be designed, developed and implemented, empowering a new social contract regarding Personal Data.

The risks, both financial and reputational, are significant if the industry doesn't change:

DATA BREACHES

$3.86M

average cost per data breach in 2020[5]

BRAND REPUTATION

9%

decrease in global annual sales from a data privacy crisis event[4]

PRIVACY REGULATIONS

€332M

GDPR fines for information security deficiencies in 2019[7]

Rise of the Protected Data Age

A new way of thinking about protecting consumer privacy

The Protected Data Age represents a new data sharing paradigm—one where the protection of information isn't derived from the assurances of trading partners, but is inherent in the manner of sharing the data itself.

Like cryptocurrencies, only when the fidelity of a transaction can be self-validated using a shared and verifiable procedure can participants in the ecosystem transact safely. This reduced dependence on assurances from institutions is a form of decentralization and is a key attribute in building a trusted computing environment where everyone benefits.

Zero trust required

The goal should be a zero-trust approach in which data privacy and security are built into the data sharing process. Zero trust employs a privacy-by-design framework to achieve the following data privacy objectives:

NO
transfer of identity data custody

NO
disclosure, retention or persistency of identities

NO
possibility of re-identification

Zero-trust data sharing: A new mechanism for a new era

It's critical in this new era to look for solutions that don't rely on matching consumer identifiers, and where data is anonymous. To get to zero trust, we should employ new techniques that rely on a matching protocol guaranteeing no party has the full identity-matching key. This allows data owners to share data freely without the risk of exposing consumer identities.

To ensure integrity, the match key should be crafted using leading-edge cryptography and encryption methods including:

- **Neutral facilitation** – Data partners don't share encryption logic
- **Differential privacy** – Random secret provided by each transaction participant
- **Pseudonymization** – Some or all of ID replaced with pseudonym
- **Anonymization** – One-time ephemeral matching key utilized

Succeeding in the Protected Data Age

Companies that excel in the new data economy will embrace consumer privacy as a core tenet of their business.

Use first-party data as competitive differentiator
Brands should master data integration to bolster their first-party data across all aspects of their business to create high-value, personalized customer experiences.

Seek consumer insights from their best source
Companies should revisit their data acquisition strategies to look beyond traditional data providers and seek partnerships that can provide more relevant, timely and accurate consumer insight data.

Adopt zero-trust approach to data sharing
Organizations should put consumer privacy at the center of their data-sharing strategies and look for new solutions to implement zero-trust data sharing.

Karlsgate

Karlsgate is an innovative data integration company. Through the Karlsgate Identity Exchange, we empower data owners, brands, publishers, agencies and technology companies to share consumer insights freely without exposing consumer identities.

Learn more about us at karlsgate.com or contact us at info@karlsgate.com.

1 The Next Level of Personalization in Retail. BCG-Google, Business Impact of Personalization in Retail Study, Consumer Survey, U.S., 2019, Boston Consulting Group, 2019.

2 Global Digital Ad Spending Update: Q2 2020, eMarketer, 2020.

3 The Big Data Market: 2018-2030: Opportunities, Challenges, Strategies, Industry Verticals & Forecasts, Research and Markets, 2018.

4 Data Privacy study 2020: 500 companies share their insight, Data Privacy Manager, 2020.

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

7 GDPR enforcement tracker.