Coalition for Innovative Media Measurement

Identity Infrastructure 2.0

Innovation, Transparency, and Privacy-First Architecture in the US TV & CTV Ecosystem

CIMM Innovation Showcase Paper

April 2026

About CIMM

The Coalition for Innovative Media Measurement (CIMM) is a nonpartisan, pan-industry coalition of companies focused on cultivating and supporting improvements, best practices, and innovations in measurement and currency; data collaboration and enablement; and the use of new metrics and approaches to understanding the value of media. CIMM embraces the entire media and advertising ecosystem and prioritizes effective collaboration to deliver meaningful change.

Foreword

The US TV and CTV marketplace is undergoing a structural transformation. As converged viewing accelerates and advertising workflows evolve, identity resolution has moved from the periphery of activation into the core of measurement, accountability, and economic coordination. What was once a technical enabler is now foundational market infrastructure.

This Innovation Showcase is the first in a new series of papers that will be published by the CIMM in 2026, focused on exploring the latest developments and improvements in critical areas of the market.

This first Showcase brings together leaders from across the ecosystem — publishers, agencies, platforms, and identity providers — to explore how the identity layer is being redesigned in response to new realities. Privacy constraints are tightening. Deterministic anchors are re-emerging as stabilizing forces. Interoperability is becoming essential rather than optional. And independent validation is reshaping assumptions about data quality and linkage accuracy.

It is more than an overview of a market in transition. It is a playbook for buyers and sellers and a manual for senior professionals.

This paper is the product of a truly collaborative effort, reflecting a structured synthesis of presentations and discussions convened during CIMM's *Innovations in Identity Resolution Showcase*, held in February 2026. The analysis presented in this paper draws directly on the frameworks, case studies, quantitative evidence, and strategic perspectives shared by participating industry leaders across the publisher, platform, agency, and identity provider communities.

The conversation reflected here is not about incremental optimization. It is about institutional design. The identity ecosystem must now support not only targeting, but cross-platform reach, frequency governance, outcome measurement, smarter planning, and AI-driven optimization — at national scale and under growing regulatory scrutiny.

The progress showcased in this paper is real and significant. Yet it also makes clear that innovation must be matched with transparency, governance, and coordination. The next phase of identity resolution will be defined not only by technological advancement, but by the market's ability to align incentives and build durable infrastructure that serves the entire ecosystem.

This paper captures that moment — and the path forward.

Jon Watts
Managing Director, The Coalition for Innovative Media Measurement.

Acknowledgements

CIMM extends its special thanks and appreciation to **Sable Mi**, Chair of CIMM's Identity and Data Collaboration Working Group, for her leadership in shaping the Showcase agenda and advancing the Coalition's work in identity and data infrastructure.

We would like to formally acknowledge the contributions made by:

Kemal Bokhari, Head of Data, Measurement & Analytics, DISH Media

Andy Johnson, Chief Data & Product Officer, Adstra Data Solutions
Rethinking Identity: Empowering Researchers Through Transparency

Scott Kozub, Vice President of Product Management, Experian
Healthcare Advertising

Aleck Schleider, Chief Revenue Officer, Blockgraph
Identity Meets Proximity: The Opportunity Ahead

Sebastien Hernoux, Chief Client Solutions Officer (US), Annalect

Aaron Ledwith, SVP, Strategic Partnership Solutions, dentsu

Erin Boelkens, Vice President of Product, LiveRamp
The Evolution of Identity in the Agentic Era

Charlie Johnson, SVP & General Manager, LocID & International, Digital Envoy
Taking Identity Back Home: Why CTV Needs IP-Based Identity

Mark Shepard, Executive Director, Addressable Activation, FreeWheel
Closing TV's Identity Gaps: How Signal Enrichment Is Making Every Screen Addressable

Their contributions have materially advanced the industry's understanding of Identity Infrastructure 2.0 and its implications for converged TV.

We'd also like to acknowledge the extraordinary contribution made by **Rachel Cascisa**, Vice President, Platform Adoption at Epsilon, for helping to strengthen and improve the arguments and analysis made set out in the paper.

Disclaimer

This paper represents an analytical consolidation and original synthesis of discussions and presentations delivered at CIMM's *Innovations in Identity Resolution Showcase* (February 2026). While it draws upon the unique insights shared by the participating executives, the interpretations, conclusions, and recommendations contained herein are those of the author and CIMM.

The views expressed in this paper do not necessarily reflect the official positions, policies, or opinions of any individual contributor, participating executive, or their respective companies or organizations. Participation in the Showcase does not imply endorsement of the analyses or conclusions presented in this report.

CONTENTS

Definitions

The following terms are used throughout this paper:

Deterministic Identity

A linkage between identifiers based on authenticated, observed, or contractually verified relationships (e.g., subscriber account to installation address; authenticated login to household). Deterministic describes the method of linkage — not a guarantee of conceptual correctness. Deterministic signals may still require validation, refresh, and governance.

Probabilistic Identity

A linkage inferred through statistical modeling, behavioral correlation, or clustering (e.g., co-occurrence patterns, shared device behavior, modeled IP associations). Probabilistic approaches expand scale but introduce uncertainty that must be quantified and managed.

Household (Identity Context)

A residential address-anchored unit representing shared living space and shared device environment. In TV and CTV, the household is often the primary transactional and measurement unit, distinct from individuals, accounts, and devices. Conflating these entities can create systemic error.

Identity Velocity

The rate at which identifiers and their linkages change over time (e.g., IP reassignment, device churn, account changes, address mobility). High identity velocity requires explicit refresh cadence and timestamp transparency to prevent silent degradation.

Signal Enrichment

The process of translating or augmenting proprietary identifiers (e.g., set-top box IDs, IP addresses) into interoperable, demand-side readable signals that can flow through standard ad-tech workflows (e.g., OpenRTB), enabling targeting, frequency control, and measurement without altering buy-side systems.

Identity Control Plane

The governance and policy layer that manages how identity data is linked, refreshed, scored, retained, and shared. A mature control plane includes consent enforcement, suppression logic, linkage confidence scoring, logging, auditability, and configurable precision thresholds by use case.

Executive Summary

Identity resolution in US TV and CTV has crossed a structural threshold. It can no longer be understood merely as an activation tactic, a vendor feature, or a "match rate" problem. It now functions as market infrastructure — determining whether buyers and sellers can transact, measure, price, and optimize converged TV with credibility. This shift reflects structural realities: heterogeneous supply environments, quantified data quality fragility, tightening privacy constraints, and the growing reliance on AI-driven optimization systems.

Linear TV still represents the majority of US TV advertising spend (approximately 61% of total TV spend, or roughly $52B, versus approximately $33B for CTV[1]), yet programmatic activation remains disproportionately concentrated in CTV. This imbalance reflects workflow friction and identity constraints rather than inherent supply limitations. With interoperable signal enrichment, billions of linear impressions could become addressable within existing buy-side workflows — unlocking measurable supply without requiring structural changes to DSP infrastructure.

At the same time, FAST viewership and ad loads are expanding rapidly. However, identity in many FAST environments remains unauthenticated and vulnerable to password sharing, IP volatility, and device churn. Deterministic household anchoring — particularly through authenticated or subscriber relationships — can materially improve measurement-grade accountability relative to inference-based linkage.

Identity resolution remains complex, and recent empirical findings underscore why. Independent CIMM research conducted with Truthset found materially lower linkage accuracy than commonly assumed — averaging approximately 51% for hashed email-to-postal matches and materially lower for inference-based IP-to-household linkages. These findings suggest that the market has been operating with greater structural uncertainty than widely recognized.

Multi-entity modeling is essential, as households, individuals, devices, and accounts represent distinct but interrelated identity layers. Modern identity graphs typically preserve these entities as separate nodes and connect them through deterministic or probabilistic linkages rather than literally "flattening" them into a single construct. However, when linkage logic is overly aggressive, insufficiently transparent, or weakly governed, the practical effect can resemble functional flattening, where signals are over-associated and entity distinctions become blurred in downstream activation or measurement workflows. Even moderate linkage inaccuracies at any layer can propagate through the graph, increasing media waste, distorting attribution signals, and contributing to reconciliation disputes.

AI is not a substitute for identity integrity. As optimization systems become more autonomous, identity quality becomes more consequential. Incorrect linkages contaminate training data, distort attribution signals, and degrade future decision quality. In the agentic era, identity becomes a prerequisite for dependable automation rather than a supporting input.

Data and identity providers are responding to these challenges. The ecosystem is shifting away from opaque, scale-first identity graphs optimized for match volume toward deterministic-first, privacy-grounded, enterprise-controlled systems optimized for measurement credibility and governance resilience. Those systems are increasingly designed to be interoperable across environments (cloud, clean rooms, direct integrations) and usable not only for activation and measurement, but as the identity substrate for AI-driven workflows, as we enter the agentic era.

Identity Infrastructure 2.0 represents a structural evolution in response to these pressures. It is characterized by disciplined deterministic anchoring where feasible; explainable linkage and documented provenance; privacy-by-design controls; interoperability across clouds and clean rooms; and measurement-grade validation with clearly articulated failure modes.

Executive Summary

These developments coalesce into four structural shifts that define Identity Infrastructure 2.0:

1. **Deterministic household identity is increasingly essential as the anchor for premium TV addressability and cross-platform measurement.** Authenticated subscriber relationships and ISP-level deterministic data provide materially more stable anchors than inference-based IP matching or probabilistic clustering. Deterministic enrichment reduces over-association, improves cross-screen frequency governance, and strengthens reconciliation credibility across trading partners.

2. **Transparency and provenance are becoming table stakes.** The market is reaching a tipping point against "black boxes," as match rate alone proves insufficient for measurement-grade use cases. Identity Infrastructure 2.0 requires linkage confidence scoring, standardized timestamp transparency, independent validation, and explicit disclosure of known limitations.

3. **Identity is becoming configurable infrastructure (composability).** Enterprises increasingly expect identity to operate within their governance perimeter — whether in their own cloud environments or interoperable clean rooms — with explicit control over thresholds, signal strength, refresh cadence, and policy rules.

4. **Signal enrichment is narrowing the structural gap between linear TV and CTV/FAST by making previously opaque supply legible to programmatic workflows.** This enables cross-screen frequency management, converged reach measurement, and outcome-based attribution in environments that were previously invisible or unreliable.

AI-enabled optimization, and the effective activation and governance of first-party data assets. As privacy constraints tighten and third-party identifiers decline, robust identity frameworks increasingly determine whether enterprises can securely organize, enrich, and activate their own customer data across channels and environments.

For senior executives, the question is no longer whether to invest in identity — but whether their current identity architecture is durable enough to support converged measurement, privacy resilience, and AI-driven growth.

Chapter 1. The Identity Problem for TV has Changed: From Tactic to Infrastructure

For much of the past decade, identity resolution was framed through a marketing activation lens: match a consumer (or device) to a digital ID so a segment can be reached in an addressable environment. That framing remains relevant, but it is increasingly incomplete for converged TV.

In TV, identity must carry three additional burdens:

1. It must support cross-screen deduplication and reach/frequency management.
2. It must enable impression-level measurement and attribution in environments where identifiers are absent, weak, or inconsistent.
3. It must do so within rapidly evolving privacy constraints and enterprise governance expectations.

This evolution moves identity into the category of industry infrastructure — similar to clearing and settlement rails in finance, numbering systems in telecom, or accreditation regimes in measurement. When identity is weak, the market does not simply "perform worse." It becomes harder to price inventory, harder to compare outcomes, harder to audit claims, and harder to coordinate shared standards.

Identity resolution in TV and CTV is uniquely challenging because the medium itself differs fundamentally from the device-centric foundations of digital advertising. These institutional dynamics are likely to become even more consequential as AI-driven and increasingly agentic planning, activation, and optimization systems reshape advertising workflows – a broader structural shift that reinforces the importance of durable identity infrastructure, even as it extends beyond the primary scope of this paper.

First, the institutional structure of the market creates complexity and misaligned incentives.

The US TV and CTV identity ecosystem sits at the intersection of four stakeholder groups:

1. **Publishers and MVPDs**, who control premium inventory and authenticated subscriber relationships.
2. **Advertisers and agencies,** who require cross-platform accountability, deduplicated reach, and outcome validation.
3. **Identity and data providers,** who build linkage, enrichment, and translation layers across environments.
4. **Platforms and ad tech intermediaries,** who execute transactions and require scalable interoperability.

These stakeholders often operate under distinct and sometimes competing incentives:

- Publishers prioritize yield optimization, audience scale, and control over first-party data.
- Advertisers prioritize precision, transparency, and measurement integrity.
- Identity providers monetize linkage, match rates, and activation depth.
- Platforms prioritize standardized, interoperable signals that function at scale.

These incentives do not automatically align. Scale-driven identity models may conflict with measurement-grade fidelity. Data control may conflict with interoperability. Operational simplicity may conflict with privacy rigor.

Chapter 1. The Identity Problem for TV has Changed: From Tactic to Infrastructure

While these incentive tensions are not unique to CTV and can be observed across digital advertising channels, the converged TV environment amplifies their practical impact. Television buying has historically depended on shared currencies, panel-based measurement conventions, and relatively standardized audience definitions. As CTV introduces impression-level activation, heterogeneous identity signals, and multiple competing measurement frameworks, coordination failures become more consequential for pricing integrity, cross-platform reach reconciliation, and frequency governance.

In this context, identity disagreements do not simply affect targeting efficiency; they can influence the credibility of trading currencies and the comparability of outcomes across premium video environments. The scale of investment in TV and the persistence of household-level viewing dynamics therefore make identity alignment a more structurally significant issue in CTV than in many purely digital channels.

The resulting coordination problem is structural rather than episodic. Each stakeholder can rationally optimize within its own incentive framework while collectively degrading ecosystem coherence. Identity Infrastructure 2.0 therefore functions not only as a technical redesign, but as an institutional mechanism for aligning scale, fidelity, and governance expectations across structurally distinct actors.

Second, TV is a household medium and co-viewing is common.

Connected TV is typically consumed on shared screens, often by multiple viewers simultaneously. Device identifiers, login credentials, and subscription accounts may not map cleanly to individual people. Co-viewing, guest usage, second homes, and account sharing introduce ambiguity that is less prevalent in single-user mobile environments. Identity systems must distinguish clearly between households, people, devices, and accounts rather than collapsing them into a single flat graph.

More advanced identity architectures increasingly support structured linkages between household-level identifiers and the individuals associated with those households. This enables marketers to plan and transact media at the household level in CTV environments while maintaining the ability to extend messaging to relevant individuals across other digital channels. Such connected identity frameworks help reconcile the household-centric nature of television viewing with person-level activation and measurement needs in converged media workflows.

Third, the supply of inventory is structurally heterogeneous, which undermines identity consistency.

The TV ecosystem spans environments with materially different signal characteristics:

- Native CTV apps may expose device IDs or login-based identifiers.
- FAST environments often rely primarily on IP signals, with inconsistent authentication.
- Linear TV, even when enabled for dynamic ad insertion (DAI) as across MVPD platforms, typically does not expose a demand-side readable identifier in the ad request.

This heterogeneity creates a structural identity problem. Identity systems depend on consistent anchors. When different supply environments expose different types of identifiers — with varying stability, persistence, and authentication strength — the identity layer cannot operate as a uniform spine across the ecosystem.

The consequences are significant:

- A household may be clearly identifiable in one environment (authenticated CTV) but opaque in another (FAST IP-based supply).
- Frequency management becomes environment-specific rather than cross-platform.
- Deduplicated reach measurement becomes probabilistic rather than deterministic.
- Attribution models must reconcile impressions generated from different identity confidence tiers.
- Buy-side workflows encounter inconsistent visibility — some impressions are fully legible; others are partially or entirely workflow-invisible.

In effect, identity fidelity becomes supply-dependent.

This fragmentation forces identity providers to build translation layers, enrichment pipelines, and probabilistic stitching mechanisms simply to approximate cross-environment continuity. It also increases reconciliation risk, as two parties may be evaluating performance based on different identity foundations.

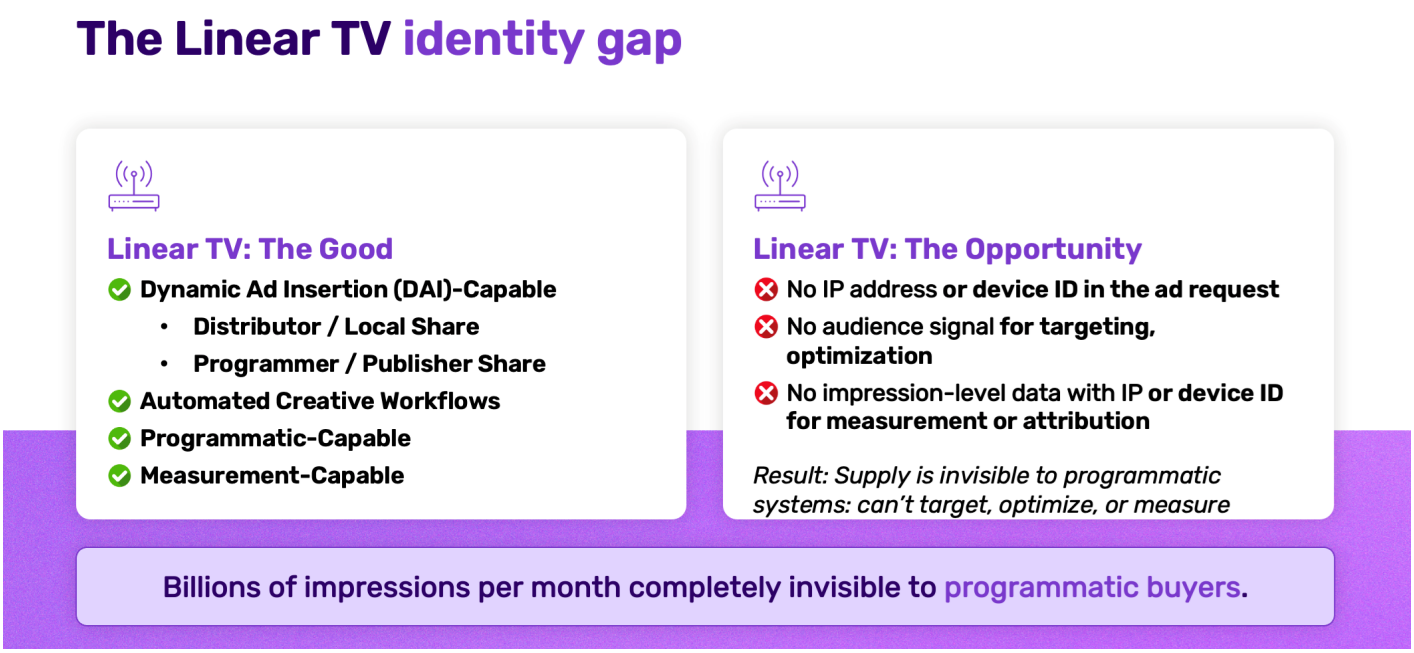
Heterogeneous supply therefore does not merely create technical variation — it undermines interoperability, increases compounding error, and makes it difficult for identity to function as shared infrastructure.

Identity systems that have mature offline to online linkages can provide a more stable graph that connects CTV identifiers not only to households, but back to individuals within a household alleviating some of the fragmentation.

Fourth, buy-side infrastructure generally assumes interoperable identifiers.

Programmatic workflows are generally built around the expectation that a usable, interoperable identifier is present in the ad request. If a DSP cannot see a reliable identifier, it cannot apply standard capabilities such as audience targeting, frequency capping, deduplication, suppression, or measurement reconciliation. In practice, many TV impressions remain "workflow-invisible" rather than inherently unaddressable.

Figure 1: The Importance of Interoperable Creative Identifiers



Source: FreeWheel

Fifth, privacy and consent regimes are fragmented and evolving.

Regulatory requirements vary by state, platform, and data source. Identity systems must be architected to withstand a shifting compliance landscape, including opt-out propagation, purpose limitation, and evolving definitions of sensitive data. Compliance resilience is now a design requirement, not an afterthought.

Chapter 1. The Identity Problem for TV has Changed: From Tactic to Infrastructure

The Core Tension: Scale vs. Fidelity

Identity systems have historically been rewarded for scale — how many identities can be resolved and activated. But TV measurement and high-value premium buying demand fidelity — how confidently an impression can be tied to a real household, and how consistently that tie persists across time and devices.

This tension appears repeatedly in showcase materials. It is not merely technical; it is institutional. Pricing models, incentives, and reporting conventions can nudge systems toward over-association and opaque logic. The result is inflated match rates with degraded measurement credibility.

Identity Infrastructure 2.0 can be understood as an attempt to reconcile scale with fidelity by making signal strength explicit, provenance visible, and controls configurable.

The Emergence of Identity Infrastructure 2.0

Identity Infrastructure 2.0 represents the market's attempt to reconcile these tensions.

The ecosystem is moving away from opaque, scale-first identity graphs toward architectures that prioritize:

- Deterministic anchoring where feasible.
- Explicit modeling of households, people, devices, and accounts.
- Interoperable signal translation across environments.
- Enterprise-level governance and policy control.
- Measurement-grade validation with clearly articulated failure modes.

The central challenge is balancing four forces simultaneously: **scale, fidelity, privacy, and operational simplicity**. Identity Infrastructure 2.0 is the market's structural response to this balancing act.

Chapter 2. The Data Quality Problem in Identity Resolution

Recent studies undertaken by CIMM, in partnership with Truthset and GoAddressable[1], suggest that there are important data quality challenges embedded in the foundations of the identity resolution (IDR) ecosystem: linkage accuracy across commonly used identifiers is materially lower than widely assumed.

These findings do not merely highlight isolated vendor variance. They challenge the prevailing assumption that large-scale identity graphs provide stable and measurement-grade linkages across households, devices, and demographic attributes. If identity is to function as infrastructure, its accuracy must be understood, measurable, and defensible. The empirical evidence suggests that the market has been operating with materially higher uncertainty than previously acknowledged.

Household Identity: Hashed Email to Postal Linkages

In 2023, the CIMM Household Identity Accuracy Project evaluated hashed email (HEM) to postal address linkages across more than 15 major data providers. The study examined approximately 1.2 billion HEM-to-postal linkages covering 792 million unique emails and 133 million postal addresses. The average linkage accuracy across providers was approximately 51%.

The study also found that:

- Accuracy varied substantially across providers, ranging from 32% to 69%.
- Dataset scale was not predictive of quality.
- Even the highest-performing providers exhibited significant internal variation, with high-accuracy and low-accuracy records coexisting within the same files.

The implication is structural: even before layering IP resolution, device stitching, or demographic enrichment, nearly half of household-level linkages may be inaccurate or uncertain. When identity systems assume that household resolution is stable, they may be building subsequent inference layers on a fragile base.

IP-to-household Linkages: Greater Instability

A subsequent 2025 CIMM/Truthset study examined IP-to-postal and IP-to-email linkage accuracy using deterministic ISP and MVPD subscriber data as ground truth. The results were materially lower than many in-market assumptions:

- IP-to-postal linkages were accurate, on average, approximately 13% of the time.
- IP-to-email linkages were accurate, on average, approximately 16% of the time.
- Providers agreed on the same IP-to-postal linkage only 6.4% of the time.
- Agreement on IP-to-email linkage was only 2.8%.
- Approximately 77% of IP-to-postal linkages fell into the lowest (<10%) accuracy decile.
- IPv6 addresses — representing roughly 54% of US internet adoption — were underrepresented by approximately 72% in commercial datasets.

These findings suggest that large-scale IP-based audience construction may be systematically unstable without deterministic grounding. Where IP resolution is used as a primary anchor, particularly in FAST and unauthenticated CTV environments, the identity layer may be significantly more volatile than assumed.

[1] Sources: CIMM, *Household Identity Accuracy Project* (2023), conducted in partnership with Truthset; CIMM / GoAddressable Truthset, *IP Address Accuracy Study* (2025).

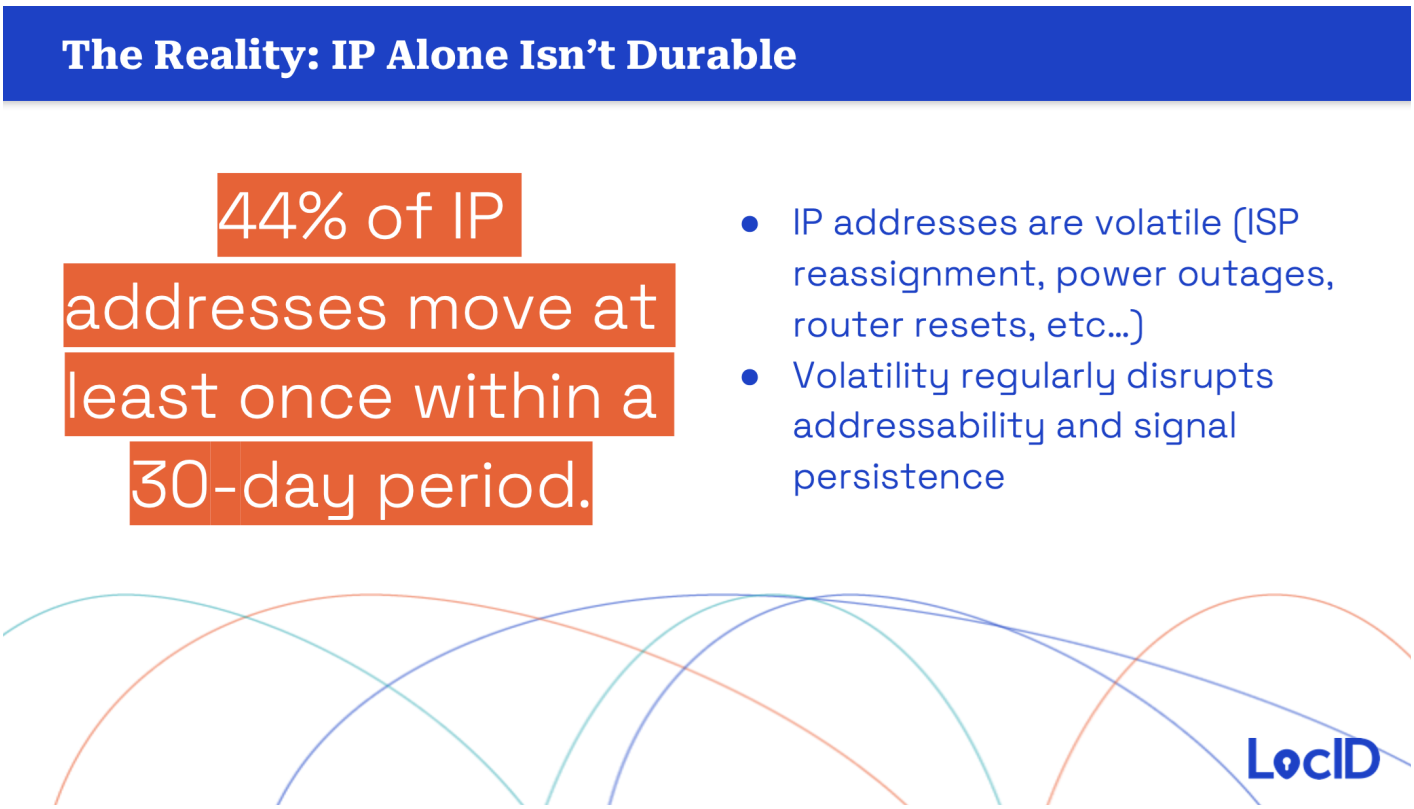
Structural Drivers of Inaccuracy

These studies identify multiple structural sources of linkage error. These are not isolated vendor defects, but are related to the characteristics of the underlying signals and collection methodologies:

- Stale linkages: IP-to-household and device-to-person associations degrade over time. Without standardized timestamp transparency, first-seen and last-seen data cannot be reliably interpreted.
- Address mobility: Younger and more mobile populations generate more frequent postal changes, accelerating decay in person-to-household resolution.
- Probabilistic over-association: Scale-first clustering models may intentionally widen linkage thresholds to increase match rates, introducing over-association.
- IP rotation and reassignment: ISPs frequently reassign IPv4 addresses for privacy and resource management. Static assumptions about IP persistence are therefore unreliable.
- VPN masking and remote routing: Virtual private networks and proxy routing obscure true household IPs, introducing systematic distortion.
- IPv6 underrepresentation: Commercial datasets disproportionately represent IPv4 traffic, despite majority IPv6 adoption, creating structural sampling biases.
- Errors compounding across layers: Inaccuracies cascade as signals move from device to account to person to household to attribute. Each linkage layer introduces additional uncertainty.

Taken together, these factors help explain why commercial datasets may contain materially more IPs per postal address than deterministic ISP data would support. The issue is not simply “noise.” It is structural signal instability interacting with scale-driven probabilistic modeling.

Figure 2: IP Address Volatility



Source: Digital Envoy

Chapter 2. The Data Quality Problem in Identity Resolution

Compounding Errors Across the Identity Chain

Identity resolution rarely occurs at a single layer. Attributes are typically attached to individuals. Individuals are linked to households. Households are associated with devices and IP addresses. Campaign targeting often relies on this entire chain. When linkage accuracy at one layer is imperfect, and additional layers introduce their own uncertainty, the degradation becomes multiplicative rather than additive. For example:

- Device-to-person linkage may operate at c.70% confidence.
- Person-to-household linkage may average c.51%.
- Household-to-demographic attribute accuracy may range from 40-80%, depending on attribute type.

When chained together, effective on-target precision can degrade dramatically. In one simplified modeling example from the IP study, degraded linkage assumptions implied that only a small fraction of media investment might reach the intended demographic audience under certain conditions.

When multiple linkage layers are combined, effective on-target precision can degrade if underlying signals are weak, stale, or insufficiently validated. In simplified modeling scenarios based on the IP accuracy study, lower-confidence linkage assumptions suggested that only a limited proportion of media investment might reach the intended demographic audience under certain conditions. In practice, mature identity architectures are designed to mitigate this risk through continuous signal evaluation, persistence logic, and deterministic anchoring where available, rather than mechanically "chaining" independent probabilistic associations.

It is also important to note that IP-based signals typically function as one input among many in contemporary identity systems. While they can play a meaningful role in device co-location, temporal refresh, or contextual inference — particularly in unauthenticated CTV or FAST environments — most large-scale identity solutions rely on a broader hierarchy of signals, including authenticated relationships, transaction data, device identifiers, and modeled behavioral patterns. The degree to which IP signals influence linkage outcomes therefore varies by environment, use case, and data availability.

This compounding effect helps explain several observable market phenomena, including:

- Campaign performance volatility.
- Inconsistent attribution results across platforms.
- Reconciliation disputes between buy-side and sell-side systems.
- Divergent reach and frequency calculations across identity methodologies.

These are not necessarily failures of optimization; they are often manifestations of upstream identity instability.

> ***We keep layering probabilistic stitching on top of probabilistic stitching and calling it scale. At some point, that's just optimism.***
>
> *— Charlie Johnson, SVP & GM LocID, Digital Envoy*

Why did the Market Not Identify these Data Quality Issues Earlier?

The persistence of these data quality weaknesses raises an institutional question: why were they not identified earlier at scale? The answer appears less technical than structural. Market incentives, limited access to deterministic benchmarks, and performance masking dynamics collectively obscured underlying linkage fragility.

Chapter 2. The Data Quality Problem in Identity Resolution

We believe that three structural dynamics contributed:

- **Scale Bias:** The market historically rewarded match rate, reach expansion, and activation volume. Verified accuracy was rarely disclosed or independently validated.
- **Limited Ground Truth Access:** Few enterprises possess deterministic ISP or MVPD subscriber data that can serve as validation benchmarks. Without reference datasets, vendor claims were difficult to test.
- **Performance Masking:** Campaign-level ROI can remain positive even when upstream data is degraded. Optimization systems may compensate for noise, obscuring root-cause linkage instability.

As long as campaign KPIs served as the primary proxy for identity quality, upstream structural error remained largely hidden.

Data Quality as the Catalyst For Identity Infrastructure 2.0

These findings are more than just a diagnostic report. They function as a catalyst for structural redesign. They underscore the necessity of:

Deterministic grounding, particularly through authenticated subscriber relationships and ISP-level data where feasible.

Transparent linkage scoring, enabling stakeholders to understand probabilistic confidence rather than relying on binary match flags.

Explicit multi-entity modeling, distinguishing households, people, devices, and accounts rather than collapsing them into flat graphs.

Standardized metadata, including harmonized timestamp definitions and freshness indicators.

Independent validation frameworks, allowing identity methodologies to be benchmarked against shared reference data.

Identity Infrastructure 2.0 should therefore be understood not as incremental feature innovation, but as a systemic response to quantified data quality fragility. If identity is to function as market infrastructure, its integrity must be measurable, explainable, and institutionally defensible.

> ***The industry's push toward Identity Infrastructure 2.0 validates what TransUnion has long believed: data quality must be the foundation. Our identity solutions are built on transparent linkage scoring, explicit multi entity modeling, and governance frameworks that give partners full visibility and control. At the same time, our proprietary, high fidelity data allows advertisers, agencies, and platforms to operate with the confidence required for mission critical use cases. This combination of transparency and superior data quality is what enables identity to function as reliable, defensible market infrastructure.***
>
> *— Sandeep Gadre, VP of Marketing Identity Solutions, TransUnion*

Chapter 3. Deterministic Household Identity as an Anchor

Today, durable, first-party household relationships remain the most stable anchor in the modern TV and CTV ecosystem. Unlike open-web environments, television has historically operated at the household level. MVPD subscriber relationships, broadband service installations, authenticated app logins, billing addresses, and physical device provisioning create deterministic links between a service provider and a residential address. These relationships are not inferred; they are operationally required. A satellite installation, a cable subscription, or a broadband account necessarily ties service to a verified physical location.

In this sense, household identity in TV is not merely a marketing construct. It is an operational artifact of service delivery.

This distinction matters. In digital ecosystems, identity graphs often aggregate signals probabilistically, connecting cookies, device IDs, IP addresses, and hashed emails based on statistical likelihood. In contrast, TV distributors and major publishers possess subscriber-level ground truth derived from contractual relationships, billing validation, and authenticated usage.

Identity Infrastructure 2.0 does not eliminate probabilistic modeling. Rather, it repositions deterministic household identity as the reference layer against which probabilistic extensions should be validated.

Why the Household Layer Matters Structurally

Identity needs to serve three simultaneous functions in TV, helping to:

1. Enable addressable targeting.
2. Support cross-platform measurement.
3. Sustain privacy compliance and consumer trust.

Each of these functions benefits from a stable household anchor.

Addressable Activation

In addressable TV, advertisers seek to minimize waste. Deterministic subscriber relationships allow distributors to target known households with defined characteristics, rather than inferred clusters. Without a verified subscriber relationship, “addressable” risks becoming an approximation rather than a controlled activation environment.

> ***Marketers should not have to sacrifice accuracy for scale. With deterministic first-party data, we know with certainty who our customers are, there is no guesswork. As a nationally distributed TV service provider, our equipment is in their homes and we have the added benefit of collecting all the viewing data in the household. This enables advanced targeting capabilities, like suppressing ads to heavy-tuning households or targeting homes that watch specific networks and program genres.***
>
> *— Kemal Bokhari, Head of Data & Analytics for DISH Media*

Chapter 3. Deterministic Household Identity as an Anchor

Measurement Reconciliation

Cross-platform measurement requires de-duplicating exposures across linear, CTV, mobile, and web. Household identity provides a structural bridge across devices within a residence. Without this anchor, identity fragmentation increases reconciliation disputes between datasets that rely on different linkage methodologies.

Privacy Durability

Privacy has become the dominant constraint shaping identity design. Deterministic subscriber relationships operate within explicit consent frameworks and contractual data governance regimes. This makes them more resilient under tightening regulatory conditions than opaque probabilistic stitching.

In short, the household anchor provides persistence, accountability, and compliance durability — three attributes increasingly necessary in a privacy-first ecosystem.

Deterministic Does not Mean Infallible

The case for deterministic household identity as a structural anchor should not be misunderstood as a claim of conceptual perfection. Determinism describes the *method* of linkage — typically rooted in authenticated subscriber relationships, billing records, or verified installation addresses. It does not guarantee that the resulting representation of audience exposure perfectly maps to lived behavioral reality.

A household subscriber record may be deterministically linked to a physical address. However, the interpretation of exposure within that household remains probabilistic at the individual level. Multiple individuals may share the same screen. Devices may be shared. Account credentials may be used outside the primary residence. College students may retain access to household streaming services while residing elsewhere. Seasonal homes introduce further complexity. Even within a single dwelling, patterns of viewing differ meaningfully by time of day and by user.

These structural realities introduce ambiguity that cannot be eliminated simply through deterministic linkage.

In addition, device ecosystems are no longer static. Tablets, laptops, and mobile devices routinely move between locations. Smart TVs may be relocated. Portable streaming devices can be plugged into multiple displays. As viewing migrates fluidly across contexts, the boundary of “the household” becomes less strictly geographic and more behavioral.

The implication is not that deterministic household identity lacks value. On the contrary, it remains the most stable available anchor in the TV and CTV ecosystem. Rather, the implication is that deterministic anchors must be embedded within governance and validation frameworks that explicitly recognize known failure modes.

Identity Infrastructure 2.0 requires a layered architecture in which:

- Deterministic household anchors establish the reference entity, which may derive from authenticated subscriber relationships, verified installation addresses, transaction records, or other persistent first-party signals.
- Device co-location and usage patterns inform household cohesion.
- Temporal refresh cycles account for mobility and decay.
- Explicit confidence scoring communicates linkage strength.
- Transparent documentation clarifies assumptions and limitations.

In this framework, deterministic household identity provides structural stability, but operational accuracy depends on disciplined graph management and ongoing validation. Deterministic anchoring is therefore necessary but not sufficient. While subscriber data often represents one of the most durable household anchors in the TV ecosystem, other combinations of persistent signals — such as stable device clusters, longitudinal behavioral patterns, and verified offline-to-online linkages — can also support deterministic household resolution when appropriately governed and validated.

Chapter 3. Deterministic Household Identity as an Anchor

IP Addresses: Signal, Not Identity

The increasing prominence of IP-based activation in CTV has created both opportunity and confusion. In many programmatic workflows, IP address has been treated as a convenient household proxy. However, treating IP as a durable identity layer introduces structural fragility.

IP addresses are inherently dynamic. Residential broadband providers routinely reassign IPv4 addresses. Carrier-grade NAT environments cause multiple households to appear behind shared infrastructure. IPv6 adoption introduces expanded address pools with different allocation characteristics. Virtual private networks and privacy routing obscure physical origin. Mobile networks introduce further variability.

Even in stable broadband environments, IP-to-household relationships degrade over time. A single IP may map to different residences across weeks or months. Conversely, a single residence may appear associated with multiple IP addresses over short intervals.

When IP is treated as identity rather than signal, over-association becomes likely. Devices may be clustered incorrectly. Households may be conflated. Frequency management and attribution logic may drift.

This suggests a new architectural framing: IP is a connective signal, not a foundational identity spine. In a properly structured system, IP should function as one of several dynamic inputs that resolve toward a more durable anchor. It can:

- Validate device co-location.
- Inform fraud detection.
- Support temporal refresh logic.
- Enhance contextual understanding.
- Assist in de-duplication modeling.

But it should not substitute for authenticated, first-party household identity.

This distinction between “IP as signal” and “IP as identity” is critical. When IP is used as a supporting variable within a governed identity framework, it adds incremental utility. When elevated to primary identifier status without deterministic grounding, it introduces volatility and systemic measurement risk.

Identity Infrastructure 2.0 depends on restoring this hierarchy.

> ***Yes, IP moves. So do people. The issue isn’t movement — it’s whether your infrastructure falls over when it happens.***
>
> *— Charlie Johnson, SVP & GM LocID, Digital Envoy*

Household Identity as an Interoperability Bridge

The TV and CTV marketplace is characterized by institutional fragmentation. Advertisers possess first-party CRM and transaction data. Publishers and distributors control subscriber relationships and viewing exposure logs. Identity providers construct translation layers. Platforms and DSPs execute activation at scale. Measurement vendors reconcile performance across datasets.

Each participant operates under distinct incentives, governance constraints, and technical architectures.

In such an environment, interoperability cannot rely solely on probabilistic stitching or opaque ID translation. It requires a shared structural reference layer.

Chapter 3. Deterministic Household Identity as an Anchor

Household identity performs this bridging function. When properly governed, a household anchor enables:

- Privacy-Safe Data Onboarding: Advertisers can match first-party data into publisher environments through clean room frameworks anchored to stable household entities, minimizing uncontrolled data movement.
- Cross-Screen De-Duplication: Exposure across linear, CTV, and digital devices can be reconciled within a common household framework, reducing overcounting and improving reach accuracy.
- Outcome Attribution: Transaction or store visitation data can be reconciled to exposure through a shared household spine, strengthening measurement credibility.
- Local and Proximity Activation: In geographically anchored use cases — such as local retail or regional campaigns — household identity enables accurate mapping between physical presence and media delivery.
- Governance Transparency: A defined anchor clarifies what entity is being matched and measured, reducing ambiguity in dispute resolution.

In the absence of such an anchor, interoperability becomes dependent on black-box translation systems. These systems may generate scale but often lack explainability. As the ecosystem moves toward greater regulatory scrutiny and AI-enabled optimization, opaque translation layers become less defensible.

Household identity does not eliminate the need for person-level modeling, device graphs, or probabilistic expansion. Rather, it can provide a practical coordination layer that enables more consistent collaboration across activation, measurement, and data-matching workflows.

In this sense, household identity should be understood not as a single standardized identifier or centrally owned asset, but as a functional reference construct that can be implemented through multiple interoperable methodologies. Different stakeholders may maintain their own identity frameworks and governance models, provided they support transparent entity definitions, reconciliation processes, and privacy-compliant data collaboration. The strategic objective is not industry consolidation around one household ID, but improved institutional alignment around how household-level entities are defined, validated, and used in converged TV trading and measurement environments.

> ***Identity isn't a feature. It's plumbing. And plumbing doesn't get applause — it just quietly prevents disaster.***
>
> *— Charlie Johnson, SVP & GM LocID, Digital Envoy*

The Strategic Repositioning of Household Identity

The industry's debate over identity has frequently been framed as a contest between deterministic and probabilistic methodologies. This framing is incomplete and often misleading.

The more consequential shift underway is architectural. Identity Infrastructure 2.0 reorders the layers of the ecosystem:

- Household identity provides structural grounding.
- Person-level models introduce behavioral granularity.
- Device graphs enable activation precision.
- Probabilistic extensions expand scale.
- Governance and transparency frameworks enforce accountability.

In this layered model, deterministic household identity becomes the reference layer — not the entire system.

This repositioning is strategically significant for three reasons.

Persistence: Compared to cookies, mobile ad IDs, or rotating IP addresses, authenticated subscriber relationships exhibit relative stability. While household composition evolves, the contractual relationship between service provider and address changes more slowly than transient digital identifiers. This persistence supports longitudinal measurement and reduces volatility in reach modeling.

Interoperability: A shared household anchor creates a common unit of analysis across stakeholders. It enables structured collaboration between advertisers, publishers, and intermediaries without requiring full exposure of raw identifiers. This is particularly important as clean room environments and privacy-enhancing technologies become standard operating practice.

Compliance Durability: As state-level privacy regimes proliferate and consumer expectations evolve, identity systems must withstand legal scrutiny. Authenticated first-party relationships operate within clearer consent and disclosure frameworks than inferred probabilistic graphs. This does not eliminate compliance risk, but it strengthens defensibility.

Taken together, these attributes position deterministic household identity as foundational infrastructure for the next phase of TV and CTV development.

Identity Infrastructure 2.0 should therefore be understood not as incremental innovation, but as institutional maturation. The market is transitioning from opportunistic linkage strategies toward layered architectures designed for transparency, resilience, and regulatory durability.

Deterministic household identity is the anchor. Probabilistic and modeled signals are extensions. IP and transient identifiers are supporting inputs.

Governance, refresh discipline, and validation are structural requirements. This is not a rejection of scale. It is a rebalancing of fidelity and interoperability within a privacy-constrained environment.

As the ecosystem moves toward AI-assisted activation and increasingly autonomous optimization systems, the stability of the underlying identity spine becomes even more consequential. Intelligent systems amplify both strengths and weaknesses. An unstable identity layer propagates error at scale. A grounded and governed anchor enables responsible automation.

As the ecosystem moves toward AI-assisted activation and increasingly autonomous optimization systems, the stability of the underlying identity spine becomes even more consequential. Intelligent systems amplify both strengths and weaknesses. An unstable or poorly governed identity layer can propagate error at scale, while durable and transparent anchoring supports responsible automation.

The strategic choice before the industry is not deterministic versus probabilistic, nor the elevation of any single data owner or methodology as the defining authority over household identity. Rather, it is a question of architectural coherence versus layered fragility. Deterministic household definitions may be derived through multiple pathways — including authenticated subscriber relationships, persistent device and usage patterns, transaction-based linkages, or other validated first-party signals. Identity Infrastructure 2.0 prioritizes interoperability, governance clarity, and signal validation across these approaches, rather than reliance on any single source of control.

Chapter 4. Transparency, Provenance, and Enterprise Control

The market is reaching a tipping point against opaque identity systems. Buyers increasingly question not just whether identities resolve, but how they resolve: what entity hierarchy is assumed, how frequently linkages are refreshed, and what degree of confidence attaches to each association.

In activation-led use cases, such opacity was often tolerated. In measurement-grade environments — where identity underpins deduplication, outcome attribution, and reconciliation — opacity becomes structural risk. Identity now functions as accounting infrastructure. When discrepancies arise, stakeholders must be able to interrogate the identity layer itself.

Identity now underpins cross-platform measurement, audience deduplication, outcome attribution, smarter planning and privacy compliance. In these contexts, identity is not simply a targeting mechanism; it is an accounting system. When discrepancies emerge between measurement systems, stakeholders must be able to interrogate the identity layer itself. If linkage logic cannot be audited, disputes cannot be resolved.

The industry is moving away from "black box logic" and toward explicit signal-level transparency. This reflects a broader industry realization: effectiveness cannot be decoupled from explainability. As digital budgets come under scrutiny and outcome accountability tightens, identity providers must demonstrate not just scale, but methodological rigor.

Opacity is no longer merely inconvenient — it is a structural risk.

> ***Transparency isn't about exposing complexity — it's about giving marketers confidence. When you can see where signals originate, understand how linkages are formed, and adjust precision by use case, identity becomes something you control, not something you inherit. Visibility empowers enterprises to make informed trade-offs between scale and precision, and to stand behind their strategy with clarity.***
>
> *— Andy Johnson, Chief Data and Product Officer, Adstra*

> ***Publishers' reluctance to share performance data, even in clean rooms, often reflects a deeper concern about loss of control on measurement methodologies and outputs. However, transparency has become a trust prerequisite for brands. When identity linkage methodology and viewer engagement signals are transparent and auditable, performance analytics become insightful for all parties in the ecosystem.***
>
> *— Sebastien Hernoux, Chief Client Solutions Officer, Annalect*

From "Does it Match?" to "How Strong is the Connection?"

Historically, identity performance was summarized in a single metric: match rate. The logic was simple — higher match rate implied greater utility.

This assumption no longer holds: a match is not a match is not a match. Within any reported match rate, linkages vary materially in confidence, persistence, and grounding. Some connections are deterministic and validated. Others are inferred. Some are refreshed daily. Others are point-in-time clusters. Without differentiation, the aggregate match rate obscures critical quality variation.

The industry response is the emergence of signal-strength and connection scoring frameworks.

Adstra, for example, defines Identity Connection Strength (ICS) tiers that allow marketers to tune identity precision versus scale. Under stricter criteria, device associations are limited to those meeting validated thresholds; under relaxed criteria, reach expands but with acknowledged trade-offs. This transforms identity from a binary system (matched / unmatched) into a graduated confidence model.

The implications are significant:

- Measurement use cases can require highest-signal tiers.
- Prospecting use cases may accept lower-confidence expansion.
- Enterprises can explicitly model the trade-off between precision and scale.

This effectively creates an identity metadata layer, an auditable framework describing how, when, and with what confidence each linkage was formed.

Equally, identity increasingly needs to be persistent, configurable, accurate, and consistent across environments. In the agentic era, where AI systems rely on identity inputs to optimize autonomously, linkage strength becomes even more consequential. AI amplifies identity weaknesses; it does not correct them.

The evolution from match-rate reporting to signal-strength transparency is not incremental — it is foundational to maintaining measurement credibility in converged TV.

The Scale Trap and The Incentive Gap

The transparency mandate cannot be separated from economic incentives. During the expansion of omnichannel activation, identity monetization frequently aligned with volume: number of resolved IDs, size of graph coverage, or scale of activation endpoints.

This created a structural "scale trap." When revenue correlates with association volume, the system is incentivized to widen linkage thresholds. Over-association inflates apparent reach but degrades measurement integrity. The Truthset findings suggest that this tension is not theoretical; it is empirically observable.

The resulting incentive asymmetry is clear:

- Identity providers monetize scale.
- Buyers require fidelity.
- Measurement stakeholders require auditability.

Identity Infrastructure 2.0 attempts to realign these incentives by elevating signal provenance, validation methodology, and configurable precision as competitive differentiators.

Composability: Identity in Your Environment

Transparency without control remains incomplete. Enterprise control over identity execution is becoming more important. Rather than forcing clients to send data into provider-controlled environments, often subject to transcoding fees and unlock taxes, identity capabilities are increasingly delivered via composable architectures.

Composability manifests in three principal forms:

- **In-environment deployment:** Identity resolution engines installed within a client's own cloud infrastructure (AWS, Snowflake, Databricks, etc.), allowing full data governance and internal policy enforcement.
- **Clean room interoperability:** Identity collaboration conducted within privacy-safe, zero-copy environments, reducing data movement and exposure risk.
- **Use-case-specific identity application controls:** Rather than "loosening" identity definitions, enterprises increasingly require the ability to govern how identity outputs are applied across activation, measurement, and modeling workflows — for example, determining which signal-confidence tiers are permissible for prospecting versus attribution use cases.

In practice, mature identity systems are designed to maintain the highest available fidelity in the construction of the underlying identity spine. Configurability typically relates not to redefining core identity linkages, but to how identity signals are operationalized in downstream workflows, including audience expansion strategies, precision-versus-scale trade-offs in activation environments, and measurement reconciliation requirements. This distinction reflects a broader architectural principle: identity integrity is foundational, while flexibility is introduced at the level of audience design, optimization strategy, and campaign execution.

This architectural shift addresses multiple structural concerns:

- **Governance:** Identity operates within enterprise privacy controls.
- **Cost efficiency:** Reduced transcoding and unlock fees.
- **Experimentation:** Enterprises can evaluate incrementality across identity partners.
- **Resilience:** Identity spines can be adapted as regulatory or market conditions evolve.

In some cases, marketers are demanding ownership, transparency, and control, not simply access to an ID key. Household identity infrastructure must therefore function as a neutral coordination layer between advertisers, publishers, identity providers, and platforms.

"Neutrality" in this context does not imply the existence of a single central operator. Rather, it reflects the need for interoperable technical standards, auditable methodologies, and governance frameworks that enable collaboration across independently operated identity systems. Industry bodies, standards organizations, measurement accreditation processes, and contractual data-collaboration frameworks can collectively play this coordinating role, helping ensure that identity linkages are explainable, privacy-compliant, and institutionally trusted without requiring consolidation around a single provider or identifier.

Transparency as a Precondition For the Agentic Era

Identity is foundational infrastructure for the "Agentic Era", an environment in which AI systems autonomously optimize media, personalize experiences, and orchestrate journeys in real time.

In this context, transparency is not merely a buyer preference; it is a systemic requirement. Autonomous systems require:

- Stable identifiers.
- Consistent entity hierarchies.
- Clear provenance of signals.
- Persistent cross-channel linkage.

When these are absent, automation compounds error. AI optimizes against distorted signals. Measurement discrepancies widen. Personalization becomes misaligned.

Identity Infrastructure 2.0 therefore rests on three pillars:

Explainability: Every linkage can be traced.

Configurable precision: Enterprises control fidelity thresholds.

Governance alignment: Identity logic operates within enterprise and regulatory constraints.

The era of opaque, volume-driven identity graphs is giving way to configurable, privacy-centered, provenance-aware identity systems.

Chapter 4. Transparency, Provenance, and Enterprise Control

> ***This framework reflects exactly where the ecosystem needs to go, and where we are focused with our customers: transparent, interoperable, and measurement-grade identity foundations. As TransUnion powers the holistic flywheel of activation, insights, and measurement, we see the value of this modernized approach translate directly into real business impact at each step for the advertisers, agencies, and platforms we serve. Interoperable and resilient, future-ready identity architecture aren't just ideals for us — they're core to what we're enabling across the ecosystem today.***
>
> *— Brian Silver, EVP of Marketing Solutions, TransUnion*

Strategic Implications

Transparency, provenance, and enterprise control collectively represent a structural evolution in identity resolution. They shift identity from vendor-controlled activation middleware toward enterprise-governed infrastructure. They also reframe performance expectations — from simple match-rate expansion toward demonstrable data stewardship, privacy resilience, and measurement credibility.

For senior executives, the most relevant strategic questions are typically not about tuning identity mechanics, but about governance, risk, and operational control. These include:

- How will our first-party data be used, combined, or modeled within identity frameworks?
- Does the identity solution operate in a privacy-compliant and regulatorily defensible manner?
- Can identity capabilities be deployed within our own cloud or governed collaboration environments?
- Does the identity approach support consistent measurement, reconciliation, and cross-platform accountability?
- Can we trust the identity layer to maintain high fidelity while enabling scalable activation through audience strategy and execution choices?

Identity Infrastructure 2.0 is not simply about better matching. It is about restoring trust in the connective tissue of converged TV.

Identity Infrastructure 2.0 is not simply about improving match performance or introducing new technical controls. It is about enabling enterprises to operate with confidence that their identity foundations are durable, privacy-aligned, and capable of supporting converged planning, activation, and measurement at scale.

Chapter 5. Identity Velocity and Deconfliction Across Expanding Touchpoints

Identity in converged TV is inherently multi-representational. A single individual may appear as a work email in one system, a hashed loyalty ID in another, a household-level CTV identifier elsewhere, and a device-level ID in programmatic logs.

None of these representations is necessarily incorrect. Each reflects a legitimate interaction within a specific system boundary. The problem is incompleteness and inconsistency.

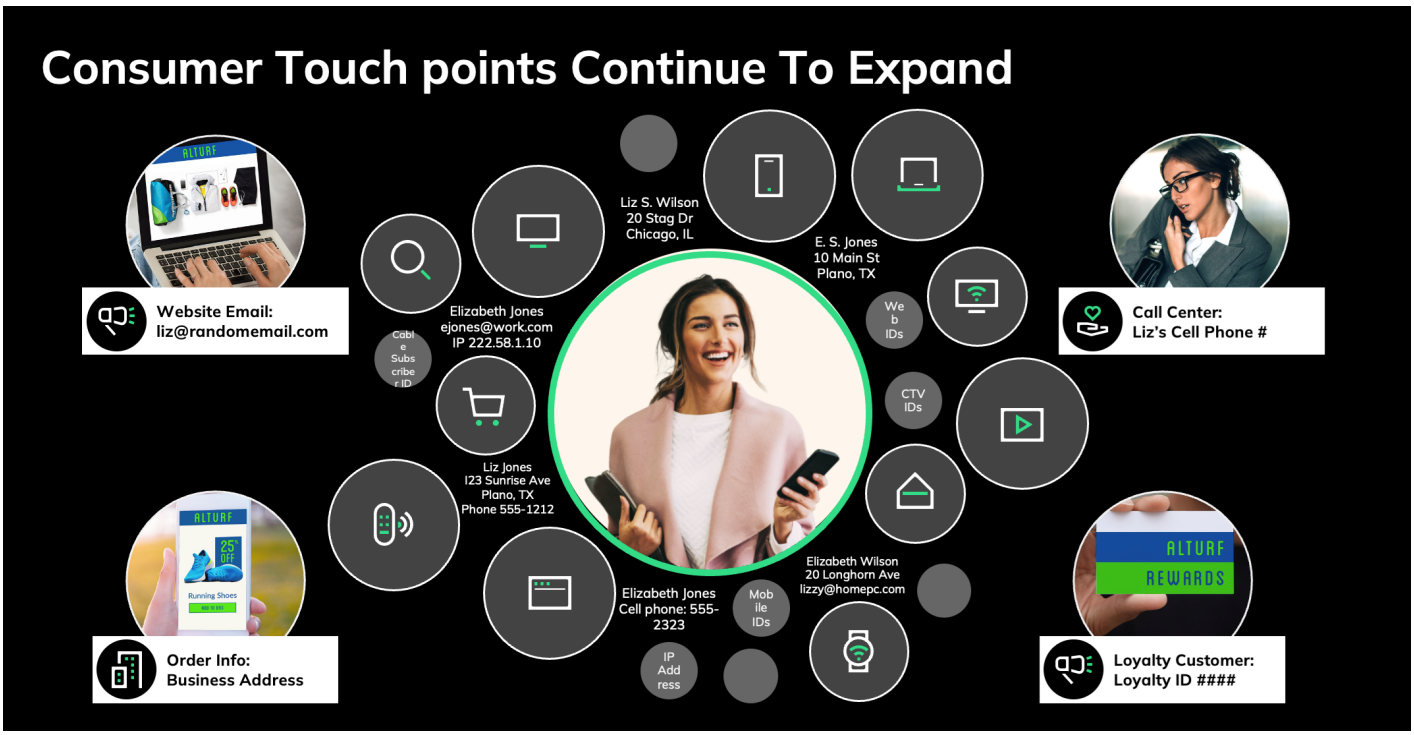
The operational challenge is deconfliction, reconciling multiple identifiers into a coherent person-household spine while preserving appropriate separation between entity layers. It requires:

- Resolving multiple identifiers to a unified entity.
- Translating identifiers across platforms (e.g., device ID to household ID).
- Deconflicting conflicting attributes (e.g., competing emails or postal records).
- Preserving appropriate separation between household and individual layers.

Consumers do not experience brands as fragmented silos. They experience them as a single enterprise. Identity infrastructure must therefore bridge identifiers responsibly and accurately so that systems see "*one person, not ten disconnected records*"[2].

In the absence of deconfliction, fragmentation compounds. In the presence of deconfliction, interoperability becomes possible.

Figure 3: Touchpoint Fragmentation



Source: LiveRamp

[2] Source: LiveRamp: *The Evolution of Identity in the Agentic Era*, CIMM Showcase (February 18, 2026)

Chapter 5. Identity Velocity and Deconfliction Across Expanding Touchpoints

These capabilities are increasingly regarded as core functional requirements of modern identity resolution systems. However, their consistent execution at national scale, across heterogeneous CTV supply environments, privacy regimes, and competing measurement frameworks remains operationally complex. In converged TV, deconfliction is not simply a technical feature but an institutional coordination challenge, requiring alignment between activation platforms, data providers, publishers, and measurement systems that may rely on different identity assumptions. As a result, what may appear as "table stakes" at the level of system design can still represent a meaningful source of variability in campaign delivery, reconciliation outcomes, and cross-platform comparability in real-world trading environments.

Beyond the Static Viewpoint: Identity as Ecosystem

Traditional identity graphs were often constructed as static clusters: a periodic stitching of signals into a point-in-time representation of relationships. This approach is increasingly insufficient.

Consumers move. Devices churn. IP addresses rotate. Apps are deleted and reinstalled. Cookies disappear. Accounts are shared. New touchpoints emerge.

Identity is not a single point in time — it is a dynamic system that is ever-evolving.

> ***Identity is not static — it constantly evolves as people move, devices change, and signals shift. The real breakthrough is architecting identity as a network, not a graph: a system built to continuously resolve, translate, and adapt. With transparent refresh and configurable governance, that network becomes a durable infrastructure that can power converged ecosystems and the next era of AI-driven growth.***
>
> *— Andy Johnson, Chief Data and Product Officer, Adstra*

The concept of identity velocity captures this reality[3]. Identity velocity refers to the ability of an identity system to:

- Ingest new signals rapidly.
- Retire stale associations.
- Update linkages based on new evidence.
- Maintain coherence across evolving device ecosystems.

A living identity network continually resolves and re-resolves connections as signals change. Static graphs provide a glimpse at a moment in time; dynamic systems track the evolving story.

From a measurement perspective, velocity matters for several reasons:

- **IP Rotation and Device Churn:** IP addresses are frequently reassigned. Device ownership changes. Without refresh logic, associations decay silently.
- **Account Sharing and Mobility:** Streaming services introduce portable viewing. Household definitions can blur across residences or travel patterns.
- **Signal Volatility in Digital Environments:** Cookies expire. Mobile advertising IDs reset. Browser-level identifiers fragment.

[3] Source: Adstra data Solutions, *Rethinking Identity: Empowering Researchers Through Transparency*, CIMM Showcase (February 18, 2026)

Chapter 5. Identity Velocity and Deconfliction Across Expanding Touchpoints

Without explicit refresh cadence and linkage governance, identity degradation accumulates invisibly. Measurement windows drift. Frequency management weakens. Attribution reliability declines.

Measurement-grade identity requires clarity about:

- Which signals are persistent (e.g., subscriber relationship, postal anchor).
- Which are transient (e.g., device-level digital identifiers).
- How often linkages are refreshed.
- What triggers reassignment or decoupling.

The distinction between identity systems optimized for activation scale and those designed to support measurement-grade persistence is increasingly recognized across the industry, but it is not always well understood outside specialist technical and analytics teams. Senior decision-makers often engage with identity outcomes, such as reach delivery, frequency control, or attribution results, rather than the underlying signal governance that shapes those outcomes. As converged TV workflows become more data-driven and AI-assisted, the ability to differentiate between scale-oriented linkage strategies and measurement-oriented identity design is likely to become more strategically consequential. This places greater emphasis on clear communication of identity assumptions, signal durability, and refresh practices as part of enterprise media governance.

Identity Infrastructure 2.0 does not merely resolve signals. It operationalizes refresh discipline. Modern identity systems must function as translation engines, serving as a Rosetta Stone across media platforms, commerce systems, clean rooms, and AI models. Identity enables enabling "*resolve, translate, and deconflict in the cloud*"[4] .

Translation includes:

- Converting a first-party CRM record into interoperable activation identifiers.
- Mapping campaign exposure logs to person-based or household-based spines.
- Aligning measurement outputs across publishers with differing identifier schemas.
- Harmonizing identity hierarchies across buy-side and sell-side platforms.

In a converged TV environment, this translation is particularly critical. CTV platforms may expose device-level identifiers. MVPDs operate at subscriber-household levels. FAST environments may be IP-based. DSPs may rely on proprietary ID spines. Without a translation layer, cross-platform frequency control and deduplicated reach become probabilistic approximations.

Translation must operate across multiple touchpoints, including:

- Person-level identifiers.
- Household-level identifiers.
- Device-level identifiers.
- Account-level identifiers.

When translation is robust, interoperability improves. When translation is opaque, discrepancies proliferate.

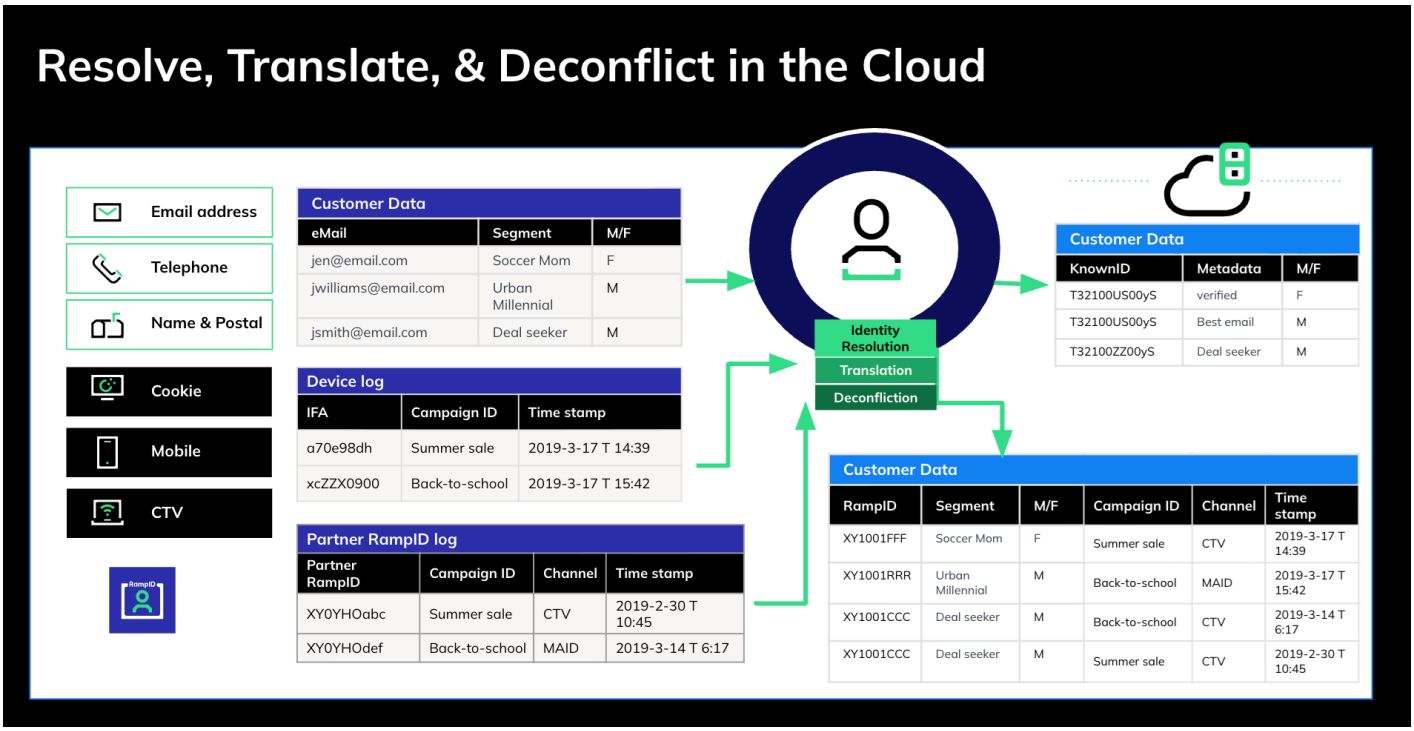
In a converged TV environment, this translation function becomes particularly critical. Identity resolution systems are responsible for linking multiple identifiers to coherent person-or household-level entities while maintaining the associated identifier relationships. However, effective cross-platform execution also requires the ability to operationalize those linkages across heterogeneous activation and measurement environments that rely on different identifier namespaces, data-access constraints, and workflow conventions.

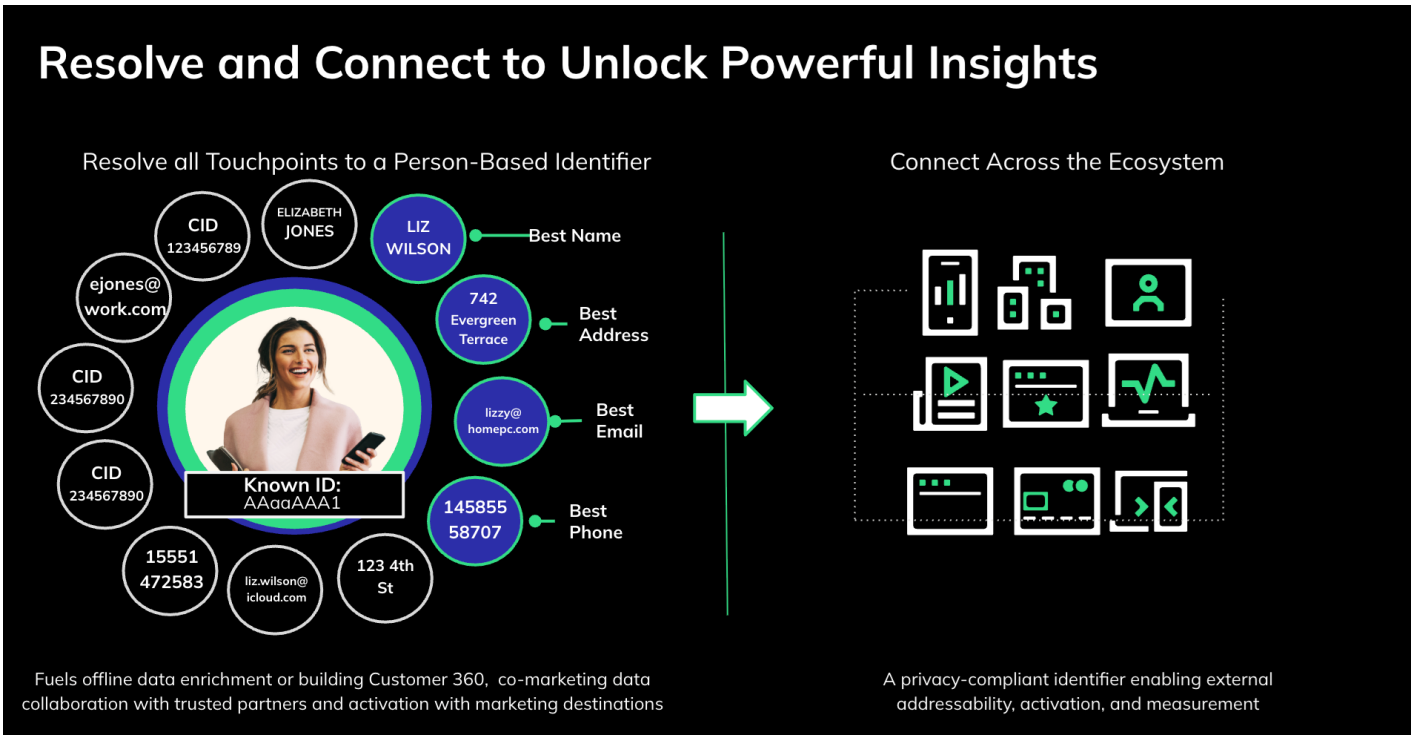
[4] Source: LiveRamp: *The Evolution of Identity in the Agentic Era*, CIMM Showcase (February 18, 2026)

Chapter 5. Identity Velocity and Deconfliction Across Expanding Touchpoints

In this sense, identity resolution provides the underlying entity spine, while additional translation processes enable identifiers to be mapped, activated, or reconciled across platforms — for example, converting household-level exposure data into demand-side addressable signals, aligning publisher-specific identifiers with buy-side ID frameworks, or enabling privacy-safe matching in clean room environments. Where this operational translation layer is robust and transparent, interoperability improves. Where linkage logic exists but cannot be effectively propagated or reconciled across systems, discrepancies in frequency control, reach measurement, and attribution outcomes are more likely to emerge.

Figure 4: Identity Resolution Process and Benefits





Source: LiveRamp

Chapter 5. Identity Velocity and Deconfliction Across Expanding Touchpoints

The Risk of Silent Drift

While insufficient refresh leads to decay, overly aggressive reassignment of identifiers can introduce instability. Rapid dissolution of associations based on short-term signal changes may fragment longitudinal measurement, particularly when campaign exposure windows must align with delayed outcome signals.

For example:

- A household IP rotates within a 30-day window.
- A device temporarily connects from a secondary location.
- A user logs in from a different residence while traveling.

If identity linkages are recalibrated too quickly, continuity in reach measurement, frequency management, and attribution analysis may deteriorate. Refresh cadence is therefore not solely a technical parameter; it is an architectural governance consideration.

In practice, mature identity systems are designed to manage refresh logic and persistence rules in service of defined use cases, prioritizing the most stable and validated signals available over time. Enterprise involvement typically focuses on transparency, policy alignment, and performance evaluation rather than manual adjustment of core identity linkages. This reflects an important distinction: identity fidelity is maintained at the infrastructure level, while scale trade-offs are more appropriately addressed through audience strategy, targeting expansion, and media execution decisions.

Identity Infrastructure 2.0 therefore emphasizes disciplined signal stewardship, explainable refresh practices, and measurement continuity, rather than direct marketer intervention in graph construction.

Velocity in the Agentic Era

The rise of autonomous AI systems intensifies the need for identity velocity and deconfliction. AI agents are beginning to optimize media, personalize experiences, and orchestrate journeys in real time[5]. These systems ingest identity signals as training inputs.

When identity is fragmented:

- AI models learn from inconsistent entity representations.
- Optimization loops amplify incorrect associations.
- Measurement and personalization drift apart.

When identity is coherent but stale:

- AI optimizes against outdated linkage.
- Campaign decisions reflect yesterday's relationships.

When identity refresh is overly aggressive:

- AI loses longitudinal continuity.
- Model stability deteriorates.

[5] Source: LiveRamp: *The Evolution of Identity in the Agentic Era*, CIMM Showcase (February 18, 2026)

As such, identity velocity must be calibrated. Autonomous systems require:

- Stable person-and household-based anchors.
- Documented signal provenance and confidence metadata, enabling AI systems and measurement processes to differentiate between deterministic, modeled, or transient identity inputs. This supports more reliable model training, clearer interpretation of optimization outcomes, and improved ability to diagnose performance variance when identity assumptions change over time.
- Configurable refresh logic.
- Continuous deconfliction across touchpoints.

In AI-assisted environments, understanding how identity linkages were derived — including signal type, recency, and confidence — helps prevent models from over-weighting weak or outdated associations and allows enterprises to interpret performance signals more accurately across platforms and time periods.

Identity becomes the operational substrate of AI.

Strategic Implications

The multi-identifier reality is not temporary. Consumer touchpoints will continue to expand across connected devices, agents, accounts and services, including:

- CTV
- Mobile
- Web
- Commerce
- Retail media
- Call centers
- AI agents

The number of identifiers per individual will not shrink. It will compound. The question is not whether fragmentation exists. It is whether enterprises can deconflict it coherently. Identity Infrastructure 2.0 requires:

- Explicit person-household-device hierarchies.
- Continuous resolution rather than static clustering.
- Transparent refresh cadence.
- Configurable persistence logic.
- Robust translation across activation and measurement systems.

Velocity without governance creates instability. Persistence without refresh creates decay. Deconfliction without transparency creates opacity. The objective is balance: stable where stability is required, adaptive where volatility is meaningful. In converged TV, identity velocity is not an optimization feature. It is a structural requirement.

Chapter 6. Privacy-by-Design and Governance Architecture

Privacy is no longer a constraint layered onto identity systems — it is the primary architectural driver of the next phase of identity infrastructure.

In the US, the absence of a single federal privacy regime, combined with the rapid expansion of state-level legislation, has created a complex and evolving compliance landscape. Enterprises increasingly design systems to satisfy the strictest applicable standard rather than optimize for minimal compliance. This "*highest common denominator*" approach is not merely defensive; it reflects recognition that identity systems must be durable under regulatory scrutiny.

The structural implication is clear: identity solutions built without privacy at their core will face escalating integration friction and commercial risk.

Historically, identity resolution systems were often optimized for scale and match rate first, with privacy controls layered on top. In contrast, Identity Infrastructure 2.0 inverts that order. It begins with consent frameworks, server-side controls, and data minimization principles, and then builds resolution capabilities within those boundaries.

Privacy-centric identity does not necessarily reduce functionality. On the contrary, it can expand collaboration opportunities. Systems designed to operate within authenticated subscriber relationships, governed clean rooms, and secure server-side environments enable advertisers and publishers to share insights without exposing raw personal data.

In this model, privacy is not a brake on innovation; it is the foundation of sustainable interoperability. Privacy is a requirement, not an option.

Consent-grounded Identity and First-party Anchoring

The shift toward privacy-by-design aligns directly with the re-anchoring of identity around deterministic household and subscriber relationships. The most resilient identity systems are grounded in authenticated, first-party relationships operating within explicit consent frameworks. When enrichment and linkage occur inside environments where the enterprise has a direct relationship with the user — whether through subscription, login, contractual services or transactions — the identity spine inherits the governance protections of that relationship.

Consent-grounded operation has several structural characteristics:

- Linkages occur within established user relationships.
- Purpose limitation aligns with disclosed use cases.
- Data use policies are contractually and technically enforced.
- Opt-out and suppression signals propagate through the system.

This architecture differs materially from third-party probabilistic stitching conducted outside authenticated contexts. The former operates within defined governance boundaries; the latter often relies on inferred associations with weaker transparency.

The long-term durability of identity infrastructure depends on embedding linkage within consent frameworks, not merely attaching disclosure statements after resolution.

More broadly, linkage strategies that extend identity associations beyond clearly consented or authenticated contexts can introduce both governance risk and operational uncertainty. Where identifiers are bridged or inferred across environments without durable validation or transparent purpose alignment, the resulting identity constructs may be less stable over time and more difficult to reconcile in activation and measurement workflows. This can contribute to misaligned audience delivery, performance variability, and increased risk of media waste.

Chapter 6. Privacy-by-Design and Governance Architecture

As privacy expectations evolve, Identity Infrastructure 2.0 places greater emphasis on ensuring that identity expansion techniques remain proportionate, explainable, and grounded in defensible consent and data-use frameworks.

Server-side Resolution and the Protection of Raw Deterministic Data

Some parts of the identity ecosystem are shifting towards server-side identity resolution. In this architecture, deterministic data — such as subscriber records or installation addresses — is not distributed broadly across the ad tech ecosystem. Instead, linkage occurs within secure environments, and buyers receive derived identifiers, enriched signals, or aggregated outputs rather than raw personal data.

This separation serves multiple governance objectives:

- **Data Minimization:** Only necessary outputs are shared; raw inputs remain protected.
- **Reduced Surface Area:** Fewer systems directly access sensitive identifiers.
- **Controlled Interoperability:** Clean rooms and privacy-enhancing technologies enable collaboration without uncontrolled data leakage.
- **Auditability:** Server-side processing allows logging, access controls, and compliance review.

Identity in the agentic era must operate inside governed cloud environments rather than across loosely controlled data transfers. This is particularly important as enterprises increasingly deploy identity inside their own cloud infrastructure, where governance policies can be centrally enforced.

The architectural pattern is clear: raw deterministic data stays close to its source and interoperable signals travel outward in controlled form.

Auditable Linkage Quality and Methodological Transparency

Identity systems should provide stakeholders with sufficient evidence to assess the reliability, stability, and appropriate use of identity associations. In many cases, this can be achieved through confidence scoring frameworks, standardized metadata, and independent validation processes rather than full disclosure of proprietary signal sources or linkage methodologies.

Examples of relevant auditability indicators may include:

- Signal provenance (where did this linkage originate?)
- Refresh cadence (when was it last validated?)
- Validation methodology (what ground truth or confidence model was applied?)
- Entity hierarchy (household, person, device, account relationships).

The objective of transparency in this context is not to require disclosure of commercially sensitive “secret sauce,” but to enable advertisers, publishers, and measurement providers to determine whether identity inputs are fit for specific activation or measurement use cases. This form of outcome-oriented transparency supports institutional trust and market comparability while preserving incentives for continued innovation in identity methodologies.

Without this metadata, privacy compliance may exist technically but fail institutionally. Stakeholders cannot interrogate discrepancies. Regulators cannot evaluate data lineage. Enterprises cannot defend their methodologies in audit or litigation scenarios.The showcase discussions reinforced that provenance is becoming table stakes. Black-box logic may achieve reach, but it undermines institutional trust.

Auditability, therefore, is not simply a feature — it is a governance requirement.

Chapter 6. Privacy-by-Design and Governance Architecture

Policy Controls and Operational Enforcement

Beyond architecture and audit trails, governance must be operationalized. Identity systems require enforceable policy controls, including:

- **Opt-out propagation:** User opt-outs must cascade across linkage layers.
- **Suppression logic:** Sensitive categories or contractual exclusions must be enforced at the resolution layer.
- **Purpose limitation controls:** Identity outputs must align with declared use cases.
- **Retention discipline:** Stale linkages must be retired according to policy.

In practice, this means that identity infrastructure must embed policy engines alongside resolution engines. The technical system and the governance system cannot be separated. As privacy regimes continue to evolve, the ability to adapt suppression logic, modify retention windows, and update consent mappings will become a competitive differentiator. Enterprises that lack configurable governance layers will struggle to adapt.

The Identity Control Plane

A useful way to conceptualize this governance layer is as an identity control plane.

Borrowing from cloud architecture terminology, the control plane governs how the system operates, while the data plane executes transactions.

Applied to identity, the control plane includes:

- Policy rule management.
- Consent mapping.
- Linkage configuration thresholds.
- Logging and monitoring.
- Access controls.
- Audit interfaces.

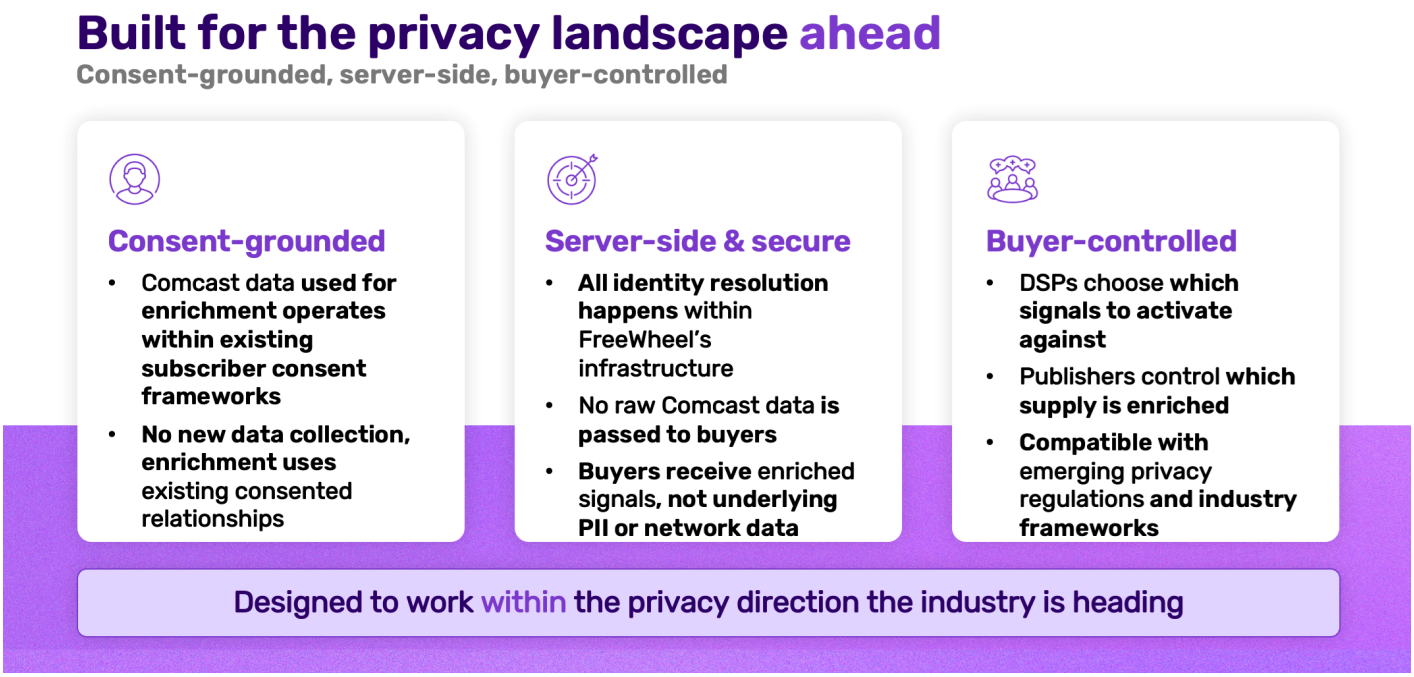
The data plane performs the resolution itself. The control plane governs when, how, and under what conditions that resolution occurs.

Chapter 6. Privacy-by-Design and Governance Architecture

In mature markets, shared infrastructure only becomes institutionally trusted when control planes are visible and standardized. Financial clearinghouses, telecommunications networks, and payment systems all operate with defined governance interfaces.

Identity Infrastructure 2.0 is moving in the same direction. While underlying identity graphs may remain diverse — deterministic-first, probabilistic-extended, or hybrid — there is likely to be convergence around standardized governance interfaces. These interfaces enable enterprises to evaluate compliance posture independently of graph methodology. In this sense, the identity control plane becomes a prerequisite for ecosystem-scale trust.

Figure 5: Identity Infrastructure 2.0 Governance Paradigms



Source: FreeWheel

Strategic Implications

Privacy-by-design and governance architecture are not compliance checklists. They are structural determinants of interoperability. As identity becomes the substrate for AI-driven activation, cross-platform measurement, and enterprise-wide personalization, governance weaknesses propagate system-wide.

Identity Infrastructure 2.0 requires:

- Consent-grounded deterministic anchoring.
- Server-side resolution and minimized data exposure.
- Transparent provenance and refresh documentation.
- Configurable policy enforcement.
- Institutionalized control planes.

Privacy is not slowing identity innovation. It is reshaping it. Systems designed for durability under regulatory scrutiny will expand collaboration opportunities. Systems optimized purely for short-term scale will face integration friction, measurement disputes, and reputational risk.

In converged TV, privacy-by-design is now a structural precondition for interoperability.

Chapter 7. Healthcare as a Stress Test for Identity Architecture

Healthcare stands apart as a structural stress test for identity systems. Healthcare advertising operates under heightened regulatory constraints, including strict protections around protected health information (PHI), limitations on data use, and elevated expectations of consumer trust. Identity resolution in this environment is not a convenience feature — it is non-negotiable infrastructure.

Unlike many consumer categories, healthcare campaigns often require:

- Sensitive audience definition (e.g., condition-based targeting).
- Separation between consumer and healthcare professional (HCP) outreach.
- Closed-loop outcome measurement (e.g., prescriptions, claims).
- Documentation sufficient to withstand compliance audit.

These requirements force identity architecture to operate under more demanding standards than typical consumer activation use cases.

Healthcare identity cannot rely on loosely governed probabilistic stitching. It must be architected around deterministic anchors, tokenization, and clear separation between regulated inputs and activation outputs.

In this sense, healthcare is not an edge case. It is a preview of where identity infrastructure must evolve as privacy expectations tighten across sectors.

Dual Identity Layers: Consumers and Healthcare Professionals

A defining characteristic of healthcare identity architecture is its dual-layer structure.

First, there is **consumer identity** — often derived from tokenized patient records or privacy-enhanced datasets. This layer supports audience construction and outcome measurement while avoiding direct exposure of regulated identifiers.

Second, there is **healthcare professional identity**, typically grounded in deterministic National Provider Identifier (NPI) frameworks. NPI-linked identity enables targeting and measurement at the physician or provider level, often connected to prescribing or claims activity.

The two layers are structurally distinct:

- Consumer identity must be tokenized and privacy-preserving.
- HCP identity is deterministic and registry-based.
- Cross-layer linkages must avoid inappropriate commingling.
- Measurement frameworks must reconcile exposures and outcomes without revealing PHI.

This duality illustrates a broader architectural principle: identity systems must support multiple entity hierarchies simultaneously.

In healthcare, that means explicitly modeling:

- Patient (tokenized entity).
- Household (where relevant).
- Provider (NPI-anchored professional).
- Device and media exposure signals.
- Outcome records (scripts, claims, visits).

Healthcare therefore forces identity architecture to mature beyond flat graphs and toward explicit multi-entity models.

Chapter 7. Healthcare as a Stress Test for Identity Architecture

Identity's Three Core Jobs in Healthcare

In healthcare, identity performs three distinct, but interdependent, roles.

1. **Translate regulated data into activatable signals:** Healthcare campaigns often begin with regulated datasets — claims, scripts, or condition-level cohorts. These inputs cannot simply be merged with digital identifiers in open ecosystems. Identity infrastructure must translate regulated data into activatable audiences without exposing PHI. This typically involves:

   - Tokenization.
   - Hashing and salting.
   - Server-side resolution.
   - Clean room collaboration.
   - Strict access controls.

   The objective is to preserve privacy while enabling media activation.

2. **Expand reach without commingling sensitive inputs:** Healthcare marketers frequently need to expand reach beyond deterministic patient lists. Modeling and cohort expansion may be used to identify lookalike audiences. However, such expansion must not commingle regulated inputs directly with open-web identifiers.

   This requires architectural separation between:

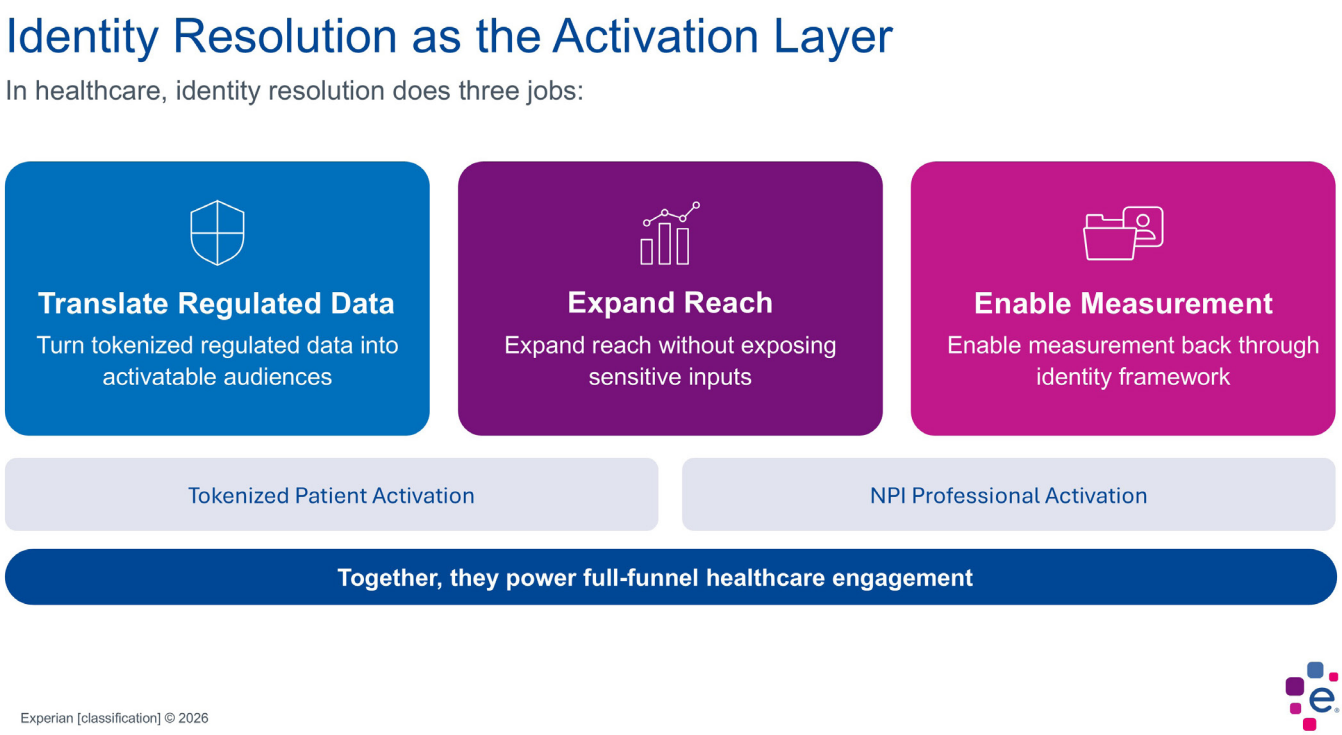
   - Deterministic seed cohorts.
   - Modeled or contextual expansion logic.
   - Media activation layers.

   The healthcare use case demonstrates how identity infrastructure can support reach expansion while preserving compliance boundaries.

3. **Enable closed-loop measurement:** Perhaps most critically, healthcare requires compliant closed-loop measurement. Exposure must be reconciled to downstream outcomes — such as prescriptions or claims — through the same identity framework that governed activation. Measurement cannot rely on a separate identity logic without risking discrepancy or audit failure.

   This reinforces a broader principle: activation and measurement identity spines must align. In healthcare, that alignment is mandatory. In other verticals, it is increasingly desirable.

Figure 6: Identity Resolution in Healthcare



Source: Experian

Identity as Intelligence Infrastructure

The healthcare session also illustrated a broader shift: identity is evolving from an activation mechanism into intelligence infrastructure. Deterministic cohorts — such as confirmed patients or verified HCPs — serve as high-quality training labels for contextual and AI systems. These cohorts can be used to identify correlated signals in environments where direct identifiers are absent.

For example:

- Deterministic patient cohorts can train contextual models to identify relevant content environments.
- Verified HCP engagement patterns can inform professional targeting algorithms.
- Closed-loop measurement can refine predictive models.

In this framework, identity does not disappear in lower-ID environments. Instead, deterministic identity seeds model training, enabling AI systems to operate responsibly where identifiers are constrained.

Healthcare demonstrates this transition clearly because the stakes are high. Models must be trained on accurate, consent-grounded signals to avoid regulatory risk.

The pattern generalizes beyond healthcare:

- Retail media can use deterministic loyalty data to train contextual models.
- Automotive brands can use verified purchase data to improve lookalike modeling.
- Financial services can use authenticated account relationships to seed AI-driven personalization.

Healthcare shows that deterministic identity is not merely for direct activation — it becomes the foundation for intelligence systems that operate in ID-light contexts.

Chapter 7. Healthcare as a Stress Test for Identity Architecture

Perspectives on Healthcare Identity – Scott Kozub, VP Product Management, Experian

Healthcare advertising operates in two different identity worlds. On one side, you have patient and consumer identity. On the other, you have deterministic provider identity tied to National Provider Identifiers (NPIs). Both are growing quickly as digital healthcare investment accelerates, and both sit inside strict regulatory guardrails. That's what makes identity resolution in healthcare fundamentally different from most other categories.

For patients, activation requires tokenization, suppression of source data, and a clear separation from digital identifiers. Claims or prescription data can't simply flow into media platforms. Identity has to function as a privacy bridge, abstracting regulated inputs into audiences that can be activated and measured without ever exposing PHI.

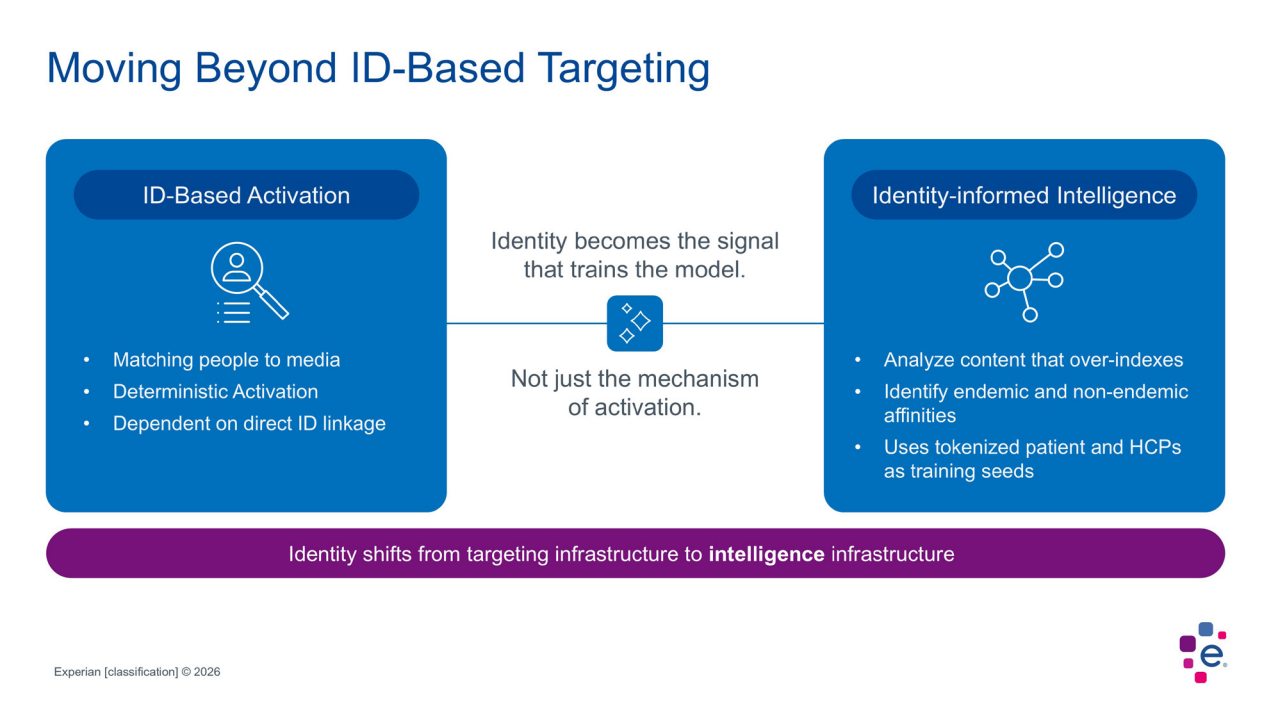
For providers, the dynamic is different. Healthcare professionals operate within a structured identity framework anchored to NPI. When NPIs are resolved to digital endpoints, advertisers can reach specialties with precision and measure outcomes back to the professional.

In this environment, identity isn't just a match key. It translates regulated data into activation, enables responsible reach expansion, and connects exposure back to outcomes for closed-loop measurement.

More recently, identity is also becoming a signal for expanded intelligence. Tokenized patient and NPI-based cohorts can inform AI and contextual models, allowing advertisers to extend reach in privacy-forward environments where direct ID matching may not be available.

Healthcare's future won't be built on matching the most IDs. It will be built on treating identity as compliant, intelligence-driven infrastructure.

Figure 7: Intelligence Infrastructure Built on Identity



Source: Experian

Chapter 7. Healthcare as a Stress Test for Identity Architecture

Broader Lessons For Converged TV

Healthcare reveals structural truths about identity architecture:

1. **Multi-layer modeling is essential:** Flat graphs are insufficient in regulated, multi-entity environments.
2. **Governance must be embedded, not layered:** Privacy controls and auditability are foundational.
3. **Activation and measurement must share an identity spine:** Divergent identity logic creates reconciliation risk.
4. **Deterministic anchors enable responsible AI expansion:** High-quality labels improve model performance in constrained environments.

Converged TV increasingly shares these characteristics:

- Sensitive demographic and behavioral targeting.
- Cross-platform measurement scrutiny.
- Heightened regulatory visibility.
- AI-driven optimization.

Healthcare therefore acts as a stress test for identity infrastructure. If identity architecture can withstand healthcare's compliance and measurement demands, it is more likely to withstand the next phase of converged TV evolution.

> ***Healthcare identity resolution isn't just about matching people to media; it's about creating a privacy-preserving infrastructure that translates regulated health insights into activatable audiences while maintaining strict separation from sensitive inputs. In healthcare, identity is the compliance backbone that enables scale without compromising trust.***
>
> *— Scott Kozub, VP Product Management, Experian*

Strategic Implications

The strategic insight from healthcare is not that every vertical must replicate its compliance complexity. Rather, it is that identity infrastructure must be built to withstand environments where:

- Privacy constraints are strict.
- Audit risk is real.
- Measurement stakes are high.
- AI systems depend on accurate labels.

Healthcare makes visible what is otherwise latent: identity fragility. Identity Infrastructure 2.0 — grounded in deterministic anchors, tokenization, server-side resolution, transparent governance, and multi-entity modeling — emerges as the architectural response.

In this sense, healthcare is not an exception. It is a preview.

Chapter 8. Identity Meets Proximity: Bringing Real-World Context into TV

One of the most consequential evolutions shaping the identity ecosystem the convergence of identity infrastructure with proximity intelligence. For decades, television advertising operated largely at the national or broad regional level. Even local linear advertising relied on market-level or ZIP-code approximations. CTV has introduced new flexibility, but much of that flexibility initially focused on audience segments rather than physical context.

Proximity intelligence changes the equation. By linking household identity to real-world geographic context — neighborhoods, store catchments, and movement patterns — TV advertising can reconnect to physical commerce environments. Household identity becomes the bridge between media exposure and place-based behavior.

This shift is occurring at the same time that:

- Local video budgets are expanding.
- Retail media networks are reshaping performance expectations.
- Advertisers demand store-level relevance and measurable outcomes.
- Cross-channel frequency management extends into CTV.

Proximity intelligence is not merely a location signal layered on top of media. It requires a stable household identity spine capable of mapping exposures to real-world context in a privacy-aware manner.

Without identity infrastructure, proximity remains descriptive. With identity infrastructure, proximity becomes actionable.

From ZIP Codes to Catchment Intelligence

Historically, local TV buying relied on coarse geographic approximations. ZIP codes and DMA boundaries served as proxies for store reach or demographic clustering.

Proximity-enabled identity models operate at a more refined level.

By anchoring exposure at the household level, identity systems can:

- Map households to specific store catchment areas.
- Model likely store visitation zones.
- Align media activation with real-world distribution footprints.
- Optimize frequency based on local retail presence.

This enables more granular strategic questions:

- Which households fall within high-value retail corridors?
- How does campaign reach differ across competitive catchments?
- Can creative messaging vary by neighborhood composition?
- How do store-level sales correlate with CTV exposure?

The key enabler is the deterministic household anchor, described earlier in this report. Household identity provides geographic persistence. Device-level identifiers alone cannot reliably map to stable place-based context.

In this model, identity transforms proximity from an abstract coordinate into a business-relevant unit of analysis.

Chapter 8. Identity Meets Proximity: Bringing Real-World Context into TV

Proximity and Outcome Accountability

The institutional implications are substantial. As advertisers demand stronger accountability, proximity-enabled identity architectures strengthen the link between exposure and outcome.

For example:

- Media exposure at the household level can be reconciled with store-level transaction data.
- Retail matchback analysis can evaluate incremental sales within defined catchments.
- Campaign performance can be compared across local strategies.

When identity and proximity are integrated within a shared governance framework, measurement gains credibility. The same household spine that governed activation governs outcome reconciliation.

This reduces reconciliation disputes and improves transparency.

In effect, proximity reintroduces physical commerce into the TV measurement equation — an increasingly important development as CTV competes with retail media and performance-oriented digital channels.

As CTV grows up, identity has to grow up with it.

One of the core tensions in converged TV is that most digital identity systems were built for individuals and devices, while television has always operated at the household level. CTV sits between those worlds. It's digital in how it's delivered, but still largely consumed as a shared household experience. When device-centric identity is forced onto that environment, fragmentation is almost inevitable.

IP tends to be framed in extremes. It's either treated as a shortcut to household identity or dismissed entirely because of volatility. In reality, it's neither.

IP is not identity on its own — it's a signal. It naturally connects devices within a home network, aligning with how CTV is consumed. But it's also dynamic. Reassignment, router resets, and network changes introduce instability if the signal isn't governed thoughtfully.

The more productive framing isn't "IP versus deterministic identity." It's how IP can be stabilized so that it functions as a durable household-level anchor.

When IP-derived signals are stabilized and designed to persist through network changes, fragmentation is reduced — particularly in FAST and unauthenticated CTV environments where other identifiers may be inconsistent or absent.

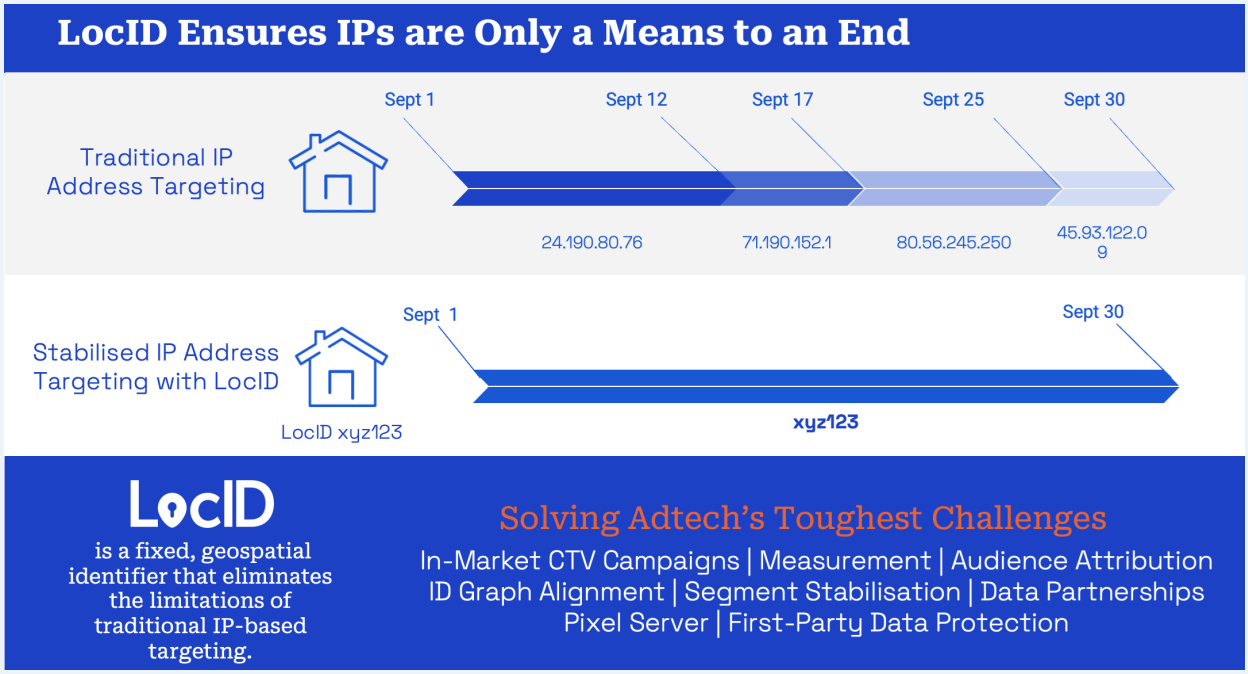
That stabilization becomes even more powerful when combined with device-level signals. With LocID Graph, device identifiers such as MAIDs are anchored to a stabilized household spine rather than allowed to float independently. By governing how those relationships persist over time, cross-device coherence can be maintained even as underlying network attributes shift.

This approach also extends beyond forward-looking activation. LocID Graph enables historical datasets to be reconciled against a consistent household framework, allowing audience segments to be recovered and revalidated instead of discarded. In an ecosystem where signals decay quickly, restoring continuity over time becomes a structural advantage.

CTV doesn't need more stitched-together device graphs. It needs architectural coherence — identity designed around the household context of television, with persistence built in from the start.

That's the lens behind LocID Graph: strengthening identity infrastructure by anchoring it to location. More broadly, the objective isn't about any single solution. It's about ensuring the identity foundation of converged TV is stable, privacy-conscious, and aligned with how people actually watch.

Figure 8: Stabilizing Identity with Location



Source: Digital Envoy

Governance and Ethical Considerations

However, proximity-enabled identity also raises new governance questions. Location signals are sensitive. Their derivation must be transparent, consent-grounded, and purpose-limited.

> ***Proximity between retail locations, service areas, and TV households is an incredibly powerful and predictive signal, but only when that proximity is derived from authenticated, privacy-conscious, stable identifiers such as postal address. Through these proximity associations, advertisers can better predict which households are most likely to convert in the real world and measure real performance.***
>
> *— Aleck Schleider, Chief Revenue Officer, Blockgraph*

Key governance considerations include:

- **Signal provenance:** How are location associations derived? From deterministic address data, modeled mobility data, or third-party enrichment?
- **Consent frameworks:** Are location inferences aligned with disclosed purposes?
- **Data minimization:** Is granular geolocation necessary, or can catchment-level aggregation suffice?
- **Bias mitigation:** Are neighborhood characteristics being used as proxies for demographic inference?

The last issue is particularly important. Geographic signals can inadvertently function as demographic proxies. Without guardrails, proximity targeting could reinforce structural inequities or produce discriminatory effects. A mature proximity-identity model must incorporate:

- Transparent linkage logic.
- Explicit suppression and policy controls.
- Bias review mechanisms.
- Documentation of modeling assumptions.

As identity infrastructure becomes more powerful, governance expectations intensify.

Proximity as Strategic Extension of Household Identity

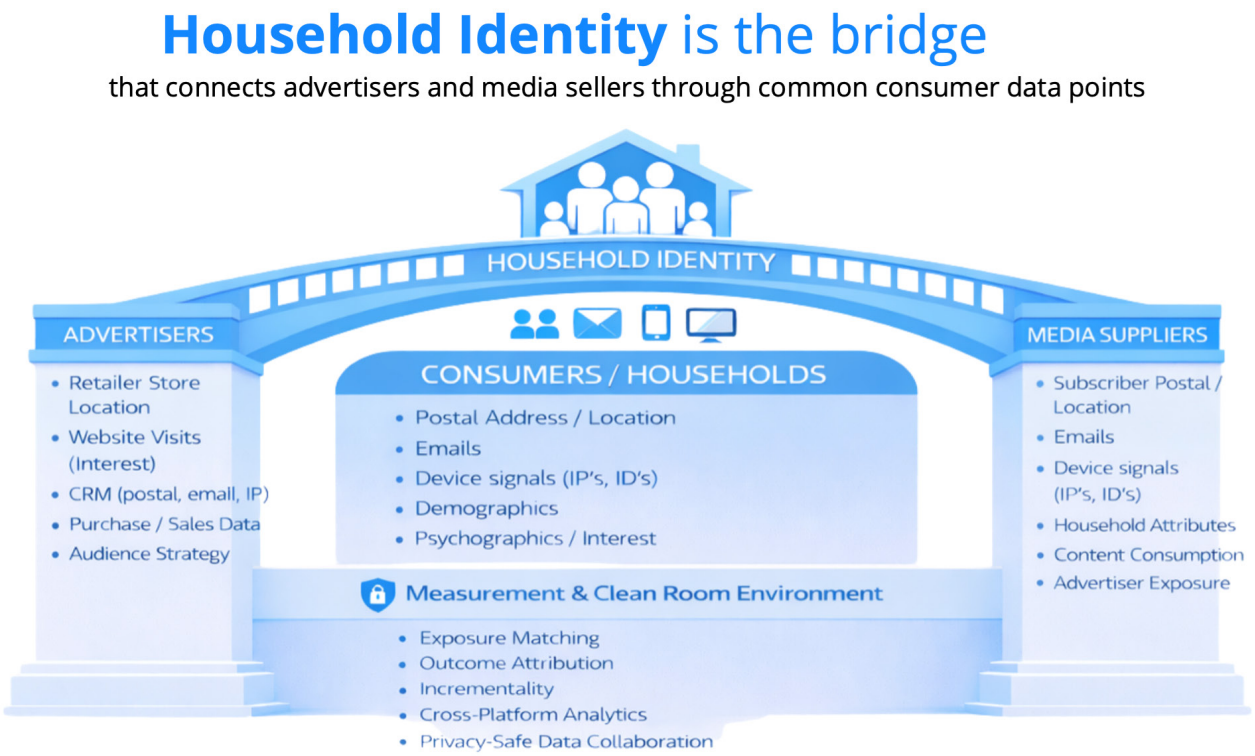
From an architectural perspective, proximity intelligence is not a separate system layered onto identity. It is an extension of the household spine.

The logic flows as follows:

1. Deterministic household identity anchors exposure.
2. Household geography connects exposure to physical context.
3. Proximity modeling aligns media with retail footprint.
4. Outcome data reconciles exposure to commerce.
5. Feedback loops inform optimization.

This integrated approach strengthens converged TV's competitive position relative to performance media channels. Proximity transforms TV from a broad awareness channel into a geographically contextualized performance instrument — without sacrificing premium inventory or privacy grounding.

Figure 9: Value of Household Identity



Source: Blockgraph

> ***Even as ecommerce grows, publishers need to ensure their advertiser solutions continue to evolve around a simple reality: most commerce still happens in the real world. Proximity intelligence allows TV advertising to reflect that reality by aligning media exposure with the households and retail footprints that shape purchasing behavior. When geographic context is anchored to authenticated households, campaigns can move beyond broad reach and toward locally relevant activation and accountable outcomes. Proximity is not a niche tactic; it is a structural capability that reconnects converged TV to real-world performance.***
>
> *— Aleck Schleider, Chief Revenue Officer, Blockgraph*

Chapter 8. Identity Meets Proximity: Bringing Real-World Context into TV

Strategic Implications

Identity Infrastructure 2.0 enables proximity to function responsibly and effectively. Without a stable household anchor:

- Location signals fragment.
- Exposure cannot be reconciled coherently.
- Measurement disputes proliferate.

Without governance guardrails:

- Privacy risks increase.
- Regulatory scrutiny intensifies.
- Trust erodes.

When identity and proximity are integrated within a privacy-by-design architecture:

- Local budgets can scale confidently.
- Outcome accountability strengthens.
- Cross-channel optimization improves.
- Retail media and TV converge strategically.

The expansion of CTV and local video budgets makes proximity not a niche capability, but a structural growth vector. In converged TV, identity does not merely resolve who was exposed. It increasingly resolves where exposure matters.

Chapter 9. The Agentic Era: Identity as AI Infrastructure

In the agentic era, AI systems will increasingly automate media optimization, personalization, and cross-channel orchestration. However, AI does not smooth over identity weaknesses. It magnifies them.

Automation systems ingest identity signals as foundational inputs. If identifiers do not align across channels, if records are incomplete, if household and person entities are conflated, or if linkage quality varies invisibly across environments, AI does not resolve those inconsistencies. It optimizes against them.

In practical terms:

- Fragmented identity leads to duplicated exposure and inefficient budget allocation.
- Misaligned entity hierarchies distort personalization logic.
- Inconsistent linkage undermines deduplicated reach modeling.
- Weak refresh cadence introduces measurement drift.
- Opaque provenance prevents meaningful model debugging.

Identity is becoming the substrate upon which AI agents operate. When the substrate is unstable, automation scales instability. When the substrate is coherent, automation scales coherence.

This reframes identity from an activation tool to a structural prerequisite for AI-enabled media ecosystems.

> ***AI doesn't solve identity fragility, it will only scale it. As optimization systems become autonomous, identity quality transforms from a performance variable into a structural prerequisite. When households are misidentified or linked incorrectly, AI agents don't correct these errors, they amplify them across every decision. The agentic era demands deterministic signals, transparent matching algorithms, and strong governance embedded into the identity infrastructure itself. Identity becomes the foundation upon which successful activation relies.***
>
> *— Sebastien Hernoux, Chief Client Solutions Officer, Annalect*

> ***In the agentic era, AI systems will increasingly automate media optimization. However, AI does not smooth over identity weaknesses; it magnifies them. Identity is the foundation upon which AI agents operate. When the foundation is unstable, automation scales instability. When it is coherent, automation scales coherence. This reframes identity from a simple tool to a structural prerequisite for the AI-enabled media ecosystem.***
>
> *— Erin Boelkans, VP Product, LiveRamp*

Chapter 9. The Agentic Era: Identity as AI Infrastructure

Identity as the Foundation of Autonomous Optimization

In traditional workflows, human planners reconciled identity inconsistencies manually. In agentic systems, optimization loops occur at machine speed.

AI-driven media orchestration depends on several identity-dependent capabilities:

- Cross-platform frequency management.
- Real-time suppression and eligibility logic.
- Household-to-person attribution.
- Outcome feedback loops.
- Sequential messaging strategies.
- Budget reallocation based on incremental performance.

Each of these requires persistent, consistent entity definitions.

If the same consumer appears as three separate records across platforms, AI agents cannot manage frequency accurately. If household definitions shift mid-campaign due to ungoverned refresh, performance models degrade. If exposure and outcome are resolved through different identity logic, attribution becomes unreliable.

Identity must be persistent, configurable, accurate, and consistent across environments to support the agentic future.

In this context, identity becomes AI infrastructure.

> ***AI-driven media orchestration requires consistent entity definitions to accurately manage cross-platform frequency or link exposures to outcomes. In the age of automation, identity isn't just data — it's the infrastructure that provides the ground truth AI requires to learn. AI increases the strategic value of deterministic identity by demanding a disciplined architecture as its foundation.***
>
> *— Erin Boelkans, VP Product, LiveRamp*

Chapter 9. The Agentic Era: Identity as AI Infrastructure

What AI-ready Identity Requires

An identity spine capable of supporting autonomous systems must meet higher standards than traditional activation workflows.

Five characteristics emerge as essential:

Persistence: Identifiers must remain stable over time to preserve measurement continuity. Longitudinal optimization and incrementality modeling require consistent entity references across campaign windows.

Consistency Across Environments: The same identity should resolve predictably across CTV, mobile, web, clean rooms, and analytics systems. Fragmented identity reduces automation effectiveness.

Configurability: AI systems operate across varied use cases — prospecting, retention, local activation, measurement validation. Identity resolution rules and confidence thresholds must be tunable by enterprise teams.

Completeness Across Touchpoints: AI orchestration depends on broad coverage. Gaps in household linkage or missing device associations reduce optimization accuracy.

Embedded Privacy Controls: AI systems must operate within consent and governance frameworks. Identity infrastructure must propagate opt-outs, enforce suppression logic, and maintain documented provenance.

In short, AI-ready identity is not a larger graph. It is a governed, persistent, configurable, privacy-aware spine.

The Counterpoint: can AI reduce Dependence on Direct IDs?

AI can also play another role, operating in low-ID or ID-less environments. Contextual targeting, cohort-based strategies, and probabilistic modeling allow campaigns to function without persistent identifiers. Advances in machine learning can identify content patterns correlated with high-performing cohorts.

However, these systems still require:

- High-quality training labels.
- Reliable feedback signals.
- Ground truth for model evaluation.
- Stable measurement anchors.

Without deterministic seeds, AI models risk drift and bias. Training sets built on unstable identity linkages propagate error. Feedback loops become noisy.

In addition, AI-driven systems operating in low-identifier environments may generate spurious correlations or unstable optimization signals when training data lacks durable identity grounding. Without robust validation anchors and feedback discipline, models can infer patterns that appear performance-enhancing in the short term but do not reflect causal audience relationships or real-world behavioral response. This increases the risk of decision drift, inefficient media allocation, and reduced measurement credibility over time.

Healthcare provided a clear illustration of this principle. Deterministic patient or provider cohorts serve as high-confidence training labels that allow contextual models to operate responsibly in ID-constrained environments.

The same pattern generalizes across verticals:

- Retail loyalty data trains lookalike models.
- Subscriber data anchors incremental lift modeling.
- Verified transaction cohorts refine contextual scoring.

Rather than eliminating the need for deterministic identity, AI increases its strategic value.

Deterministic anchors provide the labeled ground truth against which AI systems learn.

Identity as the Training Data Layer

This reframing positions identity not merely as an execution layer, but as a training data layer. AI systems depend on structured entity relationships to:

- Identify high-value cohorts.
- Detect correlated contextual signals.
- Optimize creative sequencing.
- Model lifetime value.
- Forecast incremental impact.

Identity Infrastructure 2.0 therefore supplies:

- High-confidence household anchors.
- Explicit person-device hierarchies.
- Transparent linkage scoring.
- Stable exposure-to-outcome mapping.

These components become the labeled scaffolding upon which AI agents operate. Without them, AI systems become sophisticated pattern detectors trained on unstable ground truth.

Chapter 9. The Agentic Era: Identity as AI Infrastructure

Strategic Implications

The convergence of identity and AI carries institutional consequences.

First, identity quality becomes a board-level issue. As automation scales, upstream weaknesses in identity resolution can propagate directly into financial outcomes, affecting pricing accuracy, media efficiency, and measurement credibility.

Second, governance requirements extend beyond post-hoc auditability to include meaningful human oversight. As AI systems increasingly support or automate planning, activation, and optimization decisions, enterprises must retain the ability to supervise identity assumptions, validate model behavior, and intervene where necessary. Human-in-the-loop frameworks help ensure that automated decision systems remain aligned with business objectives, regulatory expectations, and measurement integrity standards.

Third, explainability remains essential. When AI-assisted systems influence media investment decisions, organizations must be able to interpret the identity logic and signal quality underlying those outcomes in order to diagnose performance variance, manage risk, and maintain institutional trust.

Fourth, incentive alignment matters. If identity providers optimize for scale rather than fidelity, AI systems will amplify over-association errors.

Fifth, governance expectations rise. Privacy-by-design controls must be embedded within AI pipelines.

The “agentic era” is not a departure from identity infrastructure. It is a stress test for it.

Identity Infrastructure 2.0 positions deterministic household anchoring, multi-entity modeling, refresh discipline, provenance transparency, and configurable governance as prerequisites for AI-enabled media ecosystems.

Automation does not reduce the importance of identity. It increases it. In converged TV, identity is no longer merely a matching function. It is the connective tissue that allows AI agents to optimize responsibly, measure reliably, and personalize coherently. The agentic era does not eliminate identity complexity. It makes disciplined identity architecture indispensable.

Chapter 10. Signal Enrichment and Converged TV Measurement

Today, linear television remains large, effective, and under-integrated into programmatic workflows. Linear TV continues to represent a majority share of total US TV advertising spend, while daily viewing levels remain substantial. In absolute impression terms, linear often exceeds CTV due to higher ad loads and consistent reach. Yet programmatic buying remains disproportionately skewed toward CTV environments.

The structural reason is not lack of automation capability. Dynamic ad insertion (DAI) exists. Distribution infrastructure exists. Demand exists. What is missing is interoperable identity.

Standard demand-side platforms (DSPs) require readable, standardized identifiers in the bid request to:

- Target audiences.
- Suppress ineligible households.
- Manage frequency.
- Reconcile measurement.
- Optimize based on outcomes.

Linear ad delivery environments typically do not expose such identifiers in demand-side readable form. Even when proprietary set-top box IDs exist, they are not interoperable within OpenRTB workflows. The result is structural invisibility.

Linear supply may be technically addressable, but without identity enrichment it cannot participate fully in programmatic ecosystems. Signal enrichment addresses this gap.

Enriching Linear: Translating Proprietary Signals into Interoperable Identity

Signal enrichment functions as a translation layer between proprietary distribution identifiers and interoperable demand-side signals.

In simplified terms:

1. A distributor or MVPD possesses proprietary subscriber or set-top box identifiers.
2. Those identifiers are resolved within a secure identity network.
3. A universal household signal is derived.
4. The enriched identifier is attached to the bid request.
5. The bid request flows in standard OpenRTB format to DSPs.

The critical innovation is not the presence of identity per se. It is the format compatibility.

By enriching linear impressions with standardized household signals, the supply “looks like” addressable CTV to the buy side. DSPs do not need to modify core architecture. Agencies do not need to retool frequency management logic. Measurement systems can operate using existing identity frameworks.

Institutionally, this reduces coordination burden. Rather than requiring every buyer and platform to integrate proprietary identifiers, enrichment centralizes translation. It creates interoperability without forcing systemic overhaul.

From a market-structure perspective, this is significant. Linear inventory can become programmatically accessible without destabilizing buy-side infrastructure. Converged TV becomes operationally feasible.

These developments do not imply the emergence of a single standardized household identifier owned or administered by one market participant. In practice, household definitions are likely to remain distributed across multiple stakeholders — including distributors, publishers, identity providers, and measurement frameworks — each operating within their own contractual data rights and governance obligations. The institutional challenge is therefore less about

central ownership and more about establishing interoperable standards, transparent entity definitions, and clear rules for data collaboration and access. Industry bodies, standards initiatives, bilateral agreements, and privacy-safe clean room architectures are likely to play a coordinating role in enabling enriched identity signals to function consistently across trading environments while preserving competition and data stewardship responsibilities.

FAST: Correcting Signal Instability in Open Environments

FAST (Free Ad-Supported Streaming Television) environments present a related but distinct challenge. FAST supply often includes IP addresses within ad requests. However:

- Authentication may be weak or absent.
- Password sharing degrades login fidelity.
- IP signals may rotate or be reassigned.
- Device-level identifiers may be unavailable.

As noted above, IP-only linkages can be unstable without deterministic grounding. Signal enrichment in FAST environments addresses this instability by:

- Resolving IP signals against deterministic ISP-level or subscriber-level data.
- Validating household associations.
- Reducing over-association.
- Standardizing household representation.

In effect, enrichment converts an unverified signal into a verified household anchor.

This has measurable implications:

- Targeting precision improves.
- Frequency management stabilizes.
- Deduplicated reach modeling strengthens.
- Measurement reconciliation disputes decline.

FAST environments, which often lack consistent login infrastructure, particularly benefit from deterministic enrichment layers. Without enrichment, FAST supply risks operating on degraded or ambiguous identity signals. With enrichment, it can participate in converged measurement frameworks.

Chapter 10. Signal Enrichment and Converged TV Measurement

Identity as Measurement Infrastructure

Signal enrichment does more than unlock activation. It strengthens converged measurement.

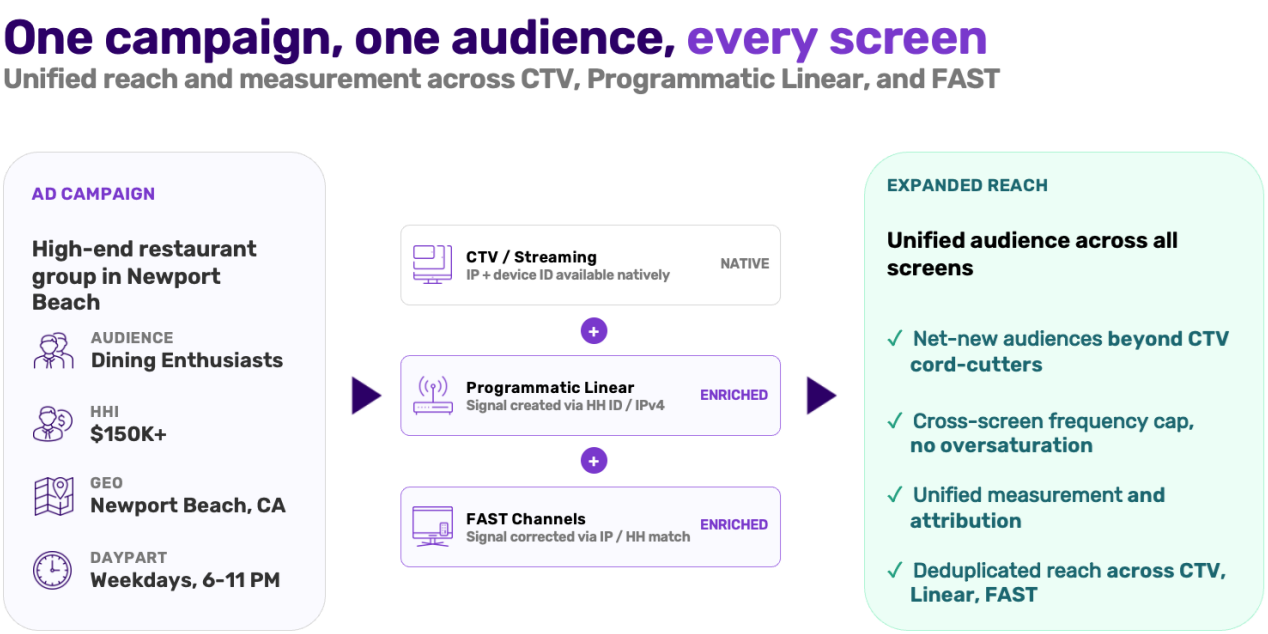
When linear and FAST supply are enriched with interoperable household signals:

- Cross-platform de-duplication becomes feasible.
- Exposure-to-outcome reconciliation operates on a shared spine.
- Incrementality modeling spans linear and CTV.
- Frequency capping can operate across environments.

The same identity layer that governs activation governs measurement. This alignment reduces systemic drift between buy-side and sell-side methodologies. It also mitigates the risk of divergent identity logic across platforms.

Signal enrichment therefore functions as infrastructure, not merely an enhancement. It closes the identity gap between linear, CTV, and FAST, enabling converged TV measurement architectures to operate coherently.

Figure 10: Signal Enrichment Impact on Measurement



Source: FreeWheel

Privacy and Governance in Enrichment Architectures

Signal enrichment, however, carries governance implications. Enrichment must operate within privacy-by-design boundaries.

Key architectural safeguards include:

- **Consent-grounded operation:** Resolution occurs within authenticated subscriber or service relationships.
- **Server-side processing:** Raw deterministic identifiers are not distributed broadly.
- **Server-side processing:** Raw deterministic identifiers are not distributed broadly.
- **Configurable controls:** Publishers and enterprises control which signals are activated.
- **Auditability:** Linkage logic, refresh cadence, and provenance are documented.

These safeguards are essential for institutional legitimacy. Enrichment cannot be perceived as a backdoor data leak. It must operate transparently and defensibly within existing governance frameworks. When enrichment layers adhere to these principles, they expand interoperability without expanding privacy risk.

Strategic Implications for Converged TV

Signal enrichment reveals a broader structural shift. Converged TV does not require the wholesale reinvention of programmatic infrastructure. It requires the normalization of identity signals across supply environments.

Linear supply contains scale.

FAST supply contains growth.

CTV supply contains automation.

Identity enrichment binds them together.

The strategic implications are clear:

- Linear inventory can be integrated into demand-side workflows without systemic disruption.
- FAST environments can correct signal instability and improve accountability.
- Measurement systems can operate on unified household spines.
- Privacy-by-design architectures can coexist with interoperability.

Signal enrichment transforms supply fragmentation into interoperable opportunity.In converged TV, identity is not merely about who saw an ad. It is about making structurally different supply environments legible to shared activation and measurement systems.

Chapter 11. Institutional Roadmap: How the Market Could Stabilize

Identity in US TV and CTV has entered a new institutional phase. What began as a collection of vendor-level matching solutions is evolving into market infrastructure. The question is no longer whether identity matters, but how the ecosystem can stabilize around durable architectural principles.

The path forward is unlikely to be defined by a single dominant provider or a universal ID spine. The TV ecosystem is structurally plural: distributors, publishers, platforms, agencies, advertisers, and data providers operate under distinct incentives, governance constraints, and technical architectures. The more realistic outcome is convergence around interoperability, not uniformity.

Identity Infrastructure 2.0 is therefore less about consolidation around one graph and more about shared expectations regarding how identity systems behave.

Standards Without Uniformity

Clearly, the market is unlikely to consolidate around a single universal identity solution. Too many stakeholders possess legitimate first-party anchors — subscriber relationships, CRM databases, authenticated app environments, retail loyalty frameworks — for uniformity to be feasible or desirable.

Instead, the market will be characterized standards without uniformity. Under this model:

- Multiple identity spines coexist.
- Deterministic anchors remain locally governed.
- Translation layers enable interoperability.
- Metadata standards describe linkage strength, refresh cadence, and provenance.
- Privacy controls are consistently enforced across environments.

Uniformity is replaced by shared rulebooks. This approach mirrors other mature infrastructure markets. Financial clearing systems, telecommunications interconnects, and internet protocols do not require a single operator. They require shared standards governing how systems communicate.

For identity in converged TV, those shared expectations may include:

- Defined entity hierarchies (household, person, device, account).
- Standardized signal-strength descriptors.
- Transparent refresh documentation.
- Privacy-by-design controls.
- Open interfaces for translation across spines.
- Standardized definitions of key identity and measurement concepts, ensuring that terms such as “household,” “reach,” “frequency,” “exposure,” and “match quality” are used consistently across platforms, identity providers, and measurement frameworks.

Clear semantic alignment reduces the risk that stakeholders interpret identity constructs differently for activation, reporting, or trading purposes. In complex converged environments, shared definitions function as institutional guardrails, supporting comparability of outcomes and reducing the likelihood of disputes driven by inconsistent terminology rather than substantive performance differences.

Chapter 11. Institutional Roadmap: How the Market Could Stabilize

Validation and Audit as Market Institutions

Measurement markets mature when validation institutions emerge. Identity has reached a stage where third-party validation and audit mechanisms become essential. As identity underpins cross-platform measurement, outcome attribution, and AI-driven optimization, stakeholders require confidence in linkage integrity.

Institutional stabilization likely requires:

- Independent validation of linkage strength.
- Standardized disclosure of identity quality metrics.
- Transparent refresh cadence reporting.
- Defined dispute resolution frameworks when measurement results diverge.

A practical near-term development could be the adoption of common identity quality scorecards — referenced in contracting, RFPs, and campaign reconciliation. Such scorecards would not mandate a single provider but would establish minimum expectations for signal quality and documentation.

This mirrors historical patterns in measurement markets: credibility improves when audit processes become normalized and when methodological disclosure becomes standard practice. Identity is approaching this inflection point.

Consolidation or Federation?

Looking forward, there are two plausible structural futures for the identity ecosystem.

One path is consolidation. As buyers seek simplicity and scale, larger identity providers could absorb smaller competitors, reducing fragmentation and streamlining integration.

The alternative path is federation. In a federated model:

- Multiple identity networks coexist.
- Interoperable plumbing enables transactions across them.
- Translation layers reduce switching costs.
- Governance standards mitigate lock-in.

Federation depends on neutral infrastructure layers — clean rooms, standardized APIs, shared metadata protocols — that allow identity diversity without systemic incompatibility. The direction of travel will depend on governance maturity.

If interoperability standards and audit frameworks solidify, federation becomes viable. If switching costs remain high and metadata standards remain opaque, consolidation pressure may intensify. Either path can produce stability. The difference lies in how incentives are aligned and how open the infrastructure remains.

Aligning Incentives Around Fidelity

Historically, identity monetization often emphasized match rate and coverage volume. As the Truthset findings and healthcare examples demonstrate, scale without fidelity undermines measurement credibility.

Institutional stabilization requires partial incentive realignment:

- Identity providers must differentiate on quality, not merely scale.
- Buyers must reward transparency and validation.
- Publishers must align enrichment architectures with privacy durability.
- AI-driven optimization systems must be calibrated against deterministic anchors.

Identity Infrastructure 2.0 implies that fidelity, provenance, and governance become competitive variables — not compliance afterthoughts. When incentives reward fidelity, infrastructure stabilizes.

Chapter 12: Identity Infrastructure 2.0 as the Foundation of Converged TV

Identity is being rebuilt as infrastructure:

Deterministic-first where possible.

Transparent where necessary.

Configurable by design.

Configurable by design.

Signal enrichment approaches offer a credible pathway to unlock linear and stabilize FAST — supply pools previously invisible or unreliable within programmatic workflows. Deterministic anchoring improves measurement credibility. Composability reduces operational friction. Governance architectures embed trust into system design.

Simultaneously, the agentic-era framing underscores that identity weakness will become more consequential as automation accelerates. AI systems amplify both coherence and fragmentation.

Identity Infrastructure 2.0 is therefore not about solving a single matching problem. It is about building durable institutional foundations:

- Incentives aligned to fidelity.
- Governance embedded into architecture.
- Standards enabling interoperability without forcing uniformity.
- Validation mechanisms that sustain trust.
- Multi-entity models that reflect real-world complexity.

Converged TV cannot function sustainably without identity infrastructure that is measurable, governable, and interoperable. Identity Infrastructure 2.0 does not resolve every structural tension in the TV ecosystem. It does, however, provide a coherent architectural framework for reconciling scale with fidelity, automation with accountability, and innovation with governance. Converged TV measurement, pricing integrity, and AI-enabled optimization will depend less on any single identity provider and more on whether the market can institutionalize shared standards for transparency, validation, and interoperability.

Appendix A: Practical Questions for Executives

These questions are intended as a strategic diagnostic tool for senior leaders responsible for media investment, data governance, measurement, and technology infrastructure. They are not technical implementation checklists. Rather, they are board-level prompts designed to surface structural risk, governance gaps, and competitive opportunity within an organization's identity architecture.

Executives should use them to assess whether identity is operating as durable infrastructure or as a collection of vendor-level tactics and to evaluate readiness for converged TV, cross-platform measurement, privacy-by-design governance, and AI-enabled optimization.

Used collectively, these questions help identify where identity fragility may be constraining growth, measurement credibility, operational efficiency, or long-term strategic resilience.

- How resilient is our identity spine across platforms, devices, and time?
- Can we trace provenance of each linkage and differentiate signal strength?
- Do we control scale vs precision thresholds by use case?
- Can we run identity in our environment (or via interoperable clean rooms) with auditable governance?
- How do we validate — independently — identity quality and measurement agreement?
- Where are the biggest identity gaps in our supply: linear, FAST, authenticated CTV, or partner ecosystems?
- How will IPv6 adoption and network architecture changes affect our reliance on IPv4 signals?

Appendix B: Quantitative Scenarios and Sensitivity Frameworks

Identity Infrastructure 2.0 shifts identity from a marginal optimization to a capital allocation variable.

This appendix translates various qualitative claims about identity into a set of illustrative quantitative scenarios. These models are not forecasts and should not be interpreted as market projections. The objective is to clarify order of magnitude benefits, directional sensitivities, and potential trade-offs under different identity architecture assumptions.

None of these models predict specific outcomes, but the analysis does illustrate some important conclusions:

1. Addressable linear expansion represents multi-billion-dollar measurable supply unlock.
2. Deterministic-first resolution reduces measurement noise nonlinearly.
3. Identity enrichment stabilizes FAST and improves pricing power.
4. Composability materially reduces operational friction.
5. Identity errors compound multiplicatively across entity layers.

Anchor figures referenced below (e.g. linear TV spend share, FAST growth context, IP accuracy benchmarks) come from referenced sources. All additional calculations are explicitly assumption-driven.

Scenario 1. Linear TV Addressability Expansion

Baseline Assumptions

- Total US TV ad spend ≈ $85B.
- Linear TV share ≈ $52B.
- Current demand-side addressable linear share c.3%.
- 3-year adoption horizon for enrichment deployment.

Current addressable linear inventory: $52B * 3% = $1.56B. This inventory is presently interoperable within standard demand-side workflows.

Scenario Framework

We model three illustrative adoption scenarios, with increment vs. today calculated as: $52B * (New\ Share - 3%). These scenarios illustrate measurable inventory eligibility but do not assume automatic spend reallocation.

Scenario	Addressable Share	Incremental Share	Addressable Inventory	Increment vs. Today
Conservative	10%	+7pp	$5.2B	+$3.64B
Base	20%	+17pp	$10.4B	+$8.84B
Ambitious	35%	+32pp	$18.2B	+$16.64B

Appendix B: Quantitative Scenarios and Sensitivity Frameworks

Interpretation

Even modest increases in interoperable identity penetration unlock multi-billion-dollar measurable inventory pools.

Important sensitivities:

- Deterministic enrichment coverage footprint.
- Buy-side adoption rates.
- Governance and privacy acceptance.
- Standardization across supply.

Scenario 2. Measurement Noise Under Inference-Based Identity

Baseline Accuracy Contrast

From the CIMM / Truthset IP study:

- Inference-based IP-to-household accuracy c.13% average.
- Low cross-provider agreement.
- Deterministic ISP benchmarks used as ground truth comparator.

Attribution Noise Simulation

Assume:

- Campaign delivers 10M impressions.
- Attribution depends on IP-to-household mapping.
- Under 13% inference accuracy:

  10M * 13% = 1.3M correct mappings.

  8.7M\ potentially\ misattributed.

Misattribution rate: 87%.

Even if partial correlation exists, structural error dominates signal.

Impact on Reach and Frequency

Assume:

- 2 impressions per household on average.
- 13% mapping accuracy.

Estimated unique household reach under inference resolution will be inflated due to duplicate and incorrect associations.

If actual unique households = 5M:

Under 87% noise, effective deduplicated reach may diverge significantly from true exposure.

Measurement drift increases nonlinearly as accuracy declines.

Appendix B: Quantitative Scenarios and Sensitivity Frameworks

Sensitivity Curve (Illustrative)

If mapping accuracy improves:

Accuracy	Correctly Attributed Impressions	Error Rate
13%	1.3M	87%
30%	3.0M	70%
60%	6.0M	40%
90%	9.0M	10%

Noise reduction is nonlinear in downstream modeling impact.

Scenario 3: FAST Identity Stabilization Model

Structural Paradox

FAST environments exhibit:

- High growth in ad-supported view volume.
- Weak authentication in many cases.
- IP-based household proxy reliance.

Resolution Scenarios

Assume:

- 1B FAST impressions delivered.
- Current deterministic resolution rate: 20%.
- Enriched resolution target: 60%.

Current verified impressions: 1B * 20% = 200M.

Post-enrichment: 1B * 60% = 600M.

Incremental verified supply: +400M\ impressions.

Pricing sensitivity (illustrative).

Assume CPM differential:

- Unverified FAST CPM: $20.
- Verified FAST CPM: $24 (20% premium due to measurement confidence).

Incremental revenue potential: 400M ÷ 1000 * (24 - 20) = $1.6M.

At scale, pricing uplift compounds significantly across large impression volumes.

Appendix B: Quantitative Scenarios and Sensitivity Frameworks

Scenario 4: Compounding Error Modeling Across Identity Layers

Identity errors cascade across entity hierarchies: Device → Person → Household → Attribute.

Assume:

- Device-to-person accuracy: 80%.
- Person-to-household accuracy: 70%.
- Household-to-demographic accuracy: 75%.

Effective end-to-end accuracy: 0.8 * 0.7 * 0.75 = 0.42 = 42%.

Even moderate per-layer accuracy produces material compounding degradation.

Deterministic anchoring at the household layer reduces multiplicative error risk.

Scenario 5: Operational Efficiency and the "Ad Tech Tax"

Integration Complexity Model

Assume enterprise:

- 5 identity partners.
- 10 activation destinations.
- Separate data feeds per partner.

Without composability: 5 * 10 = 50 integration paths.

With centralized identity layer: 1 * 10 = 10 integration paths.

Reduction: 80% decrease in integration complexity.

Activation Latency Model

Assume:

- Average onboarding cycle per partner: 30 days.
- Parallel onboarding across 5 partners: 150 total operational days.

Composable deployment reduces onboarding to: Single integration cycle: 30 days.

Time-to-market improvement: 80% faster activation.

Appendix C: Sources and References

CIMM Showcase Presentations

CIMM Showcase: Innovations in Identity Resolution. February 18, 2026.

Johnson, A. (2026). *Rethinking Identity: Empowering Researchers Through Transparency*. Adstra.

Kozub, S. (2026). *Healthcare Advertising*. Experian Marketing Services.

Schleider, A. (2026). *Identity Meets Proximity: The Opportunity Ahead*. Blockgraph.

Boelkens, E. (2026). *The Evolution of Identity in the Agentic Era*. LiveRamp.

Johnson, C. (2026). *Taking Identity Back Home: Why CTV Needs IP-Based Identity*. Digital Envoy (LocID).

Shepard, M. (2026). *Closing TV's Identity Gaps: How Signal Enrichment is Making Every Screen Addressable*. FreeWheel (Comcast).

CIMM Research Studies Referenced

CIMM / Truthset. (2023). *Household Identity Accuracy Project*.

CIMM / Go Addressable / Truthset. (2025). *IP Address Accuracy Study*.

Industry Research and Market Data Referenced in Presentations

EMARKETER. (2025). *Digital Video Forecast and Trends, Q3 2025*.

EMARKETER. (2025). *US TV Ad Spending Forecasts (2025-2029)*.

EMARKETER. (2025). *TV Ads Are the Most Acceptable Place for Advertising* (December 23, 2025).

EMARKETER. (2025). *Linear Programmatic Advertising Moves Toward Automation* (October 31, 2025).

IAB. (2025). *Digital Video Ad Spend & Strategy Full Report*.

Statista. (2025). *FAST Ad Revenue in the United States*.

FreeWheel. (2025). *Internal Data, January-June 2025*.

FreeWheel / Dynata. (2025). *Consumer Survey on FAST Viewing Behavior, July 2025*.

Comcast. (2024). *Aggregated Viewership and Ad Exposure Data, 10,000+ Campaigns, January-December 2024*.

Appendix D: About the Contributors

Blockgraph

Blockgraph enables accurate, accountable TV advertising by turning first-party data and local context into precise household audiences and measuring real outcomes. The platform supports advertisers, agencies, and media partners in planning, activating, and evaluating campaigns around real households and real neighborhoods.

By unifying audience targeting, proximity intelligence, and measurement within one platform anchored to a shared household foundation, Blockgraph connects media exposure to the physical communities where purchasing decisions are made. Advertisers can onboard customer data, define geographic zones around retail presence, and align campaigns to real-world distribution footprints with confidence that activation and reporting operate on the same structural reference layer.

The result is advertising that is more precise in who it reaches, more locally grounded in where it runs, and more accountable in what it drives beyond the screen. Blockgraph brings clarity and cohesion to converged TV, helping businesses translate data into action and media into measurable business impact.

DISH Media

DISH Media provides advertisers with intelligent solutions to efficiently maximize exposure to desired audiences across DISH TV and Sling TV while safeguarding consumer personal information. Through innovative platforms like addressable targeting and programmatic buying, viewer measurement tools and access to custom audiences on DISH TV and Sling TV, advertisers employ data-driven, demographically targeted buys that enhance their national media campaigns. DISH Media is an indirect subsidiary of EchoStar Corporation (NASDAQ: SATS).

Visit media.dish.com.

LiveRamp

LiveRamp is the data collaboration platform of choice for the world's most innovative companies, helping brands, publishers, and platforms connect data safely and effectively in a privacy-first world. With more than 20 years of innovation in identity, LiveRamp powers one of the industry's most robust and interoperable identity graphs — enabling organizations to unify fragmented customer data into durable, actionable profiles.

At the core of LiveRamp's offering is RampID — a persistent, people-based identifier that allows marketers to connect signals across devices, channels, and partners without relying on third-party cookies. This foundation enables accurate measurement, improved targeting, and seamless activation across the digital ecosystem. By resolving identity at scale and embedding privacy protections into every workflow, LiveRamp empowers companies to collaborate with confidence while maintaining consumer trust.

As identity signals continue to evolve, and consumers embrace new AI-driven experiences, LiveRamp remains focused on delivering connectivity, interoperability, and measurable outcomes across our vast data collaboration network — helping organizations drive more relevant experiences, optimize performance, and maximize the value of their data assets at a global scale.

LiveRamp is headquartered in San Francisco, California, with offices worldwide. Learn more at LiveRamp.com.

Appendix D: About the Contributors

LocID

LocID is a CTV-focused identity solution designed to address one of the core structural challenges in converged TV: IP volatility. While IP naturally connects devices within a home network, it is inherently dynamic. ISP reassignment, router resets, and network changes can disrupt persistence and fragment addressability over time.

LocID stabilizes IP-derived signals to create a durable, privacy-forward household identifier purpose-built for CTV. By maintaining continuity even as underlying IP attributes change, LocID helps reduce re-fragmentation across campaign windows and improves cross-screen reach and frequency management.

Built with privacy-by-design principles, LocID avoids exposing raw IP data while enabling interoperable household identity across CTV, FAST, and linear environments. The result is a more stable foundation for targeting, signal enrichment, and converged measurement — aligned with how television is actually consumed at the household level.

Learn more at: https://www.locid.com

Omnicom Media

Omnicom Media, an Omnicom (NYSE: OMC) Connected Capability, is the world's largest global media management network. Powered by the Omni Intelligence Platform, Omnicom Media agencies leverage $73.5 billion in billings, 40,000+ specialists across 70+ markets, and the industry's most powerful portfolio of Identity (Acxiom RealID™), Commerce (Flywheel), and Intelligence (Q™) assets to design dynamic Growth Ecosystems that enable the world's most ambitious businesses to grow faster and smarter. The Omnicom Media portfolio includes leading global media agency brands OMD, Initiative, PHD, UM, Hearts & Science, and Mediahub; Data, Identity & Analytics powerhouses Acxiom and Annalect; and a broad spectrum of specialized services.

For more information visit omnicommedia.com


cimm
Coalition for Innovative
Media Measurement
ARF