blueconic

Guide

Identity Terms: Defined

Understanding the Common Mechanisms Related to the Concept of Identity

Understanding Identity

The companies that own the relationship with their customers are the ones that 'win' today. Owning the relationship means having the ability to not only recognize customers at every point in their journey, but also orchestrate individualized/bespoke experiences that benefit both the customer and the business at every stage of the customer lifecycle.

Before companies can deliver this mutually beneficial customer experience, they need the ability to proactively resolve customer identities across multiple devices, channels, systems, and platforms into a comprehensive and dynamic single customer view. But what does "identity" really mean today?

This document explains the differences among common terms that relate to the overall concept of identity, where each identity mechanism falls in terms of the confidence and utility they offer to business users, and how you can evaluate and improve your company's customer identity confidence and utility levels.

Common Identity Terms

In the context of customer data, there are a number of identity-related terms that are often used interchangeably, but shouldn't be confused with one another:

- **Identity:** Identity is conceptually simple. It refers to an individual person, and it can evolve and change over time, much like the person herself. For example, though you remain the same human being, your identity as a student is replaced by employee when you enter the workforce. Thus, identity is fluid and everchanging, but inextricably linked to a single person. Companies do not own or control identities, but need to understand all the dimensions of identity that relate to an individual in order to engage them effectively.

- **Identifiers:** Identifiers are pieces of information that help you recognize a distinct person. Depending on the context, an identifier might be an anonymous cookie ID, a device ID, an email address, or a customer record. Each type of identifier is distinguished by how it is stored, what types of information can be associated with it, and the systems in which it is used. For example, one system might distinguish one person from another using consumer identifiers (e.g., name, email), whereas others may use company identifiers (e.g., customer ID, tokenized identifier).

There are also several ways of maintaining identity within a system. These mechanisms are both constructs of customer data, aggregated from disparate systems, channels, and sources:

- Identity Graph: An identity graph provides a moment-in-time snapshot of the current, raw state of your customer data. Though the data itself continues to reside in separate systems, it can be queried to create a current view of the data that accounts for any changes. Identity graphs can be used to associate – but not consolidate – multiple identities using one master ID in support of batch marketing processes (e.g., segment creation, current-state reporting).

- Profile: A profile is a mechanism to maintain a single repository of information about an individual person, which enables the resolution of multiple identities into a single, consolidated identity. A profile centralizes and houses customer data, aggregated from disparate systems, channels, and sources. In other words, it's the storage construct for identifiers and associated identity-related attributes—both definitional (e.g., consent status) and synthetic (e.g., engagement score).

While a profile and identity graph are similar, only a profile is an actual entity that combines true historic and real-time customer data to provide a comprehensive, unified, and persistent view of known and anonymous customers that can be stored and analyzed over time. Identity graphs, on the other hand, often purge data after 90 days because storing events for longer would lead to exploding costs.

Identity	Identifiers	Identity Graph	Profile
An individual person	Fragmented pieces of information that recognize a person (e.g., email address, cookie ID, etc.)	Temporary, moment-in-time snapshot of your raw customer data	Single repository of information (identifiers & attributes) about an individual that's updated in real time

Identity Confidence/Utility Framework

Each of the identity mechanisms outlined above differs in terms of the confidence and utility they offer to marketing, analytics, customer experience, and other teams responsible for interacting with customers and/or driving business growth.

Confidence means the customer data accounts for consent (i.e., GDPR, CCPA, and other regulations) and is unified across all systems and sources. Utility means growth-focused teams can actually use the data when and where they need it without time lost due to manual processes and/or reliance on IT, analytics teams, and outside agencies.

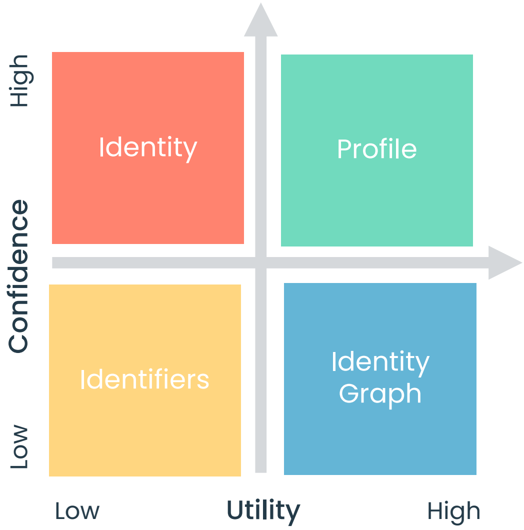
Here's where each identity mechanism falls in terms of both confidence and utility:

- **Identifiers are low confidence, low utility**: Identifiers are collected and used across systems and technologies for various purposes, but on their own, they offer little confidence or utility for creating orchestrated customer experiences and more importantly, can pose risks for compliance with burgeoning privacy regulations. For example, if you only have an email address, it's impossible to know what that person's consent preferences are for onsite personalization from that email address alone.

- **Identity is high confidence, low utility**: Various methods can be used to link identifiers (and any attributes related to an identifier) in an effort to understand identity in context. Since identity belongs to the individual only, it brings high confidence, but low utility.

- **Identity graphs are low confidence, high utility:** Identity graphs increasingly cement and extend the understanding of identity beyond a single channel, system, or interaction. However, identity graphs may rely on fleeting identifiers, like third-party cookies. Creating an "identity" based on anonymous or anonymized data that doesn't account for consent can be risky, especially in today's privacy environment. Typically, the data in an identity graph is associated with one another but isn't an actual entity.

- **Profiles are high confidence, high utility:** Unified profiles provide the most comprehensive and up-to-date record of what you know about your customers; it is the proxy for the individual person. The high quality of the profile data accounts for everything from individual consent status, to frequency of data updates, to identity resolution. Equally important, unified profiles are immediately available for activation rather than queried to create a current view of the data. Growth teams can easily access and use this rich profile data to create targeted segments, conduct modeling and analytics, and deliver relevant, personalized cross-channel experiences that deepen customer engagement.



Improving Your Customer Identity Confidence and Utility

When it comes to orchestrating individualized experiences, the pairing of confidence and utility in unified profiles is especially critical. It's not enough to bring on a technology that checks the box on providing a unified customer profile with a high degree of confidence (in terms of its accuracy and completeness) if the data cannot be used when and where it's needed.

Conversely, there is limited value in activating lifecycle marketing programs and personalized experiences based on a unified customer profile that is incomplete — or worse, activating based on a customer profile that is inaccurate or lacks the ability to recognize individual privacy and consent preferences across marketing and communications channels.

Improving your company's customer identity confidence and utility levels starts with examining your existing systems and databases to see how you currently collect and store customer data, so you can identify how to improve your data collection processes.

Here are the most common customer identity confidence and utility levels we see in companies today:

- Absent: This one's fairly simple: It's when you have zero individual-level data on which to base your customer engagement strategies. You may have broad audience data you glean from tools like Google Analytics and tag management software. But you don't have any PII on specific users, anonymous or known, who interact with your organization in one form or another.

- Anonymous: Anonymous data is information that's collected from delivery channels themselves using mechanisms such as web cookies, device IDs, or tracking pixels. The confidence and utility offered by these types of identifiers are dramatically impacted by privacy regulations like GDPR and CCPA, and are where browser privacy changes like ITP and Chrome's depreciation of third-party cookies are having a dramatic effect.

- Anonymized: Anonymized data (not to be confused with anonymous data) is stripped of core identifiers like email and instead uses proxies for identity, like cookies, that are historically temporary. Data management platforms (DMPs) and some analytics tools are good examples of systems that handle anonymized data. These tools typically rely on a de-identified layer that stores personally identifiable information (PII) separately to ensure compliance with consumer privacy regulations. Like anonymous data, the confidence and utility offered by these types of identifiers are drastically diminished by rising third-party cookie and privacy-related data restrictions.

- Associated: At this level, you've secured data associated with an actual person. Associated data includes information such as email, postal address, first and last name, etc. that is stored in campaign management systems or customer relationship management tools (CRM). Typically, companies are not as confident that associated data is up-to-date or accurate, primarily because it's collected once, used repeatedly for campaigns, and often relies on manual processes to keep it clean.

- Authenticated: Authenticated data comes from a customer, and you likely have high confidence in it because they've voluntarily provided this information as a means to get value from your company. For example, they might create a login to access to an account or piece of content or create a loyalty profile in order to earn points or rewards. This data is stored in backend systems like a data warehouse or relational database. Authenticated data is great for accuracy but can be hard for teams to access and use without involving IT or analytics teams, making it difficult to act in the moment.

- Aggregated: Only a CDP like BlueConic lets you collect and store any kind of identifier – along with any associated identity-related attributes (e.g., browsing behavior, consent status, transaction history, geolocation) – to create a complete and dynamic 'single customer view' in the form of a unified customer profile, and then activate that data in real-time across systems and channels. These profiles are a foundational and critical capability of BlueConic, and where the value in our platform starts. With access to unified, actionable data, your growth teams can decide in what ways they want to activate the data to support their use cases and drive business growth.

Conclusion

Great customer experiences rely on data that companies can use with confidence and utility at the speed they need. Unlike legacy databases and systems, only a CDP like BlueConic provides a way for business users to leverage identity in real and meaningful ways.

For more information about how BlueConic can provide your growth-focused teams with access to unified and actionable customer data that offers both confidence and utility whenever and wherever they need it to transform customer relationships and drive business growth, please contact us at info@blueconic.com.

blueconic

Liberate your data

Learn how to transform your relationships with consumers and unleash business growth with our customer data platform.

Request demo

179 Lincoln Street, 5th Floor, Boston, MA 02111
+1 888 440 2583 • info@blueconic.com