Privacy and the Future of TV Advertising

Planning, Activation and Measurement in the Privacy-Forward Era

cimm coalition for innovative media measurement

Think Medium

SHULLMAN ADVISORY

A's

Executive Summary

Privacy regulations and platform policies are creating significant uncertainties for the advertising industry and its data practices. With the rise of connected TV (CTV) alongside broadcast/linear, planning, activation, and measurement solutions have been iterating for a number of years, and privacy changes are only adding to the state of flux. To date, TV companies have mostly viewed privacy through the lens of compliance, while regulatory and platform shifts are now creating an imperative to think and act strategically about their solutions portfolio.

When considering the optimal, privacy-forward approach to TV advertising, we recommend the following structure and provocations:

1. **The move towards privacy is about people.**

   The advertising ecosystem depends on a fair value exchange between people (consumers) and businesses, and regulators, consumers, and their advocates are demanding privacy rights and protections as a part of that exchange. Individual US states and platforms controlling devices and operating systems have been developing privacy-motivated policies, and their impact creates another layer of complexity.

   Our perspective: Unless a more complex approach is justified by revenue, strategy, or your business model, do not get distracted by the details of state-by-state legislation. Create an approach that meets the highest bar required for compliance and build towards that across your practices and solutions.

2. **Channels and formats matter.**

   Legacy TV planning/activation and measurement solutions are relatively resilient to privacy concerns, as they generally rely less on people-based signals.

   Our perspective: Long-form video is a more established, standardized media format and has corresponding advertising solutions with resilient foundations. However, cross-media advertising will require newer techniques if more granular planning/activation and measurement are desired.

3. **Measurement lags planning and activation.**

   You have to be able to measure what you do, and planning and activation (especially targeting) solutions are at greater risk of disruption by privacy as a whole because existing solutions rely heavily on identity and access to and deployment of 1:1 person-level data across technology layers and consumer touchpoints.

   Our perspective: Prioritize addressing planning disruption over changing measurement practices today, and get comfortable using less data in general. Measurement will adapt based on activation strategies, as registering delivery and proof of performance is paramount.

4. **Establish/Refine your foundation.**

   Platform policies impact 1:1 person-level and device-level signals faster than regulations, and some use cases are more affected by signal loss and data collection than others. Established solutions will be increasingly impacted by platform policies over the long term, as well.

   Our perspective: To support baseline capabilities, select one or more established solutions that are less dependent on nascent technologies or techniques and have corresponding standards, as they will generally be durable and have industry support to flex with ongoing shifts.

5. **Innovate with emerging solutions.**

   Certain CTV use cases cannot be served by established solutions alone and require newer tools. However, emerging solutions have more nuanced privacy considerations given the use cases they support and the data they require – especially while corresponding regulatory and industry consensus is still forming.

   Our perspective: Test and learn with new solutions. Consider ease of implementation, fragmentation or interoperability, and the ability to scale with more or less granular data. Priority of investment depends on the scale of the participants and data you are measuring, as well as signals of emerging standards. Adopting privacy-enhancing technologies as enablers will be advantageous over time.

This report defines four frameworks – **Stakeholders, Use Cases, Privacy,** and **Solutions** – that are the building blocks of a **Solutions Heatmap** to provide insights into the solutions and technologies that are likely to be more or less useful and durable in the face of privacy-related regulatory and platform changes. The report was developed with input from ThinkMedium, Shullman Advisory, CIMM, 4A's, industry leaders, and legal experts.

Solution	Use Case(s)	Utility (Planning/Activation &/or Measurement)	Privacy Durability		Efficiency (Deployment & Operation)	Industry Adoption	Overall Viability
			Regulatory Scrutiny Risk	Platform Policy Risk			
Solution A	*Multi-Use*						

Solutions Framework

Privacy Framework

Use Case Framework

Stakeholder Framework → Action Plans

We encourage you to think about this structured approach through the lens of your own organization's strategy and the *tradeoffs you are willing to make between utility and privacy risk* in the medium to long term. The Solutions Heatmap within this report provides a way for you to assess the relative ease of adoption and durability of each solution, and for you to then apply your own filter of relative value to determine suitability for your business needs.

> *As an industry, we need to see the call for privacy as an opportunity to empower the conscious sharing of data, which ultimately builds consumer trust and allows us to provide a more accurate representation of viewership in a privacy-respectful way.*
>
> **– Joshua Chasin, Chief Measurability Officer, Videoamp**

Table of Contents

Introduction

Television – premium, professionally-produced, long-form video – is undergoing its most significant upheaval since the rise of cable TV and VCRs. The market has fragmented across devices and channels with notable shifts toward connected TV (CTV), mobile, and on-demand streaming. No longer is *traditional linear TV* – programming on a predetermined schedule and channel – the only or even primary TV-based option for advertisers. Now, *Advanced TV (CTV and Addressable TV)* is capitalizing on the same data-enabled technologies and practices that have propelled digital to offer fine-grained targeting and measurement options for advertisers, a feat inconceivable for TV even a decade ago. These shifts have made more content available to a wider range of consumers and advertisers, with the cost of further complicating TV planning, activation, and measurement, and bifurcating it across linear and digital channels.

> *Fragmentation means you need to be able to operate in different environments so standardization across the board is critical not only in how you transact or measure, but even in what data looks like when it's delivered*
>
> **–Yee Pang, Group Director, Research & Measurement, Group M**

Just as TV has become addressable and more measurable, increasingly complex privacy regulations and platform (device and operating system) policies have arisen. Questions about how the ad ecosystem has accessed, shared, and used consumer data motivated these changes and only continue to gain momentum. Consumers and advocates are demanding the TV and advertising ecosystem prioritize efforts to protect individuals – and savvy advertisers and publishers are realizing they should also protect their own data in the process.

Altogether these forces are disrupting established and even emerging TV practices. It is not obvious how to understand and navigate new regulations and policies, especially as new ones continue to be introduced.

It is impossible to embrace and optimize between existing and expanded TV opportunities without a solid understanding of where the industry is headed in terms of privacy and a robust foundation of privacy-forward practices in place. This means privacy needs to be a top business priority. Resistance and piecemeal responses will not suffice.

> *You can't band-aid your way into the future*
>
> **– Jesse Redniss, CEO, Qonsent**

Instead, a privacy-forward mindset must be adopted for all strategies and decisions moving forward. The first step to achieving privacy-by-design is to internalize the fact that the underlying motivation is about people.

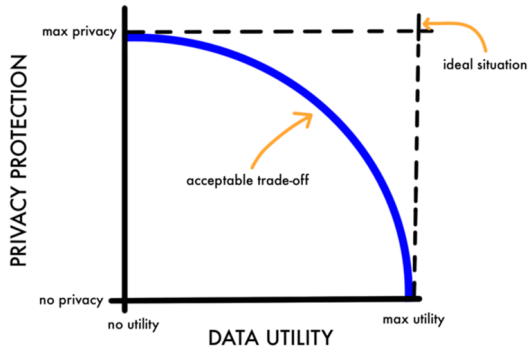
Privacy Can Be Good for People *and* Good for Business

The TV ecosystem is largely powered by advertising spend, which is in turn reliant upon a meaningful value exchange between consumers and businesses. Even when not obvious, consumers derive many benefits from TV advertising, including free content, discounts, and the discovery of new products. Ultimately, however, business success depends upon meeting consumers' needs and it is clear consumer *privacy* is a central component of the digital (including TV) advertising value exchange. Therefore, taking action around privacy may be one of the most important and consequential opportunities one can take to meet the needs of customers and secure the future of one's business.

> *To be proactive on privacy, [ecosystem constituents] need to get ahead of policy & regulations and align with consumers*
>
> **– Claudio Marcus, Independent Industry Expert**

Balancing Privacy and Utility

Ideally, the advertising and media ecosystem would already fully employ strategies that protect consumer *privacy* and enable advertising planning and measurement use cases *(utility)*. In reality, the privacy and utility of many existing solutions are at odds because the very practices that drive business value, such as the usage of person-level data, can inherently infringe on consumer privacy. In order to evaluate and implement privacy-forward solutions for planning and measurement, it is helpful to consider if and how each potential solution strikes a "balance" between privacy and utility.



Finding the right balance means understanding the tradeoffs and risks of how much your business prioritizes one element compared to the other and determining an optimal point (see Figure)[1].

Each business differs in needs, privacy requirements, risk profile, and appetite for risk, so the target balance, and thus the set of viable privacy-forward advertising solutions, will not be the same for all players and all use cases – and may vary over time for a given business.

Without a doubt, enabling privacy long-term requires active participation and collaboration from the entire TV ecosystem. But, privacy changes are happening *now* and are already having real implications for businesses *today*. Likewise, organizations have their own ideal privacy-utility balance and unique existing business practices, capabilities, and constraints.

So what exactly can you do to get ahead of uncertainty and do right by your business *and* your customers?

> *Partners can't do all the work for you, you also need to look inward and ensure your own business practices are up to the same standard.*
>
> **– Delphine Fabre-Hernoux, Chief Data & Analytics Officer, GroupM**

Report Overview

Your business will need to adopt a robust catalog of privacy-forward solutions, strategies, and practices, which requires reevaluating current approaches and committing to taking action based on findings. This report provides guidance for executing this process and was created in partnership with CIMM, 4A's, ThinkMedium, Shullman Advisory, and direct engagement with other industry leaders (see Appendix for the full project steering group). Interviews, input from experts, and secondary research were used to develop and calibrate each element of the frameworks and heatmap provided.

This process starts with understanding the TV advertising ecosystem and the intricate web of stakeholders, use cases, and privacy considerations. This view is needed to assess each existing or new solution that your business (may) use for durability against existing privacy laws and policies.

> *You need to ensure your investments are privacy durable*
>
> **– John Chen, Director of Product Management, Google**

[1] Practical Implications of Sharing Data: A Primer on Data Privacy, Anonymization, and De-Identification – Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Data-Privacy-Protection-versus-Data-Utility_fig5_318866074

With a list of current solutions in hand, the (self-determined) utility your business derives from each can be compared to determine the privacy-utility tradeoff for that solution. Based on these investigations, decide which practices are durable and valuable enough to continue leveraging as-is and which must be adapted or phased out; this will determine your next steps. Once privacy-forward planning and measurement strategies are in place, innovate with emerging solutions and technologies as necessary. Continue to reassess your portfolio as new policies and opportunities emerge.

The report culminates in an evaluative **Solutions Heat Map** that provides insights into the durability of existing solutions and emerging technologies available for enabling critical advertising use cases against privacy-related changes in the US. The provided assessments can serve as the foundation for your own privacy-utility determinations.

Four frameworks serve as the building blocks for the current evaluations and should inform your understanding and usage of the heatmap in practice. Those frameworks are:

1. **Stakeholder Framework:**
   Defines players engaged in the TV advertising industry.
2. **Use Case Framework:**
   Establishes the measurement and activation use cases most critical for TV advertising.
3. **Privacy Framework:**
   Outlines what to consider when evaluating if a use case, solution, and the ecosystem partners that enable it are durable with (or at risk of tripping) existing privacy regulations and platform policies. Each solution can be evaluated against this framework.
4. **Solutions Framework:**
   Identifies and classifies key solutions – tools, processes, methodologies, and technologies – that enable advertising use cases.

STAKEHOLDER & USE CASE FRAMEWORK	+	PRIVACY FRAMEWORK	+	SOLUTIONS FRAMEWORK	=	SOLUTIONS HEATMAP
TV advertising stakeholders and planning/activation and measurement use cases	→	Privacy regulations and policies threatening existing solutions	→	Range of existing and emerging alternative solutions	→	Which solutions are most viable given continued privacy pressures

Each section includes a description of *key takeaways, what* the framework is, its structure, *why* it is valuable, and *how* to use it. Frameworks have been pared down to critical content in the body of the report, along with footnotes for clarity, but we urge you to also consult the Appendix for additional detail and context where needed.

Note that these frameworks are flexible and made to evolve as regulations, policies, and solutions themselves continue to change. While specific details within each framework may need to be adjusted in the long-term, the underlying structure provides a robust foundation that can continue to be revisited to successfully enable your business and privacy strategy far into the future.

Stakeholder Framework

Key Takeaways

- Understanding the TV landscape is crucial for adapting your tools, strategies, and partnerships to meet privacy expectations.
- Various players in the TV ecosystem are responsible for different data-related functions that power advertising – varying from data access, collection, preparation (aggregating and packaging data for use by other ecosystem players), and deployment.
- As each stakeholder navigates the evolving ecosystem, they should contemplate their own unique combination of considerations and priorities around:
    - *Their structural position in the ecosystem* including their relationship with the consumer in the context of TV advertising, dependence on upstream partners for data access and deployment, transparency and communication with consumers around TV advertising, and breadth of data sharing needs.
    - *Compliance* with an increasingly complex patchwork of privacy laws and platform policies. A stakeholder's compliance requirements and risks are dependent on their structural position vis-a-vis the user and how (if at all) they collect, use, and share data.
    - *Business value and cost* of continuing to meet market needs, while minimizing the potentially high costs of implementing privacy changes. This is especially reliant on:
        - Offering *consumer value and providing ad/privacy experiences* that meet consumers' privacy expectations and minimize the onus of advertising consents and privacy tools.
        - Creating *value for business clients* and demonstrating ROAS through measurement.
    - Maximizing *efficiency and effectiveness* across all areas through enhanced data linkage capabilities, continuing to enable granular data usage for priority use cases, and ensuring all facets of tools and strategies are scalable.

Background

Why is it important? The TV ecosystem is composed of a complex mix of players – for some, there is a vested interest in enabling advertising, and for others, it is only a peripheral concern. Nevertheless, the ability of advertisers to reach consumers at scale is dependent on intermediaries: for example, for a consumer to see a TV ad they must have a TV-enabled device, which is likely manufactured by another player in the ecosystem. Each player may be responsible for a variety of functions related to data and data transfers that enable advertising, whether for collection, preparation and packaging, or deployment. For better or worse, the behaviors and decisions of each stakeholder in this chain affect whether you can even access and use device and consumer-level data signals. This means compliance with privacy requirements is contingent on the behavior of your collaboration partners as well. To begin to understand where or how tools, strategies, and partnerships must evolve, you must first understand the makeup and dynamics of the ecosystem and your role in it.

What is in it? The Stakeholder Framework outlines the pivotal players that comprise and shape the TV ecosystem, regardless of whether advertising is a priority for that player. The full framework (included in the Appendix) contains deep dives into each stakeholder of the current TV advertising ecosystem with explanations of their roles, priorities, concerns, and example companies in each space. The players and considerations identified were adapted from interviews with industry leaders from each category, market research, and the guidance of CIMM and the 4A's.

The abbreviated framework below highlights various TV stakeholders, grouped into categories where they provide similar or related functions within the ecosystem, followed by a summarized view of the concerns and priorities that surfaced across stakeholders.

How to use it. The stakeholder framework can be used in a variety of ways to:

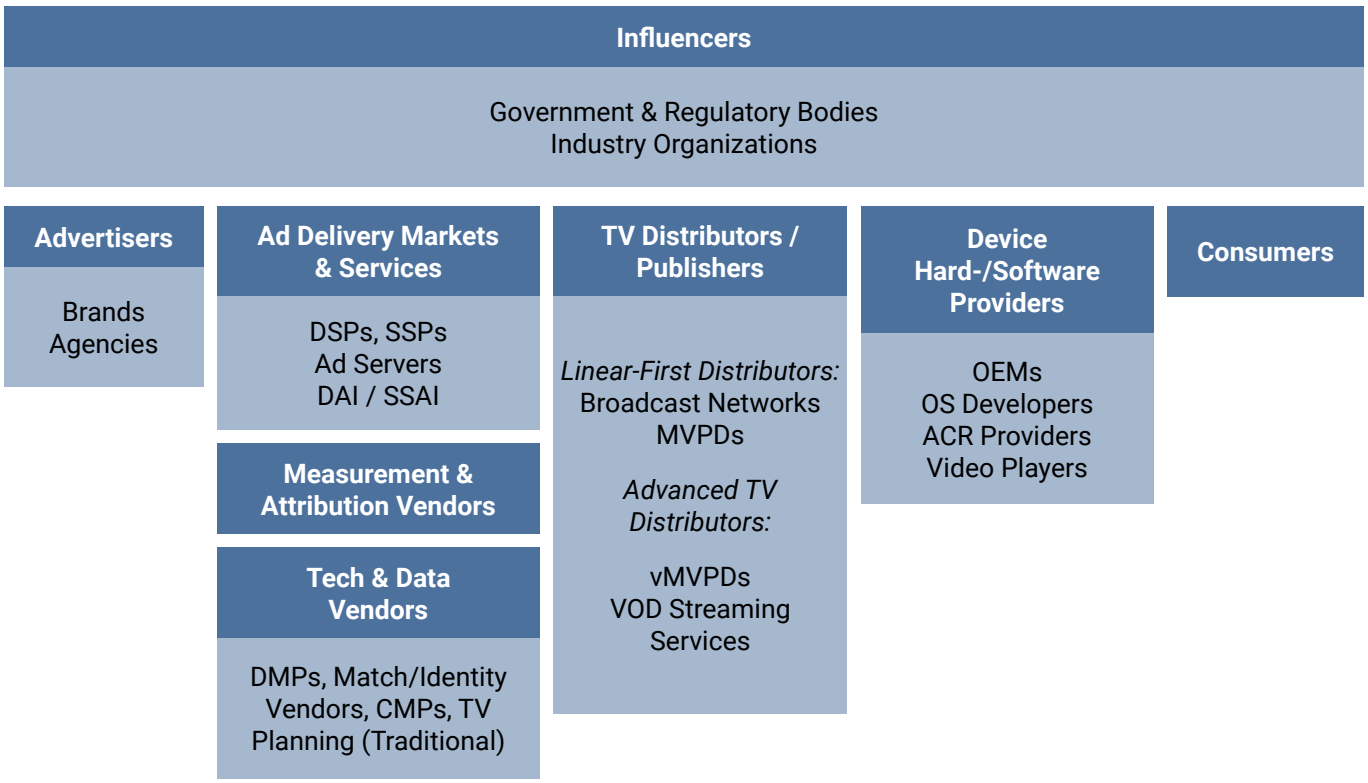
1) Determine your structural position in the ecosystem,
2) Identify who you must engage with as you evaluate and adjust your strategies for privacy compliance,
3) Inform your engagement strategy with different players by understanding their priorities and concerns, and
4) Provide a tool for defining and structuring your own approach to priorities and considerations within your business.

Key Stakeholders

The arrangement of stakeholders reflects a general flow of ads and/or data across the value chain. However, each stakeholder may also form direct data collaborations with others or even consumers directly, regardless of their position in the framework.

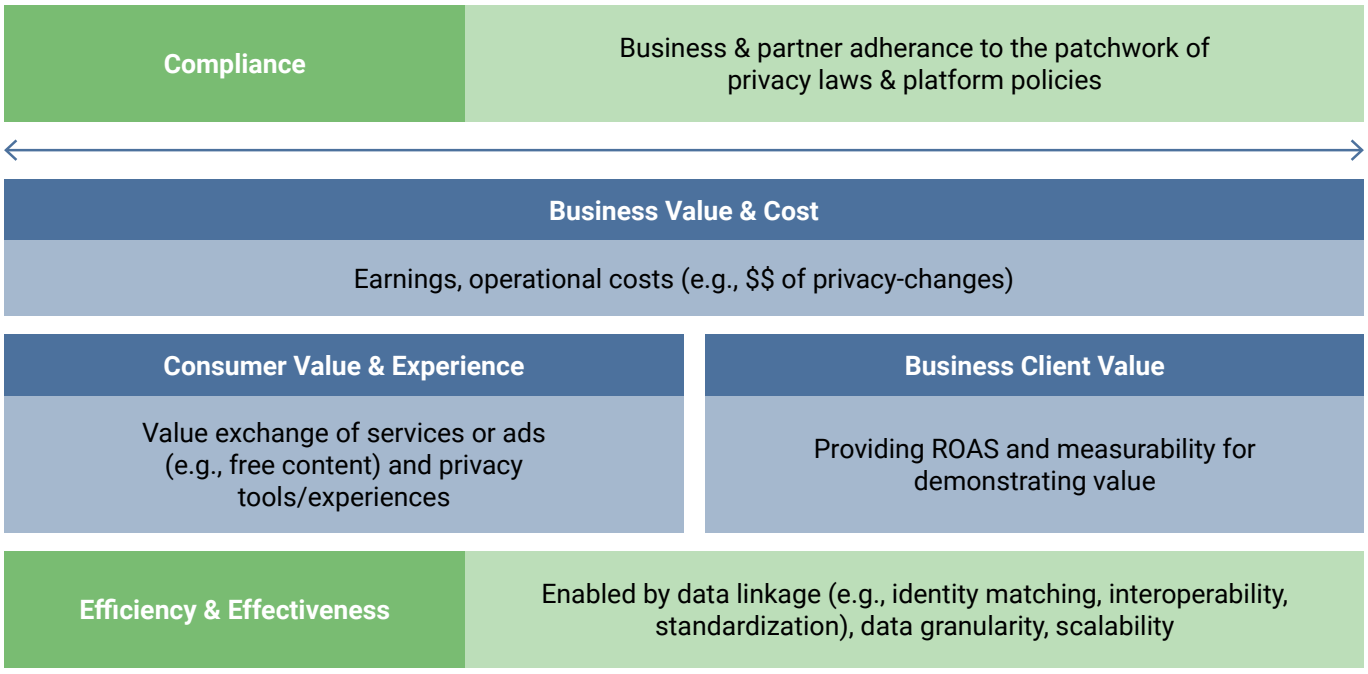
Each stakeholder needs to understand their structural position in the ecosystem as this has implications for adhering to privacy regulations and policies. We suggest leveraging this framework and considering:

- Do you have a direct relationship with a user/ consumer?
- Are you dependent on an upstream party to access and deploy user data?
- Are you dependent on an upstream party to communicate with a user and to provide transparency into their data collection, use, and sharing practices?
- Are you reliant on sharing data with multiple parties to power their business needs?



Concern Themes

Across our stakeholder discussions, similar concerns about advertising generally and privacy specifically emerged. The themes are described in brief below and details that apply specifically to each type of stakeholder are included in the full framework in the Appendix. These themes can serve as a tool to organize thinking about and/or gut-check areas of concern for one's own business or with partners.



At a high level, expected evergreen considerations surfaced – namely that stakeholders must fundamentally prioritize the value and costs any changes or behaviors have on their own business. And, inherent in maximizing this value is meeting the needs of clients, consumers, and/or other businesses – both efficiently and effectively. However, privacy compliance, control over commercial data leakage, and continued access to data signals in the face of platform policy changes and emerging solutions are now a top concern and greatly impact the elements and urgency of what stakeholders are prioritizing across these evergreen areas. Let's dive deeper into similarities heard in how stakeholders think about and prioritize these areas:

- **Compliance:** All stakeholders were concerned with the challenges of adhering to the increasingly complex patchwork of privacy laws and platform policies, such as state-by-state privacy legislation, within one's business and with up- and downstream data partners. For most interviewees, this was the most top-of-mind concern they considering today.

> *State-by-state policies are leading to whack-a-mole. Right now, the most efficient strategy seems to be finding the common denominator across policies and implementing the strategy that best meets these requirements nationally*
>
> **– Reed Barker, Head of Advertising, Philo**

Interviewees highlighted that compliance requires:

- *Ongoing vigilance, awareness, and understanding of new requirements,* which may require hiring or partnering with experts,
- *Identification of if and where one's business is directly or indirectly responsible* for upholding privacy obligations, and
- *Development and implementation of privacy-compliant strategies* internally and with one's partners wherever data is collected, processed, or deployed. Potential strategies are varied but may include elements of:
  1) updating or changing internal operations, technological infrastructure, and solutions,
  2) adopting tools to enable technical guarantees for proper data collection, usage, or sharing, or
  3) creating auditing or contractual processes.
- **Business Value and Cost:** Business performance requires meeting the needs of and creating value for clients while minimizing costs. Stakeholders expressed concerns about how ecosystem changes may lead to reduced ROI for themselves and clients (e.g., using less data for delivery →less effectiveness), plus concerns with how implementing privacy-related changes can be especially costly (e.g., hiring experts, deprecating or developing new infrastructure or operations). Business value is dependent on providing value to one's clients, whether they are people, other businesses, or both.
  - **Consumer Value and Ad Privacy Experience** covers the value exchange between consumers and businesses collecting, using, and sharing a consumer's data to deliver an ad-supported or data-powered experience such as the quality of TV content and free or heavily subsidized access to content through ad-supported offerings. This also concerns the strategies and tools businesses use to respect consumers' privacy expectations, for example minimizing the disruption and complexity of user choice experiences or the amount of data collected (*data minimization*).

> *[It is key to] improve overall consumer experience to demonstrate the value of advertising to consumers.*
>
> **– Joshua Chasin, Chief Measurability Officer, Videoamp**

  - **Business client value** includes the ability to actually provide value to other businesses AND often the ability to demonstrate ROAS (e.g., with delivery metrics, lift studies). Stakeholders across the ecosystem were concerned that the ability to measure delivery and/or connect delivery to outcome data (e.g., retail, purchase) is at risk, which can lead to brands undervaluing the partnership or media buys.

> *More marketers are leaning into direct outcomes or proxies for outcomes*
>
> **– Claudio Marcus, Independent Industry Expert**

- **Efficiency and Effectiveness:** Stakeholders agreed that unlocking value in the ecosystem while meeting privacy expectations requires maximizing efficiency and effectiveness across all practices and strategies. Opportunities stakeholders surfaced for enabling efficiency and effectiveness include:
    - **Data linkage capabilities** across providers, platforms, and channels to connect delivery, consumer, and partner data (e.g., identity, demographic, behavioral data). While linear TV was traditionally considered separately from other digital media, with the proliferation of advanced TV there are increasing calls to provide more opportunities for holistic planning and measurement across channels to inform decisions around limited budgets.

> *Without some way to link data across channels, the question becomes 'how much can you deliver with my first-party data alone?' which is not very scalable*
>
> **– Reed Barker, Head of Advertising, Philo**

        - **Identity matching:** Previously, data linkage often relied on sharing data to facilitate **identity matching** at the person/household-level with identifiers like IP address, email, or location. Due to concerns about the durability of personal identifiers, like IP addresses, most stakeholders emphasized that finding a privacy-forward identity matching alternative that relies on less physical data sharing and access is an extremely high priority.
        - **Control, interoperability, and standardization:** Likewise, stakeholders reported that data collaboration can be onerous, lead to commercial value erosion (specifically commercial data leakage), or even be impossible because of differences in levels of data granularity, formats, and identifiers. Standardization is necessary to enable efficient interoperability and buying.

> *As we aim for interoperability, we respect that data owners do not want their data to move around unnecessarily to avoid the risk of data leakage.*
>
> **– Kelly Barrett, SVP Product Management, Comscore**

    - **Data granularity:** Effective ad personalization and measurement has been reliant on using granular data at the person or household level. Therefore, ecosystem players are concerned with identifying where they can use fewer and less granular data points, while still collecting or leveraging a granular enough level of data for key use cases in a privacy-compliant way. This was especially pronounced amongst digital-first stakeholders who are more accustomed to using consumer-level data.
    - **Scalability:** Stakeholders emphasized all facets of advertising and data strategies must scale across touchpoints and use cases for efficiency and to motivate adoption.

Use Case Framework

Key Takeaways

- Data is used across a variety of use cases – needs, functions, or capabilities – that create value within TV advertising and for businesses, such as reducing wasted spend or quantifying the return on advertising campaigns.
- In practice, implementing each use case depends on multiple stakeholders, processes, methodologies, and technologies.
- To evaluate and determine the best privacy-forward solutions for your business, you must first identify and align on which use cases are most important to your business. This framework identifies use cases across two broad categories:
  - *Planning and activation* for developing and implementing TV advertising, such as targeting
  - *Measurement* to assess effectiveness and efficiency of TV advertising, such as verification and performance
- Additionally, this framework highlights which stakeholders are typically involved in enabling each use case to support your strategy, highlighting who you must coordinate with to ensure all privacy expectations and policies are adhered to.

Background

Why is it important? Industry practices across planning, activation, and measurement vary in their reliance on consumer data and thus whether they are impacted by ongoing privacy changes or not. New privacy regulations and policies will likely have implications across all areas of your business and ultimately on compliance. To approach this strategically, you must identify where consumer data is used and how important each use case is to your business.

What is in it? The Use Case Framework defines the critical planning, activation, and measurement use cases where TV advertising may rely on consumer data. Use cases are the needs, functions, or capabilities that advertisers employ to create value. Whereas solutions, explored further in the Solutions Framework and Heatmap, are the tools, processes, methodologies, and technologies that enable each use case. Use cases fall into two broad categories:

- *Planning and activation* use cases include any processes for developing and implementing advertising – from targeting strategies reliant on first- and/or third-party data to the processes and technologies employed to enable brand suitability, ad activation, optimization, and delivery.
- *Measurement* use cases or the metrics and currencies used to assess the effectiveness and efficiency of advertising. Measurement use cases vary from broad counting, verification, and validation to more specific evaluations of performance and impact.

The high-level framework included here highlights potential consumer data use cases based on what purpose they serve for advertisers. The full framework included in the Appendix provides further explanation of each use case and which TV ecosystem stakeholders may have a hand in enabling each use case.

How to use it. Before diving into specific solutions, leverage the Use Case Framework to:

1) Identify planning, activation, and measurement use case essential to the functioning of your business,
2) Consider the importance of each use case to establish investment prioritization if you have not already,
3) Use the stakeholder component to determine which other players you must coordinate with to enable this use case and ensure privacy requirements and policies are met, and
4) Employ the framework as a tool to align with partners across the industry on which use cases need to be prioritized as solutions continue to evolve or are developed.

	Purpose / Use Case	
Planning and Activation	Targeting - Existing Customers	Using 1st or 1st + 3rd-party data
	Targeting - Prospecting	Using 3rd or 1st + 3rd-party data
	Reach Extension	Using 1st + 3rd-party data
	Suitability	
	Campaign Activation	
	Optimization	
	Ad Delivery / Serving	
Measurement	Audience Counting	- Reach/ Frequency - Gross Rating Point (GRP)
	Protection / Verification	- Fraud/Security - Brand Safety
	Audience Validation	- Viewability - In-Target Audience - Attention
	Performance / Impact	- Conversion / Attribution - Brand Lift

Privacy Framework

Key Takeaways

- Privacy regulations, self-regulatory solutions, and platform policies differ by market, type of data, stakeholders, and more.
- But, all privacy regulations, self-regulatory solutions, and platform policies are based on standardized principles: the Fair Information Practice Principles ("FIPPS").
- Given FIPPs, the impact of privacy regulations and platform policies on the durability of existing and emerging solutions can be analyzed by reviewing the application of each solution for a specific use case through a framework of FIPPS-driven lenses.
- The first lens is whether data is personal or not (on a spectrum from directly identifiable to pseudonymous to anonymous).
- The second lens is whether a solution or use case may lose its future durability due to a platform technical policy (e.g., removing access to data signal) and, separately, if continued use may remain viable under regulations.
- The third lens is, if data remains accessible, what user choice (if any) is required based on a party's collection, use, and sharing practices.
- It is easy to assume assessments for the second and third lens are binary – i.e., that each solution or use case is subject to the same technical changes and user choice requirements. Unfortunately, that is not how regulators analyze use cases and solutions and it is not the impact platform policies have on stakeholders and the solutions they apply to different use cases.
- Generally, solutions that rely heavily on identity and access to and deployment of 1:1 person-level data are most at risk. But, the durability of each solution is dependent on a number of other factors, including what it is used for, the stakeholder using it, that party's relationship with the user, and that party's structural position in the advertising ecosystem.
- Therefore, the privacy framework is designed to enable a stakeholder to analyze the durability of a solution for a use case by running *each potential solution for each applicable use case by stakeholder* through a number of vectors.

Background

Why is it important? As surfaced by interviewees, privacy regulations and platform policies are fragmented and disjointed. Privacy regulations differ by state, country, channel, stakeholder, and even data type, and what is required on one platform may not apply to another. Consents required can vary depending on the party collecting and using the data and whether it is shared. The implications and intricacies across the portfolio of television advertising opportunities are enormous. For example, certain types of data – such as precise geolocation, video viewing, and ACR data – have *opt-in* requirements for various television advertising use cases. Certain other use cases—such as cross-context behavioral advertising or targeted advertising – require a user to be provided the option to opt out. Altogether, it is exceedingly difficult to understand regulatory requirements, platform policies, and their impact on television. On top of this, analyzing if the strategies and solutions your business uses for planning, activation, and measurement are compliant with these policies can feel impossible.

Several law firms and industry associations have created specific compliance guidance for different segmentations of marketers. The joint agency report from 4A's and Venable LLP on "U.S. State Privacy Laws" is one valuable example.

However, it is clear that more holistic, accessible guidance is needed. Notably, it is crucial to recognize that beneath the surface all privacy regulations, self-regulatory solutions, and platform policies are derived from a standardized set of principles, the Fair Information Practice Principles ("FIPPS"). This means FIPPS can provide a foundational understanding of requirements, but what this means in practice and how it applies to TV advertising data use cases and the solutions that power them is still a challenge given requirements apply differently to different use cases and different stakeholders.

What is in it? Building off FIPPs, we created a Privacy Framework to assess the legal and technical durability of the application of solutions to power use cases by stakeholders *across* privacy regulations and platform policies. By using these principles as our foundation, the Privacy Framework not only provides insights into solution compliance with *existing* regulations and policies, but also offers a forward-looking view of durability against yet-to-be-determined policies similarly developed based on FIPPS principles.

The *Privacy Framework* is a set of questions to uncover where and how data usage may be subject to and impacted by privacy regulations, policies, and technical changes. The questions are focused on the consumer entry point for data (e.g., operating system or device); the relationship between the consumer and the party collecting, using, or sharing personal data; how data is accessed or collected; how the data is used; the type of data; and the breadth and method of data sharing and collaboration.

For a selected solution, use case, and stakeholder, the framework helps determine:

- Whether data is personal or not, and
- If data is personal, the requirements and impacts on data collection, usage, and sharing for that specific use case, including:
    - User transparency (what type, granularity and you can or should provide it)
    - User choice (what type: none, opt-out, opt-in)
    - Or if data usage is prohibited by a regulation or platform policy (e.g., because the platform blocks access to a user-level signal it controls)

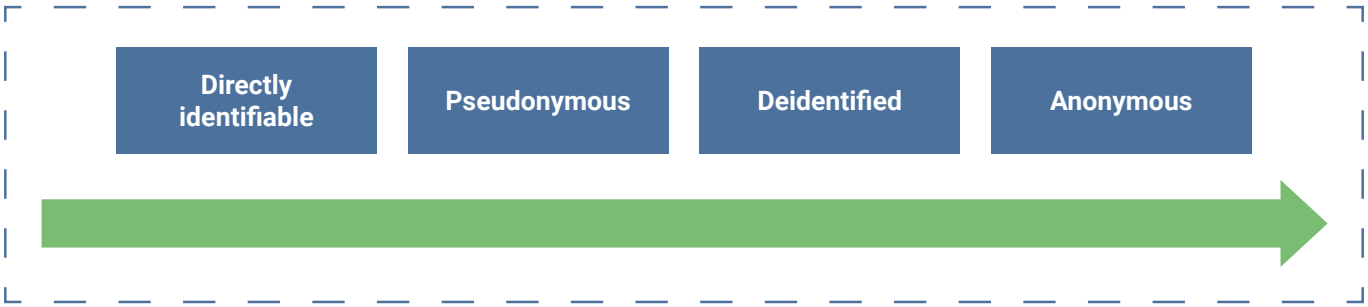
Rules of thumb mapping use cases and stakeholders to types of regulations and requirements are provided to assist usage of the privacy framework.

A guide to the various layers of technology that affect solution input or output is included in the Appendix and can inform assessments using this framework. Privacy risk is not universal across technology and solution layers, so you may need to consider using the Privacy Framework to assess compliance for each of the layers.

How to use it. **To assess compliance and risk, run each *potential solution* for each *applicable use case* by *stakeholder* through each element of the framework.** Enlist collaborative partners (technologists and product owners) and lawyers to facilitate the process. The frameworks and process are as follows:

Identifying Personal Data Usage

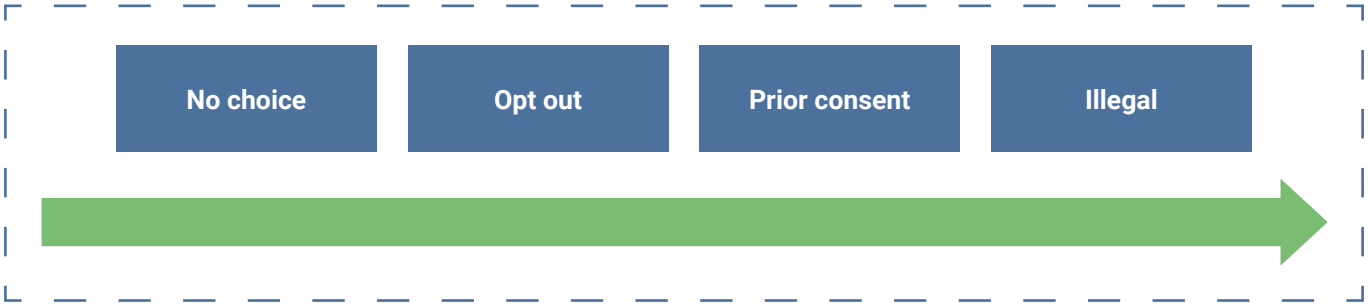
Step 1: Consider whether *any* data leveraged for the solution is personal or not. Data can be classified as directly identifiable, pseudonymous, de-identified, or anonymous. Any consumer data that is not fully anonymous may be subject to privacy laws and policies. *Ask:* Can the party holding the data or anyone who may access the data associate it with a user, either directly or by tying it to other data?



Assessing Data Access, Privacy Compliance, and Durability and Establishing Requirements or Constraints

Step 2: If data is determined to be personal, the next lens to consider is whether data collection, usage, and sharing are resilient against platform technical policies (e.g., an operating system removing access to data signal) and separately against regulations, using the questions outlined below. Unfortunately, no solution is likely to be durable and compliant across all use cases, stakeholders, and policies. In fact, certain technical changes from platforms only apply to certain solutions for specific use cases and stakeholders. For example, Apple's App Tracking Transparency (ATT) policy applies different consent requirements for app developers, content providers, and vendors *and* the policies differ by use cases (e.g. sharing data for targeted advertising). This is why you must consider the solution, use case, parties involved, and type of policy when conducting each evaluation.

Step 3: If continued access to data signals is durable under platform policies and continued collection, use, and sharing (where applicable) is permissible under regulations, the final lens to consider is what level of user choice (if any) must be implemented to ensure compliance. This determination is based on the parties involved and practices for collecting, using, and sharing data. This is the most difficult vector to consider because it is most open to interpretation. Again, this analysis may not be straightforward, as each solution and use case may not always be subject to the same user choice requirements in the eyes of regulators.



Steps 2 and 3 can be completed at the same time or iteratively using the same underlying Privacy Framework below. To conduct these investigations, examine the use of each solution by applicable use case for durability under platform policies and regulatory compliance and constraints across the following vectors:

Vector	Considerations	Examples
User Entry Point	• Which device is used? • Which operating system or browser is running on the device? • What signals does that entry point allow or block?	Amazon Fire TVs may never share user-level data vs. LG TVs may Android OS may limit access to IFAs / IP addresses in the future, whereas Apple may simply require opt-in consent to share IFAs.
User/party Relationship	What is the relationship between the user and the party collecting, using, sharing, and/or deploying data? • Does the user have an account with the party? • Is the party collecting, using, or sharing and deploying the data a vendor of a user entry point or consent provider? • Was the data collected by a party that does have a direct relationship with the user but that party then uses it in another context?	Structurally, is the party using data using it in the same context in which it was collected? Amazon sees a user watch a certain show on Amazon Prime and shows the user a Tune-in ad for a similar show. vs. An advertiser collects purchase or intent data in its store and then uses the data to target ads to its users on Amazon Prime content.
Data Use	What is the party accessing, using, or sharing data using the data for?	Is the data used to: • Facilitate security? • Prevent fraud? • Ensure the user doesn't see the same ad over and over? • Build/enhance profiles of the user used to target ads across multiple publishers? • Build a device graph used to enable advertisers or publishers to use data they collected in one context in another context (see user/party relationship above)?
Data Type	• Is the data an identifier, data associated with that identifier (e.g., viewing history), a device graph, or inferences based on prior behavior? • Is the data subject to additional laws (precise geo, biometric, sensitive, video viewing data)	Video Privacy Protection Act The Biometric Information Privacy Act FTC guidance on precise geolocation

Vector	Considerations	Examples
Data Collection	How is data collected? • Did the user hand it over? • Is the data collected by the user entry point? • Is the data collected by a vendor enabled by the user entry point or enabled by the provider of content accessed via the entry point? • What transparency did the user have into planned data use and sharing?	FTC Vizio decision related to the collection of viewing histories via automatic content recognition technology Various pending lawsuits related to the use of pixels and the Video Privacy Protection Act Various pending lawsuits related to the potential violation of Wiretapping laws California Attorney General decision related to Sephora
Sharing Breadth	How broadly is the data provided or collected shared? • Is it limited to the party that collected it? • Is it limited to a few trusted parties? • Is the data locked down and held only by the party that collected/received it but others can join their data with it or benefit from insights about the data? • How is that limitation enforced? Technically enforced (via APIs that restrict jobs run and which parties can access or join data) or by contract? • If contract, are they direct between the parties or via a "chain" of publisher to vendor(s) to advertiser? • Once data is shared, can a user easily know which parties received its data, opt-out, delete its data, request a copy, etc.? • How can the parties receiving the data prove they do what they say they do and don't do what they say they don't do?	Open programmatic, sharing data with thousands of potential vendors vs. Technically controlled collaboration (limited by use case and party) in a clean room vs. Complete on-device processing vs. Centralized portal facilitating transparency, opt-out, and deletion

Regulations and Use Case Mapping

We suggest using the following table to familiarize yourself with the common advertising use cases and types of data covered by privacy regulations and self-regulatory frameworks. As highlighted above, these may vary by regulation or platform. Overall, the combinations of use cases and stakeholders listed here are generally "regulated", which requires transparency, providing a level of user choice, and reasonableness in the breadth of sharing. A few rules of thumb for where regulations apply are to consider:

- *Use case*
    - Where collection of data occurs in one context, but it is used to influence or measure a consumer's behavior or measure in another context
    - Where collection and use of data using technology that is unexpected for consumers
- *Types of data* where the collection and use of data is considered "sensitive"

> *An industry misconception is that transparency leads to more opt-outs. Research shows that transparency and accessibility for consumers actually increases opt-in*
>
> **– Jesse Redniss, CEO, Qonsent**

Use the full table below to determine exact limitations and requirements.

Covered use cases and data types

Covered Use Case / Data	Use case / data	User choice	Stakeholder
Sharing video viewing activity	Data	Consent	First or third party
Collecting video viewing activity	Data	Opt-out / consent	First or third party
Sharing device / app activity	Data	Opt-out / consent	First or third party
Collecting device / app activity	Data	Opt-out / consent	First or third party
"Wiretapping"	Use case	Consent	First or third party
Sensitive health data	Data	Consent	First or third party
Precise geolocation data	Data	Consent	First or third party
Automatic content recognition	Use case	Consent	First or third party
"Unexpected data collection / use"	Use case	Consent	First or third party
Cross-Context Behavioral Advertising	Use case	Opt-out	First or third party
Targeted Advertising	Use case	Opt-out	Third party
Behavioral advertising (EU)	Use case	Consent[2]	First or third party
Online behavioral advertising (DAA)	Use case	Opt-out	Third party
Tailored advertising and related use cases (NAI)	Use case	Various	Third party

[2] Putting ePrivacy aside, we still believe a world exists in which *certain* first parties can collect and use data in a limited manner for ad use cases in reliance on legitimate interests. Devil is in the details.

Again, this guidance is not definitive and many of these areas are open to debate. This includes:

- ***Application to First-Party Data Use and Broader Use Cases.*** Historical ad industry consumer control solutions were limited to controlling "third parties" and to specific third-party use cases (e.g., building and using behavioral profiles across unaffiliated digital properties). Certain new regulations may increase this scope, mandating consumer control over:
    - **First-party data deployment on an unaffiliated digital property.** For example, a consumer brand uses data it collects directly from a consumer to target ads to that consumer on a social media platform, streaming service, or smart TV. This is commonly referred to as audience extension, ad networks, or matching.
    - **Use of measurement and reporting data collected on unaffiliated digital properties to enhance profiles.** This includes not only third-party but also first-party use of data on unaffiliated digital properties, such as data collected through a measurement provider's pixels on advertiser properties, which feeds bid ranking logic for future buys.
- ***Video Viewing and Activity Data Consent Details.*** The Video Privacy Protection Act and the FTC's Vizio decision require consent to share video viewing history and use unexpected technology to collect video viewing history and activity data. What constitutes appropriate consent is open to interpretation.
- ***Sensitive Data.*** The impact of consent requirements on the use of data, even with consent. For example, Washington State's My Health My Data Act arguably broadens the definition of health data covered, requires consent arguably impossible to obtain, and includes a right for consumers to sue companies for violations to a degree that advertising in any manner tenuously associated with health may be deemed too risky by certain companies.

A number of additional industry frameworks and guidance exist to help stakeholders manage the impact of privacy regulations and platform policies on advertising use cases. They may be helpful to inform decisioning here and include:

- IAB Multi-State Privacy Agreement (see Schedule A - Digital Advertising use cases)
- IAB Europe Transparency and Consent Framework (see Appendix A Purposes)
- Network Advertising Initiative Code of Conduct
- Digital Advertising Alliance Self-Regulatory Principles

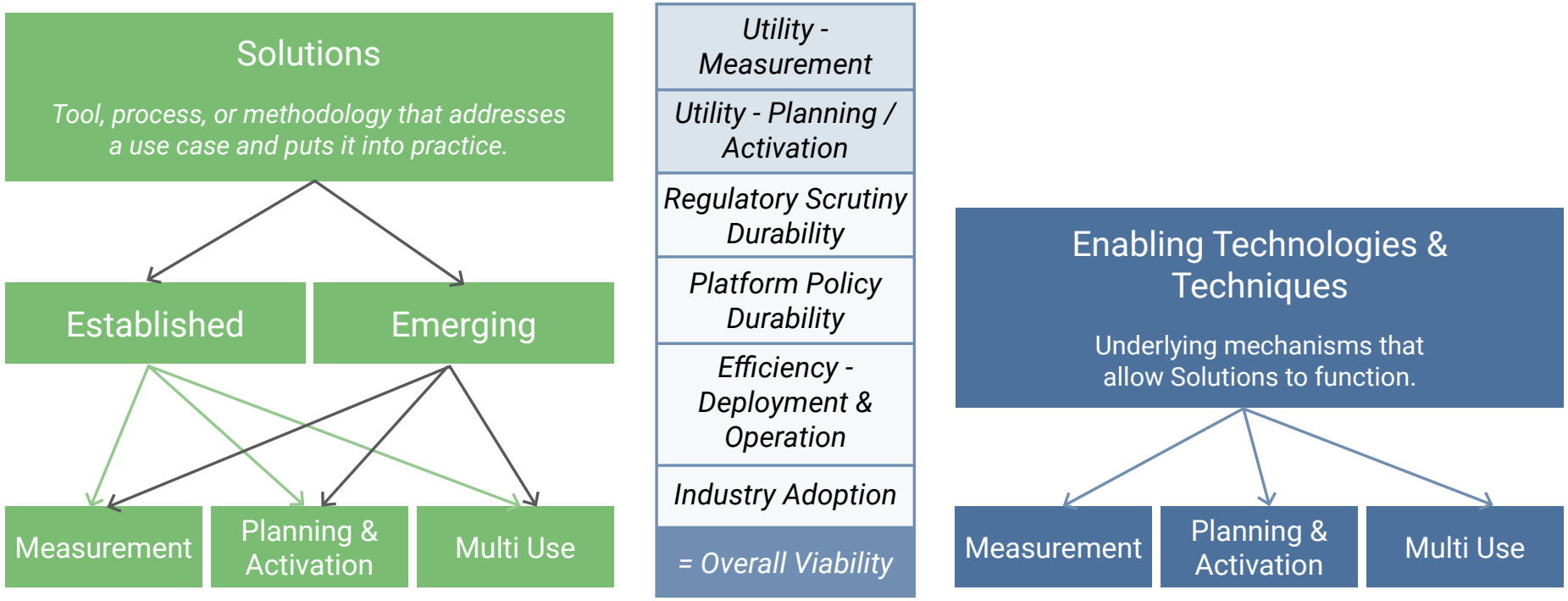
Given the devil is in the details, we advise you to seek your own legal advice when analyzing your use cases and solutions.

Solutions Framework

Key Takeaways

- A foundational set of solutions (tools, process, methods, or methodologies) and enabling technologies or techniques (underlying technological mechanisms) enable advertising use cases. Vendors can combine or tweak solutions and technologies to put a use case into practice, but the underlying components and mechanics are largely the same.
- By first working to understand the basic pros and cons of each type of solution your business uses, you are better positioned to dig into the details, nuances, and subsequent privacy implications of whatever specific product offering you use.
- This framework provides a guide – termed the *Solutions Index* – for identifying the solutions your business uses for TV planning, activation, and measurement. Core solutions and techniques are defined and classified as existing, emerging, or enabling to reflect the level of industry adoption or enablement.
- Key dimensions for evaluating each solution – utility, privacy durability, efficiency, and industry adoption – are explored in the *Evaluative Dimensions* component of the framework.

> *Contemporary and future media measurement necessitates a variety of data collection methods. Triangulating these various sources, is the path to addressing the diversity of media distribution and consumption.*
>
> **– David Algranati, Chief Product Officer, Comscore**



Background

Why is it important? In practice, use cases are implemented using solutions – sets of tools, processes, and methodologies, supported by various technologies and techniques. There are dozens of types of solutions, such as brand lift studies or panel-based ad ratings, each with unique benefits, pitfalls, and potential privacy concerns. Further, the specific composition and name of a solution offering can vary by vendor for any given use case even if the underlying mechanisms are the same. The strengths, priorities, and constraints of your business mean the solutions that make sense for you may not work for others. With so many potential solutions available, you may first want to level set on what the foundational solutions are and the pros and cons of each. This can help you then focus energy on uncovering the idiosyncrasies and privacy implications of the offering you use in practice.

Just as there are a variety of solutions available, there are a variety of factors to consider when evaluating them. Given the importance of these assessments, you need a structure to focus your approach on the elements that matter most.

What is in it? The Solutions Framework consists of a Solutions Index and a list of Evaluative Dimensions to consider when assessing each solution. Together these two pieces will help you identify what solutions to evaluate and what to consider when determining their overall viability (accounting for the latest platform policies and privacy regulations).

The *Solutions Index* provides an up-to-date list of foundational solutions relevant to TV planning, activation, and measurement[3]. TV solutions are categorized as *established* (traditional), *emerging* (recently available or adopted), or *enabling techniques and technologies* (supporting processes that enable them). The framework describes each solution[4] and indicates if it is primarily employed for planning/activation, measurement, or both – denoted as multi-use. The list has been distilled as much as possible to the core elements underlying various implementations. As such, any specific offering you leverage may be a derivative or combination of multiple solutions listed here.

The list of *Evaluative Dimensions* – utility, regulatory and platform durability, efficiency, and industry adoption – are the core elements to consider when assessing each solution. These map to the privacy-utility tradeoff (see Executive Summary) and were derived from the considerations industry leaders surfaced during interviews.

How to use it. The Solutions Index can be used to:

- Map which solutions your business employs for each critical use case,
- Identify which dimensions your business needs to consider when evaluating the impact of platform policies and privacy compliance and any utility tradeoff, and
- Explore alternative solutions for implementing critical use cases, if needed.

> *Panels are one piece (of measurement) for calibration, not a single source of truth. Panels, along with many other data sets, are all signals that should be included in measurement. It's a shift in the industry that's akin to Copernicus saying the Earth is not the center of the universe.*
>
> **– Kelly Barrett, SVP, Product Management, Comscore**

[3] Core solution types and classifications were selected based on their level of adoption, their relevance to the measurement and activation scope of the study, and the existence of supporting standards. The final list was calibrated using research interviews and feedback from the advisory committee.

[4] Definitions for a given solution may differ by vertical or market segment. For simplicity, in this report the most common industry definitions are included and considered.

Solutions Index

Established Solutions

Established solutions include approaches that have traditionally been employed in the TV industry for measurement insights and planning, as well as time-tested digital solutions that can apply to TV planning and media buying.

Solutions – Established	Use Cases	Description
Ad Verification Solutions	*Multi-Use*	Verification solutions designed to ascertain the viewability and suitability of ads, and take action accordingly.
Addressable – CTV	*Planning/Activation*	Advertising applied to Connected TV, enabling targeted and more personalized ads at scale.
Addressable – MVPD	*Planning/Activation*	Allows personalized ads at the household level within a multichannel video service like cable or satellite TV.
Brand Lift Studies	*Measurement*	Ad reach and campaign effectiveness studies based on polling and A/B tests.
Collaborative Data Pools	*Multi-Use*	Aggregated, anonymized data pools shared among several collaborating stakeholders.
Contextual Advertising	*Planning/Activation*	Contextual solutions where targeting is based on content being viewed.
Conversion & Incremental Lift Studies	*Measurement*	Sales lift and incremental lift studies utilizing A/B test experiments to demonstrate lift.
Digital & Programmatic OOH	*Planning/Activation*	Technologies that enable advertisers to dynamically display content on digital screens in public spaces.
ID-Based Targeting	*Planning/Activation*	Solutions utilizing unique identifiers to deliver personalized ads to consumers across digital platforms.
IVT Solutions (Fraud)	*Multi-Use*	Solutions to identify and prevent Invalid Traffic (IVT) to ensure the integrity and effectiveness of ad campaigns.
Media Mix Models (MMM)	*Multi-Use*	Statistical models based on historical data and variables to gauge channel efficiency and inform budget decisions.
Multi-Touch Attribution (MTA)	*Measurement*	Measures touchpoints in the customer journey, attributing credit to channels to understand their contribution.

Solutions – Established	Use Cases	Description
Out-of-Home Measurement (OOH)	*Measurement*	OOH measurement solutions for TV sets in public places e.g., bars, events, etc.
Panel-Based Ad Ratings	*Measurement*	Ensemble of metrics designed to assess campaign reach and effectiveness
Private Marketplaces (PMPs) – SSP Data	*Planning/Activation*	Platforms where advertisers bid on premium ad inventory from publishers. Solutions with data at SSP level use publisher-side data to optimize ad inventory and pricing, focusing on maximizing the value of publisher assets.
PMPs – Ad Server Data	*Planning/Activation*	Solutions with data at the ad server level utilize data from the ad server, providing a perspective that includes both publisher and advertiser insights, allowing for targeted and efficient ad placements.
Social Media Listening	*Measurement*	Conversation and trend monitoring on social platforms about TV content to gain insights into engagement.

Emerging Solutions

Emerging solutions include new and developing solutions that are being tested or progressively adopted by the TV industry to gain additional measurement insights and unlock new planning and activation capabilities. Digital solutions that apply to new forms of TV, such as CTV, are included as well.

Solutions – Emerging	Use Cases	Description
Attention-Based Advertising	*Multi-Use*	Advertising based on user attention signals, e.g., viewership type, duration, etc.
Consent Management Platforms (CMPs)	*Multi-Use*	Tools focused on user consent collection, compliance, and overall consent UX.
Contextual 2.0 (ML-Enabled)	*Planning/Activation*	Emerging form of Contextual leveraging ML to parse content and serve ads accordingly.
Customer Data Platforms (CDPs)	*Multi-Use*	Systems that collect and analyze customer data from various sources to enable personalized interactions.
Data Augmentation (2nd-Party)	*Multi-Use*	Dataset combination through partnerships or data exchanges to enhance insights and targeting capabilities.
Data Clean Rooms	*Multi-Use*	Computing environments enabling 3rd-party data collaboration without exposing underlying data sets.

Solutions – Established	Use Cases	Description
Privacy-Forward Industry Frameworks	*Multi-Use*	Privacy-forward frameworks & standards proposed by platforms/ industry bodies.
Retail Media Integration	*Multi-Use*	Integrating with Retailer platforms to gain expanded advertising opportunities.
Seller-Defined Audiences (SDA)	*Planning/Activation*	IAB standard for publishers to monetize audience segments based on 1st-party data.

> *Fast MMM, although still not widely adopted, has potential to be the future*
>
> **– Delphine Fabre-Hernoux, Chief Data & Analytics Officer, Group M**
>
> *Clean rooms are just one part of a much larger system and [still] need fully consented provenance*
>
> **– Jesse Redniss, CEO, Qonsent**
>
> *Incrementality is the future of MMM, [as it is] a great way to calibrate and feed more intelligence to it*
>
> **– Rodrigo Carone, Director, Video Measurement Solutions, Google**

Enabling Technologies & Techniques

Emerging solutions include new and developing solutions that are being tested or progressively adopted by the TV industry to gain Enabling technologies and techniques "power" or support both established and emerging solutions, supporting processes such as identity resolution for measurement, or adding a layer of privacy to data collaboration solutions.

Enablers	Use Cases	Description
Automatic Content Recognition (ACR)	*Measurement*	Technology that identifies specific content played on a device, enabling targeted ads and viewer analytics.
AI/ML Conversion Modeling	*Multi-Use*	AI-powered Machine Learning to help to fill gaps in measurement via conversion modeling.
Content Tagging & IDs	*Multi-Use*	Facilitate precise measurement and targeting of TV and video content with consistent tagging metadata.
Calibration Panels	*Measurement*	Meter-powered panels with statistical sampling used for reach & effectiveness measurement calibration.
CTV/OTT SDKs & Analytics	*Multi-Use*	Software toolkits designed for developers to integrate and enhance ad serving, analytics functionality.
First-Party Data Activation	*Planning/Activation*	Leveraging a company's directly collected customer data to create personalized marketing campaigns.
Identity Solutions	*Multi-Use*	Technologies that help identify users across different platforms and devices, enabling more precise targeting.
Privacy-Enhancing Techniques	*Multi-Use*	Methods to protect user data in light of privacy regulations, while still enabling advertising use cases.
Privacy-Enhancing Technologies	*Multi-Use*	Technologies adding a layer of privacy by adding obfuscation to, or injecting noise into, data sets.
On-Device Segmentation and Auction	*Planning/Activation*	Processing data on a device to prevent leakage while still allowing targeting and activation.
Privacy Controls – Device/Platform/Provider	*Multi-Use*	Process of adding privacy controls at various levels for consumers to retain control over their data.
Sentiment Analysis	*Measurement*	Interpreting and classifying the emotional tone behind consumer feedback or social media content
Server-Side Ad Insertion (DAI/SSAI)	*Planning/Activation*	Technology that customizes ads and stitches them seamlessly into a single video stream.
Statistical Sampling	*Measurement*	Technique used to extrapolate behaviors and trends of a larger population, based on a sample.
Surveys	*Measurement*	Gather direct feedback from targeted audiences, helping brands understand consumer preferences.

> *We all need to become more comfortable with measurement [based on more] modeling. We all need to start accepting AI/ML can help represent what is happening even [with less data]*
>
> **– Delphine Fabre-Hernoux,**
> **Chief Data & Analytics Officer, Group M**

Evaluative Features

In order to decide where to maintain or evolve your business practices, consider the following dimensions for each solution:

Dimension Criteria	Description	Considerations
Utility (Planning & Activation / Measurement)	The value your business (and clients) derive from a solution For example, level of actionability, scalability, breadth and depth of enabled use cases in the context of measurement, and planning/ activation.	The elements your business prioritizes may be unique to your business, so you need to determine how *you operationalize and score value.* A single solution may provide different value for a planning and activation versus measurement use case. *Consider evaluating the value for planning/activation and measurement use cases separately.*
Regulatory/Policy Durability	Regulatory and platform policy compliance and resulting durability (or lack thereof)	***Use the Privacy Framework outlined above to conduct these evaluations.*** Regulations and platform policies are evolving at different paces and the penalties for noncompliance vary. As such, *investigate regulatory and platform policy risk separately.*
Efficiency, Deployment, & Operations	Assessed cost and level of effort required to deploy & operationally maintain a solution	*See Stakeholder Framework for more details.*
Industry Adoption	Relative level of market adoption, including industry coverage and consensus around solutions and standards	Solutions with greater industry standardization and more support may be easier to integrate and maintain longer into the future.

Solutions Heatmap

Key Takeaways

- The solutions heatmap is a tool for evaluating solutions across utility, privacy durability, efficiency, and adoption.
- These dimensions can then be combined to create a unified "Viability Score" metric for weighing the privacy-utility tradeoff and industry considerations for each solution you use. Scores serve as a cautionary flag or opportunity indicator of where it is most urgent to investigate further and act.
- Foundational evaluations are provided (except utility as this differs widely per business), but which solutions to focus on and utility scoring should be tailored to reflect your own business priorities.
- Viability varies widely across solutions, but few solutions and technologies are optimally privacy-durable or disqualified. This means the *devil is in the details of the underlying data inputs, outputs, stakeholders, and use cases.*
- Several trends are apparent in the generalized heatmap:
  - Legacy TV solutions appear more resilient to privacy concerns as they have historically relied on less people-based signals. On the other hand, solutions leveraging "big data" – such as emerging solutions or those used on digital platforms – may require more attention because they rely heavily on data collaboration.
  - Compared to measurement use cases, planning and activation solutions are at greater risk for disruption because currently, they tend to use and share more person-level data.
  - Platform (device and operating system) policies impact signal availability faster than regulations – do not ignore platform considerations

Background

Why is it important? Now it is time to translate these frameworks and the wealth of information you have gathered about your business into actionable insights and strategies for TV planning, activation, and measurement. This requires evaluating which solutions are meeting your business and privacy needs and which are not. The *Solutions Heatmap* provides a user-friendly tool for organizing your assessments across selected solutions and dimensions. It also offers an approach for combining ratings across dimensions into a single unified score for each solution. With solution evaluations simplified and organized into a color-coded heatmap, it is easier and more intuitive to identify risks and make comparisons across solutions.

Initial assessments are provided to illustrate our point of view and facilitate getting started, but the heatmap can be customized and updated to suit your specific business needs.

What is in it? The *Solutions Heatmap* consists of a row for each solution and six columns corresponding to the *primary use case* of the solution (measurement, planning, or multi-use) and evaluative dimensions – *utility, privacy durability, efficiency, and industry adoption*. Privacy risk is divided into "Regulatory Risk" and "Platform Risk" as described in the Solution Framework because regulatory requirements differ from platform policies in their risk nature, their pace

of implementation, and their enforcing entities. Each solution (for the stated use case) was run through the *Privacy Framework* to determine the "Regulatory Durability" and "Platform Durability" score.

All dimensions are combined to generate a final column – the "Viability Score" – reflecting the anticipated resilience and usefulness of a given solution amidst privacy-related changes. These scores range from "high resilience" to "significant risk." The Viability Score should not be interpreted as good or bad, but rather as where further investigation is needed most urgently. More details on determining and calculating scores are included in the "Methodology" section of the heatmap.

Initial evaluations *generalized* across stakeholders are provided for each solution based on the collective expertise of the ThinkMedium and Shullman Advisory teams combined with industry research (e.g., reports, documentation). Scores were calibrated against stakeholder interviews and input from the advisory council. We invested significant time to provide evidence-based scoring, (with rationales provided in detailed footnotes in the Appendix), but ultimately our conclusions might differ from other industry definitions and points of view.

Established, emerging, and enabling solutions or technologies are scored in separate heatmaps for simplicity and to emphasize how you think about each solution will evolve over time. For example, the lack of industry adoption or standardization, not privacy compliance, may be the reason some emerging solutions and enabling technologies are considered less viable today. Solutions in their infancy today may be more promising in the future and long-employed solutions of today may fall out of favor over time.

How to use it. Use the general evaluations provided in the Heatmap and it can be customized further to reflect your own needs, priorities, and appetite for risk. Either way, plan to continue updating the heatmap as new solutions become available and regulations and policies roll out. By creating a holistic view of your solutions and assessments, you can identify which planning, activation, and measurement solutions are most at risk to inform where you need to focus your attention to ensure privacy durability and utility. To use the heatmap:

1) Explore the privacy durablity and industry concerns of the solutions your business already leverages,

2) Determine and organize utility scores for each solution reflecting your business's unique point of view,

3) *(If desired)* Implement customized weighting to reflect your own business priorities and calculate tailored viability scores, and

4) Examine areas of high risk versus value in order to prioritize which solutions to explore deeper for privacy compliance.

As the Privacy Framework draws on the foundational FIPPS principles and given current policy and product development trends, we have high confidence the evaluations provided using this framework will hold for at least the next 12 months, if not longer. The existing scores are to be used as is, but can be adjusted in the mid-term if large shifts occur (although they are not currently predicted).

Scoring Methodology

Heatmap Criteria & Scoring

Each solution in the heat map needs to be evaluated against the dimensions outlined in the Solutions Framework – utility, risk, efficiency, and industry adoption – as shown below. The current heatmap is filled in with foundational assessments across all dimensions except utility, which is left up to the reader to determine for their own business.

Criteria	Utility	Regulatory Scrutiny Durability	Platform Policy Durability	Efficiency – Deployment and Operation	Industry Adoption
Explainer	*To be scored by stakeholders for their specific use case(s)*	*Scored by ThinkMedium & Shullman Advisory based on desk research, research interviews with industry stakeholders, and collective industry knowledge. Scoring rationales are available in the Appendix section.*			

Each solution is graded on how well it performs on a given dimension using the following 5-point scale. Color-coding is used for simplicity, but if you wish to conduct your own evaluations and calculations, use the corresponding numerical scores included in parentheses:

(3)	Consistently better-than-average performance in a given criteria, e.g., high regulatory scrutiny durability.
(2.5)	Satisfactory performance in a given criteria most of the time, e.g., generally satisfactory resilience to regulatory scrutiny.
(2)	Nuanced performance in given criteria, e.g., level of regulatory scrutiny is dependent on the use case, inputs, and outputs.
(1.5)	Performance in a given criteria has notable caveats, e.g., a significant likelihood of regulatory scrutiny across most use cases.
(1)	Performance in a given criteria includes significant concerns, e.g., a high likelihood of future regulatory scrutiny.

Scoring Rationales

Individual scores used in foundational assessments across dimensions (minus utility, which is left to the reader) are explained in detail via footnotes in the Appendix – Solutions Framework section.

"Viability Score" Definition & Weighting

A "Viability Score" is produced for each solution by combining the dimensional scores. High or low scores are not an endorsement for or recommendation against any specific solution. Instead, low viability scores signal caution and that further measures must be taken to understand the benefits, risks, and long-term implications of continuing to use that solution. Viability scores can be interpreted using the following scale.

Viability Score	Scoring Calculation Brackets	Score Definitions
	x >2.5	High degree of industry standardization, scalability, with demonstrated utility and likely future-looking privacy durability.
	2.25< x <2.5	Generally satisfactory degree of industry standardization, scalability, demonstrated utility, and likely future-looking durability.
	2< x <2.25	Certain use cases might require additional care and/or resources to address scalability, standardization, utility, or durability.
	1.75< x <2	Demands closer attention and/or resources in one or several areas across standards, scalability, utility, and/or durability.
	x <1.75	One or more area(s) of significant concern across industry standardization, scalability, cost, utility, and/or privacy durability.

Calculation of the "Viability Score" is dependent on how your business prioritizes each evaluative dimension against one another. The Solutions and Stakeholder Frameworks can inform how to think about these dimensions, but ultimately what your business prioritizes depends on your unique context, concerns, and risk aversion. Once you have defined your preferred balance, create weighting coefficients that will be assigned to each dimension across solutions. To compute the viability scores, calculate the weighted average.[5]

In the provided evaluations, the following weighting coefficients were used to reflect the input and prioritizations surfaced during stakeholder interviews:

- ***Regulatory Scrutiny Risk [1.5x]:*** receives a higher coefficient to reflect the critical role of regulatory compliance in ensuring future-state solution & tech viability.
- ***Platform Policy Risk [1.5x]:*** receives a similarly high coefficient to reflect the far-reaching impact of platform policies on future-state solutions & tech viability.
- ***Efficiency – Deployment, Operation [1x]:*** scoring reflects the important yet nuanced nature of efficiency and cost as a viability component, as it can be a dealbreaker for smaller organizations, but may be a lesser concern for larger companies.
- ***Industry Adoption [0.75x]:*** receives a slightly lower score coefficient than other dimensions in order to avoid penalizing emerging solutions and technologies for their inherent lower level of overall adoption.
- ***Utility [n/a]:*** scores are not currently included in the viability calculation, however, if you wish to incorporate it in your calculations we recommend starting with a weighting coefficient of [1x] and adjusting from there based on your own preferences.

[5] The weighted average is calculated by multiplying the score on each dimension by its assigned weight, summing these values, and dividing by the sum of the total weights.

Example Heatmap Evaluation and Interpretation:

The following walks through how to interpret each column, how each dimension was evaluated, and how the final score was calculated using Media Mix Modeling as an example. Each solution was run through the same process across use cases, stakeholders, and layers to produce the provided heatmap table.

Output in Heatmap Table

	Legacy & Established Solutions	***Primary Use Case***	***Utility***	***Regulatory Scrutiny Risk***	***Platform Policy Risk***	***Efficiency – Deployment & Operation***	***Industry Adoption***	***Viability Score***
Solution	***Media Mix Modeling (MMM)***	*Multi-Use*	*Use Case-Dependent*					
Input and Process Behind Each Score								
Interpretation / Evidence *(see footnotes)*	*Name of Solution + Link to Appendix definitions and footnotes*	*Caters to both Measurement and Planning/ Activation use cases.*	*Report readers should leverage the framework and scoring scale and apply their own relative utility score.*	*High level of assessed regulatory durability*[6]	*Satisfactory level of resilience to platform policy shifts*[7]	*Medium level of deployment efficiency and cost*[8]	*Satisfactory level of industry adoption and standard-ization*[9]	*High Viability Score in light of privacy shifts, efficiency, industry criteria (calculated based on criteria scores)*
Scoring & Weighting		*Multi-Use*		*3 (x1.5)*	*2.5 (x1.5)*	*2 (x1)*	*2.5 (x.75)*	*2.55* *See Appendix for calculation*

Overall Interpretation: My business uses MMM today, but only once a year to inform allocation decisions. Overall, I see it is relatively robust against privacy-related changes, is widely available across the industry, and – although it may require some investment to onboard – it is not especially cumbersome for my business to use and maintain. If another preferred solution becomes unavailable, we may be able to revert to MMM as a stopgap as we explore other solutions. Alternatively, we could proactively increase our usage of MMM-based solutions whenever possible to allow greater flexibility and timeliness in response to privacy changes.

[6] Require anonymization to uphold "green" rating, more resilient for 1st-party. Inputs at risk when they include user/device-level sensitive click/conversion data.

[7] Platform policies and signal loss curb data availability to feed media mix models, thus likely affecting accuracy. Platforms offer their own MMM pipelines.

[8] Reliant on data science expertise and quality data inputs, lighter and faster approaches have been developed recently (incl. by specialized vendors).

[9] Historically a landmark solution in measurement toolboxes, recognized for its go-forward durability (e.g., cited in interviews: SambaTV, Google, etc.).

Established Solutions Heatmap

Note: click on the Solutions links in the first column to view detailed scoring and definitions.

Established Solutions	Primary Use Case	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Viability Score
Ad Verification Solutions	*Multi-Use*						
Addressable – CTV	*Planning/ Activation*						
Addressable – MVPD	*Planning/ Activation*						
Brand Lift Studies	*Measurement*						
Collaborative Data Pools	*Multi-Use*						
Contextual Advertising	*Planning/ Activation*						
Conversion & Incremental Lift Studies	*Measurement*						
ID-Based Targeting	*Planning/ Activation*						
IVT Solutions (Fraud)	*Multi-Use*						

Established Solutions	Primary Use Case	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Viability Score
Media Mix Models (MMM)	*Multi-Use*						
Multi-Touch Attribution (MTA)	*Measurement*						
Digital & Programmatic OOH	*Planning/ Activation*						
Out-of-Home Measurement (OOH)	*Measurement*						
Panel-Based Ad Ratings	*Measurement*						
Private Marketplaces (PMPs) – SSP Data	*Planning/ Activation*						
PMPs – Ad Server Data	*Planning/ Activation*						
Social Media Listening	*Measurement*						

Emerging Solutions Heatmap

Note: click on Solutions links in the first column to view detailed scoring and definitions.

Emerging Solutions	Primary Use Case	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Viability Score
Attention-Based Advertising	*Multi-Use*						
Customer Data Platforms (CDPs)	*Multi-Use*						
Contextual 2.0 (ML-Enabled)	*Planning/ Activation*						
Consent Management Platforms (CMPs)	*Multi-Use*						
Data Clean Rooms	*Multi-Use*						
Data Augmentation (2nd-Party)	*Multi-Use*						
Privacy-Forward Industry Frameworks	*Multi-Use*						
Retail Media Integration	*Multi-Use*						
Seller-Defined Audiences (SDA)	*Planning/ Activation*						

Enabling Tech Heatmap

Note: click on Enabling Tech links in the first column to view detailed scoring and definitions.

Enabling Technologies & Techniques	Primary Use Case	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Viability Score
Automatic Content Recognition (ACR)	*Measurement*					
AI/ML Conversion Modeling	*Multi-Use*					
Content Tagging & IDs	*Multi-Use*					
Calibration Panels	*Measurement*					
CTV/OTT SDKs & Analytics	*Multi-Use*					
First-Party Data Activation	*Planning/ Activation*					
Identity Solutions	*Multi-Use*					
Privacy-Enhancing Techniques	*Multi-Use*					
Privacy-Enhancing Technologies	*Multi-Use*					
On-Device Segmentation and Auction	*Planning/ Activation*					
Privacy Controls – Device/Platform/ Provider	*Multi-Use*					
Sentiment Analysis	*Measurement*					
Server-Side Ad Insertion (DAI/SSAI)	*Planning/ Activation*					
Statistical Sampling	*Measurement*					

Enabling Technologies & Techniques	Primary Use Case	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Viability Score
Automatic Content Recognition (ACR)	*Measurement*					
AI/ML Conversion Modeling	*Multi-Use*					
Content Tagging & IDs	*Multi-Use*					
Calibration Panels	*Measurement*					
CTV/OTT SDKs & Analytics	*Multi-Use*					
First-Party Data Activation	*Planning/ Activation*					
Identity Solutions	*Multi-Use*					
Privacy-Enhancing Techniques	*Multi-Use*					
Privacy-Enhancing Technologies	*Multi-Use*					
On-Device Segmentation and Auction	*Planning/ Activation*					
Privacy Controls – Device/Platform/ Provider	*Multi-Use*					
Sentiment Analysis	*Measurement*					
Server-Side Ad Insertion (DAI/SSAI)	*Planning/ Activation*					
Surveys	*Measurement*					

Conclusion & Action Plan

Television, once dominated by traditional TV programming, has joined the digital revolution with the rise of CTV, mobile, and on-demand streaming. Advertisers are now able to capitalize on linear and Advanced TV offerings. Alongside these shifts, privacy-forward regulations and platform policies have arisen to address consumers' demands for privacy. Embracing privacy is not only crucial for compliance, but because your business' success is dependent on meeting the needs of your customers. You must take action now to align your current practices with existing regulatory and platform policies – there are no durable work arounds. At the same time, you have a strategic opportunity to proactively mitigate the impact of future privacy changes by identifying areas of potential risk and adjusting your current planning, activation, and measurement practices accordingly.

Action Plan

Although understanding and adhering to the latest privacy shifts seems daunting, the frameworks and heatmap outlined in this report serve as a guide to facilitate taking action. As highlighted throughout the report, each framework builds upon one another. The action plan below provides a roadmap for how to use elements of each framework concurrently in order to develop a strategic plan to adopt privacy-forward solutions wherever possible. This is an iterative cycle consisting of three phases:

Step 1 - **Identify:** Once you understand the key stakeholders and dynamics of the ecosystem (see *Stakeholder Framework*), start gathering foundational information (e.g., from documentation, inbound, internal experts) specific to your business. Identify:

- Your critical TV advertising use cases that may use personal data - See *Use Case Framework*.
- Current solutions your business employs to implement each use case - Refer to *Solutions Framework*.
- Partners/Vendors who have any role, no matter how large or small, in implementing your solutions or leveraging output - See *Stakeholder Framework*.
- Any other practices, processes, or partnerships that may be subject to privacy policies - *See "Personal Data" spectrum in the Privacy Framework and consider any practices that use any data that is not anonymous or aggregated.*

Step 2 - **Evaluate:** Next, evaluate each solution or technology that you currently or may consider using for planning, activation, and measurement. To achieve this

- Determine how important each dimension of the framework - utility, risk, efficiency, and industry adoption - is to your business based on your own needs, priorities, and concerns - See *Solutions Heatmap and Stakeholder Frameworks* to explore concerns and guidance on creating and applying weighting.
- Refine the existing assessment to reflect your specific utility scoring of each solution for your business and *(if preferred)* apply the priority weighting across dimensions - See *Solutions Heatmap*.
    - If you wish to evaluate a solution for an alternative or specific use case (e.g., for multi-purpose solutions), simply add a row for the additional solution-use case combination. Use the same methodology as the rest of the heatmap for any assessments and calculations.
- Prioritize where you want to investigate deeper and wider based on the heatmap scoring.
- Conduct a thorough examination into the privacy compliance and resilience of your priority solutions - Consult the *Privacy Framework* to determine where and why these solutions may or may not align with current privacy standards.
    - For technical assistance and to ensure partners are adhering to data-related practices refer to the *Use Case Framework* to identify your potential partners who may be involved throughout the process.

The evaluations provided in this report reflect the existing state of the industry today and some known pending changes and trends. Again, we anticipate the current evaluations are robust and will be applicable for at least the next 12 months, but as the industry continues to evolve you may need to reconsider your scores if any monumental changes occur beyond then.

Step 3: **Evolve:** - Now that you have customized evaluations of how valuable and privacy-forward certain TV solutions are for your business, commit to making a plan and taking action on your findings. You must carefully consider the privacy-utility trade off of each solution you are using to determine next steps, the "Viability Score" is one metric to examine this concept.

Which actions to take are varied and can involve anything from simply evolving existing practices to overhauling operational processes. Changing anything about the solutions you use - even eliminating low value, high risk solutions or adopting high value, low risk solutions - can require massive updates to your existing infrastructure and processes. The good news is that even if a solution is at risk, you may not need to fully eliminate that solution altogether; first investigating alternative approaches may be especially fruitful for high utility solutions your business relies on. Consider all your options and test what works for your business, such as:

> *Just because you have access to the data doesn't mean you should use it, data minimization is important and consent is key.*
>
> **– Delphine Fabre-Hernoux, Chief Data & Analytics Officer, Group M**

- Adjusting processes or methodologies where possible (e.g., data minimization, limited data collaborators),
- Adding privacy-related terms to contracts and processes or leveraging technological guarantees for data collaboration, and
- Adopting lower risk partnership or solutions, where necessary.

One final caution is to remember the knowledge and investigations here focused on the long-form video format. If your business relies on other formats across your media strategy, you need to understand the risks of optimizing towards one format and find the balance that is right for your business.

With privacy-forward solutions in place, create a plan for continuing to reassess and update your solutions and technologies to account for progress in privacy policies and technology development. If use cases and solutions critical to your business are currently at high risk with no foreseeable resolution, consider how you may engage with industry associations and working groups to prioritize development and evolution in these areas.

Final Thoughts

While taking action may seem like a monumental task, rest assured that you are not navigating these changes alone. While this report will help you get started, there are also experts you can engage to guide you in developing your own customized privacy-forward strategy. By prioritizing and building toward privacy in all your planning, activation, and measurement practices, you can tackle any future disruption with the confidence that you are doing what is good for your business and good for your customers.

Appendix: Framework Details and Scoring Rationale

Stakeholder Framework: Details

Stakeholder Engagement with Consumer Data " Tags"

Throughout the stakeholder framework, "tags" are included for each stakeholder to indicate where they are typically involved in the enablement, collection, and usage of consumer data for advertising purposes. These tags can help inform which partners to get information from or coordinate with to ensure privacy expectations are being met or evaluated correctly across the lifecycle of consumer data for key use cases. The tags and definitions are as follows:

- **Data Collection:** Direct collection of data from consumers (1PD) or enablement of data collection.
- **Data Preparation (Prep):** Processing, cleaning, packaging, and/or integration of consumer data to make it available as input for other stakeholders or use cases. For example, this can include third-party vendors ingesting and packaging consumer data across multiple sources or the processes first-party data collectors use to gate and/or monetize data collaboration.
- **Data Analysis:** Leveraging data collected directly (1PD) and/or indirectly (2PD, 3PD) to generate insights that can inform future decision-making.
- **Data Activation:** Leveraging data collected directly (1PD) and/or indirectly (2PD, 3PD) to maximize campaign performance.

Full Stakeholder Framework

The full framework includes specific details of who each stakeholder is, how they most commonly engage with consumer data, key areas of priority and concerns regarding advertising and privacy, plus example companies in the space.

Stakeholder			Description[10]	Key Concerns[11]	Examples
Consumers			Consumers of media and advertising, brand customers.	• **Consumer value,** e.g., content quality, free or reduced cost, ease of platform use, discovery opportunities, brand offerings, and discounts • **Consumer Ads/Privacy experience,** incl. transparency, control, security, anonymity, and trust (See Privacy Framework)	Often considered at the individual or household (HH) level
Advertisers Providers of goods or services	**Brands**[12] *Data collection* *Data prep* *Data analysis* *Data activation*	**Digital-first**	Brands historically reliant on digital marketing channels (e.g., search, programmatic, email) for advertising.	• **Business value and costs:** ROAS (including ad measurability[13]), operational costs • **Compliance** with fragmented legal and platform policies as 1PD collectors and 2/3PD users • **Efficiency and Effectiveness:** durable data linkage[14] (e.g., with identity matching) across 1P/2P/3P; granularity, scalability + standardization for data formatting/availability, reporting and performance insights, & currencies • **Consumer value and privacy experience with ads and brand,** such as personalization, onsite purchase experiences, non-disruptive ad experiences	
		Linear-first	Brands historically reliant on linear-television for advertising.		

[10] Where possible, descriptions pull from the ARF-CIMM Lexicon 4.0 (2021).

[11] Input for these concerns are generalized from stakeholder interviews and desk research. As such, concerns highlighted here may not apply to all "Examples" in the category and may not be exhaustive.

[12] ARF-CIMM Lexicon 4.0 (2021)

[13] Linear-first brands reported they may have an advantage in adopting privacy-first solutions because traditional TV measurement has relied on extrapolating from representative panels for decades so they are already comfortable with less deterministic strategies. Conversely, digital-first brands, accustomed to more granular views of consumers, expressed concerns about sample size, quality, and accuracy of panels and modeled data. Interviewees also noted that increasing legislation on granular, sensitive data may compromise panel composition and accuracy.

[14] As digital and linear continue to converge, there are increasing industry calls to connect spend and purchase data across channels, which requires record linkage.

Stakeholder		Description[10]	Key Concerns[11]	Examples
	Agencies *Data Prep* *Data activation*	Intermediaries that work with brands to create, implement, and/or manage advertising and marketing activities.	See 'Brand' concerns above, plus • **Business client value,** esp. demonstrating ongoing agency value to brands	WPP, Publicis, Omnicom Group, IPG, Dentsu, Havas
Personal Device Hardware and Software Providers *Data collection* *Data prep*	**Original Equipment Manufacturers (OEMs)**	Producers and/ or packagers of the device where media is delivered. This includes manufacturers of TVs, OTT devices, and mobile or desktop devices.	• **Business Value,** incl. optimizing consumer and/or advertising monetization streams • **Compliance** as potential 1PD data collectors, 2/3PD providers • **Consumer value:** product UX, cost • **Consumer ad/privacy experience:** minimize disruption; *if applicable,* consent prompts[15]	*TVs:* Samsung, LG, Sony, Vizio, Hisense, TCL, Roku (Smart) TV, Amazon Fire (smart) TV *OTT/CTV Streaming devices:* Amazon Fire TV Stick, Chromecast, Apple TV, Roku Streaming Stick *Mobile/Desktop:* Apple, Samsung, Google, LG, Motorola (Lenovo-owned), Lenovo, HP, Dell, Asus, Acer
	Operating System (OS) Developers	Creators of the underlying device software "that enables all other software to run"[16] on a device.		*TV:* Google TV, Android TV, Roku TV, Fire TV, (LG) WebOS, (Samsung) TizenOS, Apple tvOS, SmartCast (Vizio) *Desktop:* Microsoft

[15] Many OEMs/OS manufacturers now handle enablement and collection of consumer data on devices, such as CTVs prompting users for consent during setup. These providers are the first point of media consumption so they also have the power to privacy-related policies, like standardized consent prompts or data sharing delays, which impacts downstream stakeholders.

[16] ARF-CIMM Lexicon 4.0 (2021)

Stakeholder			Description[10]	Key Concerns[11]	Examples
			OEMs can produce their own operating systems, license software from another provider, or use an open source OS.		Windows, macOS, Linux *Mobile:* Apple iOS, Google Android
	Automated Content Recognition (ACR) Service Providers[17]		Developers of identification technology that tracks TV exposure by matching audio and/or video playing on a device to a reference library. ACR software is typically incorporated into a device OS.	• **Business & business client value, costs,** esp. dependent on coverage & breadth of identifiable content • **Compliance** as 1PD collectors, 2PD providers, e.g., opt-in collection only • **Efficiency and Effectiveness:** durable data linkage for deduplication across devices, channels, and manufacturers • **Consumer value and ad experience,** such as minimal viewing disruption; simplicity and clarity of consents	Samba TV, Inscape, Nielsen Gracenote *Some OEMs – such as Samsung, LG, and Roku – offer in-house ACR solutions*
TV Distributors and Publishers Providers who deliver content to individuals or households.	**Linear-First Distributor[18]** (Traditional) Providers that transmit linear TV, many of whom have now evolved to offer digital services to offer digital services	**Broadcast Networks** *Data prep*	Distributors that use *public airwaves* to transmit no cost TV programming to viewers on a predetermined schedule.	• **Business value,** incl. optimizing advertiser and MVPD monetization • **Compliance and certifications,** e.g., VVPA • **Business client value and measurement** esp. scalability, standardization; secondary: cross-channel linkage • **Consumer value and ad experience,** such as offering quality content; ad suitability	NBC (Comcast owned), CBS (Paramount Global owned), ABC (Disney owned), Fox (Fox Corporation owned), The CW (joint ownership)

[17] AdExchanger (2023). "What TV Advertisers Need To Know About ACR In 2023"

[18] IAB UK (2021). A Guide to the Connected TV Supply Chain

Stakeholder			Description[10]	Key Concerns[11]	Examples
Advertising is one opportunity distributors/ publishers may select to monetize content.		**Multi-channel video programming distributor (MVPDs)**[19] *Data collection* *Data prep* *Data activation*	Distributors that use a *cable or satellite* to transmit TV programming to viewers on a predetermined schedule	• **Business value,** incl. optimizing consumer and/or advertising monetization • **Compliance and certifications,** e.g., VVPA • **Client value and measurement** • **Consumer value and ad experience,** e.g., offering quality content; ad suitability	Windows, macOS, Linux *Mobile:* Apple iOS, Google Android
	Advanced TV Distributors[20] Providers that transmit digital content through the internet, funded by ads, subscriptions, transactions, or a hybrid. *Data collection* *Data prep* *Data activation*	**Virtual Multichannel Video Programming Distributor (vMVPD)**	Distributors that use the *internet* to offer streaming of live linear programming AND access to video on demand (VOD) content	• **Business value,** incl. optimizing consumer and/or advertiser monetization • **Compliance and certifications** as 1PD collectors, 2/3P providers (e.g., OEM app certifications) • **Efficiency and Effectiveness:** durable data linkage across channels; granularity; scalability + standardization • **Business client value and measurement** of ad delivery/performance • **Consumer value and ad experience,** such as offering quality content; ad frequency capping; consent experience	Sling TV, Youtube TV, Hulu + Live TV, Pluto TV, PhiloTV, fuboTV, DirecTV Stream
		VOD Streaming Services	Distributors that use the internet to enable viewers to stream VOD programming "wherever and whenever they choose" versus on a predetermined schedule[21]		Ad-supported Video on Demand (AVOD) and AVOD hybrid providers include: Tubi, Youtube, Hulu (w/ Ads), Peacock, Paramount+, HBO Max, Vudu Free, Amazon Freevee, Netflix (Ad-Supported Plan), Disney+

19 ARF-CIMM Lexicon 4.0 (2021)

20 This category includes all digital video publishers. Here we focus on distributors where the primary service provided to consumers is the delivery of video content, however this category can also include more traditional digital publishers that incorporate video content into broader offerings.

21 IAB Europe Guide to the Programmatic CTV opportunity in Europe (2023)

Stakeholder		Description[10]	Key Concerns[11]	Examples
Media Marketplaces and Delivery Services *Some providers offer more than one service listed or already integrate solutions across platforms/ exchanges/ servers.*	**Demand-side platforms (DSPs)** *Data prep* *Data activation*	Software platform that facilitates the buying of ad inventory at scale. Purchases can be made directly or through an auction (the latter is typically automated).	• **Business and business client value** to maximize ROI with ad delivery and measure performance • **Compliance** among data collaboration partners as 2P/3PD users, e.g., proper consents for data sharing; granularity of data provided • **Efficiency and Effectiveness:** durable data linkage across channels; granularity; scalability + standardization of available data • **Consumer ad experience,** such as minimizing disruption (e.g., delivery speed, ad load latency)	The Trade Desk, (Google) Display & Video 360, Xandr, Adobe Advertising Cloud, Criteo
	Sell-side platforms (SSPs) *Data prep* *Data activation*	Software platform that allows publishers to manage and monetize (digital) ad inventory by connecting with ad exchanges, networks, and DSPs.		OpenX, Xandr (formerly AppNexus) Pubmatic, Google AdX (Google Ad Manager SSP)
	Ad Servers *Data prep* *Data activation*	Providers of technology that stores and delivers advertisements to end-user devices. This tool often includes management, monitoring, and reporting. Typically advertisers and publishers have ad servers.		Elemental/Adopler, Freewheel, Innovid
	Dynamic Ad Insertion (DAI) or Server-Side Ad Insertion (SSAI) Vendors *Data prep* *Data activation*	Providers of insertion technology that sits between an ad server and video player that stitches an ad and video stream together before it loads on a user's device[22]	• **Business and business client value,** e.g., increasing viewability • **Compliance** as 2/3PD users (typically rely on upstream providers for consent) • **Consumer value and experience,** such as personalization, minimizing ad delivery disruption[23]	Amagi, Amazon AWS Elemental, Brightcove, Adobe Primetime, Verizon upLynk

[22] AdExchanger (2022) AdExplainer: What Is Server-Side Ad Insertion (SSAI)

[23] IAB Europe Guide to CTV Updated (2023)

Stakeholder		Description[10]	Key Concerns[11]	Examples
	(Ad-enabled) Video Players *Data collection* *Data prep* *Data activation*	Technology that enables playback of video content and video ad creative on a user's device	• **Business and business client value and measurability:** e.g., viewability • **Compliance** as 1PD collectors (people, event, and server data) and 2P/3PD providers • **Efficiency and Effectiveness:** durable data linkage across channels; granularity; scalability • **People value and experience,** such as UX, ad load, ad controls, consents	Brightcove, JW Player, Oooyala, Video.js, BridTV
Technology & Data vendors	**Data Management Platform (DMPs)** *Data prep* *Data activation*	A data warehouse that collects, categorizes, stores, and manages people/household data (e.g., audience and purchase) from across consumer touchpoints.	• **Business and business client value:** e.g., integration coverage, quality of data • **Compliance** as 2P/3PD users/providers • **Efficiency and Effectiveness:** durable data linkage across channels; granularity; scalability; standardization of data	Nielsen, Oracle, Salesforce Audience Studio, Lotame, The TradeDesk
	Match Vendors *Data prep*	Providers of technology/ identifiers for matching consumer data across platforms or channels.	• **Business and business client value and measurability** (key use case) • **Compliance** as 2P/3PD providers • **Efficiency and Effectiveness:** durable data linkage across channels; granularity; scalability	Liveramp, Experian
	TV Planning (Traditional) *Data activation*	Intermediaries that work with brands to allocate budgets and develop strategies for advertising across channels	• **Business and advertiser value** to achieve and demonstrate maximum ROI • **Compliance** *(if applicable)*	Mediaocean, Ampersand

Stakeholder		Description[10]	Key Concerns[11]	Examples
	Consent management platforms (CMPs) *Data collection* *Data prep*	Technology that enables playback of video content and video ad creative on a user's device	• **Business and Business client value** to simplify collecting, managing, and adhering to policies • **Compliance** as 1PD collectors and collaborators, e.g., enforcing purpose use limitations • **Efficiency and Effectiveness:** data linkage insofar as it can streamline implementing a consumers' choice across touchpoints; scalability • **People value and experience** such as, simplicity and clarity of consent prompts, enforcing adherence to consent decisions across touchpoints	OneTrust, LiveRamp Privacy Manager, Quantcast, Qonsent
Measurement & Attribution Vendors[24] *Data collection* (esp. for linear TV measurement) *Data prep* *Data analysis*		Providers that help advertisers assess the performance of their advertising (e.g., verification, outcomes measurement)	• **Business and business client value and measurement,** esp. dependent on quality, accuracy, and linkage concerns. • **Efficiency and Effectiveness:** durable record linkage across 1P/2P/3P; granularity; scalability; standardization of data • **Compliance** as 1PD collectors and 2P/3PD users/providers: e.g., certifications to tag media; not collecting sensitive data for panel composition	Nielsen, iSpot, VideoAmp, Conviva, Comscore, Infosum, Samba

[24] ARF-CIMM Lexicon 4.0 (2021)

Stakeholder		Description[10]	Key Concerns[11]	Examples
Influencers, Intermed- iaries	**Industry organizations / coalitions**	Industry bodies, brands, and/or ecosystem players that join together to address industry-wide challenges such as education, adoption of new solutions, and development of standards	Focused on continuing to enable value for advertisers and consumers within the ecosystem	CIMM, 4A's, ARF, IAB Tech Lab
	Governments and Regulatory Bodies	National or regional governments that can impose restrictions and requirements for data collection, usage, and exchange	**Consumer privacy concerns** *See privacy framework for full breakdown of concerns and policies marketers need to be aware of in the US*	

Use Case Framework: Details and Stakeholders

Theme	Purpose	Use Case	Details	Stakeholders[25] who may be typically involved in enabling each use case[26]
Planning and Activation	**Targeting – Existing Customers**	1P Data	Directing ad delivery towards past customers using data they have previously shared directly with a brand.	• Advertisers • TV Distributors/Publishers • Delivery markets/services • *Technology & data vendors:* DMPs, CMPs, Match Vendors • Traditional TV planners • Personal Device Providers
		1P + 3P Data	Directing ad delivery towards past customers using a combination of data shared directly with a brand and data collected by other ecosystem players.	• Advertisers • TV Distributors/Publishers • Delivery markets/services • *Technology & data vendors:* DMPs, CMPs, Match Vendors • Traditional TV planners • Personal Device Providers
	Targeting – Prospecting	1P + 3P Data	Directing ad delivery towards new potential customers using data that has previously been shared directly with a brand and augmented with data collected by other ecosystem players. For example, this could include targeting new customers with similar profiles to existing customers or retargeting customers who have shown some interest in one's brand.	
		3P Data	Directing ad delivery towards new customers using data collected by ecosystem players external to a brand and/or by a player where one's brand does not have a direct relationship.	• TV Distributors/Publishers • Delivery markets/services • *Technology & data vendors:* DMPs, CMPs, Match Vendors • Traditional TV planners • Personal Device Providers

[25] Stakeholders include both primary stakeholders whose business value is reliant on enabling the use case and ancillary stakeholders who may be involved in data collection or collaboration, but enabling the use case is not necessarily a critical component of their business offering.

[26] Unless otherwise noted, usage of a stakeholder grouping refers to the entire class as outlined in the "Stakeholder Framework." Italicized stakeholder groupings followed by a list of specific stakeholders within that grouping indicates you should consider the entire class, but the listed stakeholders are likely most relevant for that use case.

Theme	Purpose	Use Case	Details	Stakeholders[25] who may be typically involved in enabling each use case[26]
	Targeting – Reach Extension	1P + 3P Data	When a publisher creates audiences using data they collect directly from viewers of their content and sells these audiences to be used in directing ad delivery even outside the publisher's owned and operated medium/platform.	• TV Distributors/Publishers • Delivery markets/services • *Technology & data vendors:* DMPs, CMPs, Match Vendors • Traditional TV planners • Personal Device Providers
	Suitability		Enabling media buyers to block the display of their ads alongside content that is harmful or inappropriate for one's brand.	• TV Distributors/Publishers • Measurement and attribution vendors • Delivery markets/services • Traditional TV planners • Personal Device Providers
	Campaign Activation		Variety of processes, tools, and tactics for developing, implementing, and launching advertising.	• Advertisers • TV Distributors/Publishers • Delivery markets/services • *Technology & data vendors:* DMPs, CMPs, Match Vendors • Traditional TV planners • Personal Device Providers
	Optimization		Method (automated or manual) for maximizing ad spend efficiency by tracking ad performance and making adjustments across media/channels while a campaign is live.	
	Ad Delivery/Serving		The process of delivering ads to a person through an ad server. This can include a variety of activities such as ad selection, tracking, management, reporting, and billing.	

Theme	Purpose	Use Case	Details	Stakeholders[25] who may be typically involved in enabling each use case[26]
Measurement *Metrics and currencies to assess equivalency, effectiveness, and efficiency*	**Audience Counting**	Reach, Frequency	*Reach:* measurement/metric indicating the number of people or households an ad was delivered to. Incremental reach refers to the unique, de-duplicated audience across channels. *Frequency:* measurement/metric indicating how many times, on average, an ad was delivered to a specific viewer or a household.	• Measurement & attribution vendors • *TV Distributors/Publishers:* Advanced TV, Linear-First[27] • Delivery markets/services • Personal Device Providers
		Gross Rating Point (GRP)	Measurement/metric, traditionally used for linear TV, that incorporates reach and frequency metrics to provide insight into the delivery of an ad.	• Measurement and attribution vendors • Linear-first TV Distributors
	Protection / Verification	Fraud/Security	Verification that ads were delivered to valid traffic as specified in the delivery agreement.	• Measurement & attribution vendors • *TV Distributors/Publishers:* Advanced TV • Delivery markets/services • Personal Device Providers
		Brand Safety	Evaluates if ads were delivered in a context damaging for one's brand. *See also Suitability Activation*	
	Audience Validation	Viewability	Tracking of impressions that were actually seen by users as defined by a platform's viewability standard	• Measurement & attribution vendors • *TV Distributors/Publishers:* Advanced TV • Delivery markets/services • Personal Device Providers
		In-target audience	Indicates what percentage of ad traffic was delivered to the intended/targeted audience (e.g., demographics, location).	• Advertisers • Measurement & attribution vendors • *TV Distributors/Publishers:* Advanced TV, Linear-first • Delivery markets/services • *Technology & data vendors:* DMPs, Match Vendors • Personal Device Providers

[27] Previously, audience counting of linear-TV has relied on metrics like GRP to calculate reach and frequency. Now, some measurement providers, like SambaTV, are expanding coverage of reach and frequency to linear buys.

Theme	Purpose	Use Case	Details	Stakeholders[25] who may be typically involved in enabling each use case[26]
		Attention	Measurement that aims to determine if consumers were paying attention to an ad. *How best to measure "attention" is ongoing, but currently may incorporate data from proxy metrics, like viewability, and panel-based eye tracking studies.*	• Measurement & attribution vendors • *TV Distributors/Publishers:* Advanced TV • Delivery markets/services • *Technology & data vendors:* DMPs • Personal Device Providers
	Performance / Impact	Conversion / Attribution[28]	Methods for determining if an ad (or multiple media touchpoints) drove specific business outcomes (e.g., online/offline sales, web visits, app downloads). Example solutions include: multi-touch attribution (MTA), experimentation, and market mix modeling (MMM).	• Advertisers • Measurement and attribution vendors • *TV Distributors/Publishers:* Advanced TV, Linear-first • Delivery markets/services • Match Vendors • Personal Device Providers (if applicable)
		Brand Lift	Method for determining if an ad or multiple media touchpoints drove perceptual ad or brand-related outcomes (e.g., awareness, intent, affinity).	

Privacy Framework Details

Data Input/Output Layers

Television and advertising solutions consisat of several data environments or "layers" to function within the ecosystem. For example, an operating system and device manufacturer make up different layers of the solution that enables TV advertising. Any vulnerability within one layer can have a cascading effect on others – a solution with a vulnerability in one layer is a problem for the solution as a whole. This is further complicated by the fact that each layer may be impacted differently by platform policy restrictions and subject to different privacy requirements and risk factors.

To ensure a planning, activation, or measurement solution is durable under platform policy restrictions and meets privacy regulations and policies, you must understand the impact of platform policy restrictions and ensure that each layer underlying the solution adheres to the relevant privacy requirements. Ideally, you run each data layer through the Privacy Framework. We considered the following layers in each assessment of privacy risk in the final Solutions Heatmap:

[28] Breakdowns of different attribution methodologies are addressed in the Solutions Framework.

Layer	Examples	Privacy & Data Security Implications
Hardware (Physical) Layer	Computer, smartphone, smartwatch, Internet-of-Things (IoT) devices, set-top-boxes, panel meters, CTV device	• Physical access to the device can lead to data breaches • IoT devices can continuously read information without the user's explicit knowledge • Firmware vulnerabilities can lead to unauthorized access • Hardware manufacturers may allow use, restrict or forbid access to device identifiers • Hardware manufacturers may know what users do on the device, using functionality provided by the device or within the OS controlled by it. • Hardware manufacturers may collect consented (or allowed by Terms of Service) user signals for QA and diagnostic purposes (e.g., authorizing diagnostics data to help diagnose bugs when registering a new device)
Operating System (OS) Layer	Windows, Android, iOS/tvOS, Linux, WebOS (LG), others	• OS vulnerabilities can be exploited for unauthorized access • OS-level permissions define what data apps can access • Some OSs collect telemetry data that can have some privacy implications, (e.g., user logs to inform troubleshooting and product analytics) • OS updates can change or update privacy settings, or add new ones (e.g., browser-specific functionality designed to curb or prevent IP reading) • OS-level restrictions can limit, obfuscate, or withdraw access to user data • OS layer may provide knowledge into user browsing behaviors that could provide insight into private information
Platform/ Environment Layer	Web browsers, virtual machines, Trusted-Execution Environments (TEEs), data clean rooms	• Web browsers can track user activity, store cookies and browsing history • Web browsers can obfuscate certain activity signals, blocking cross-site tracking • Containerized environments like TEEs or clean rooms can add a layer of isolation to the data, adding a layer of protection • Containerized environments like clean rooms might still accept sensitive data as inputs, and leak sensitive data as outputs • Browser plugins or extensions can access and share browsing data

Layer	Examples	Privacy & Data Security Implications
Application Layer	Emails apps, messaging apps, office suite, cloud storage apps, streaming apps	• Apps can collect user data, including location, contact details, messages and other sensitive information tied to individual app design (preferences, demographics, health, etc.) • Data shared with apps (e.g., photos uploaded to Cloud or health information can be accessed if there is a data breach) • Third-party integrations within apps can further share data • App ToS may allow the collection of specific user signals for QA and diagnostic, debugging purposes, personalized advertising, etc. • App developers may have unique visibility into content watched (e.g., streaming apps), viewing behaviors and patterns, and the actions they take.
Communication Layer	Wi-Fi, Bluetooth, NFC, cellular networks, etc,	• Unsecured Wi-Fi can lead to data interception • Devices can be tracked via their communication protocols (e.g., triangulating a device location) • Data transmitted over networks can be intercepted if not encrypted, or due to user error (e.g., sending data to the wrong recipient)
Cloud/Server Layer	Cloud storage server, application backend server, databases and APIs accessing them	• Data stored in the cloud can be accessed if not secured • Third-party cloud providers might have access to sensitive data or might be compelled by governments to release data • Server vulnerabilities can lead to large-scale data breaches • Data transmitted via APIs can be intercepted if not encrypted, API endpoints can be accessed by unauthorized users if not secured

Solutions Examples

Disclaimer: the below list is not meant to be a comprehensive representation of all technology vendors, and the solutions they provide. Examples displayed here do not constitute an implicit endorsement, nor a quality and competitive assessment of their solutions.

If you would like your company to be included, please email us at info@thinkmedium.tech.

Solution	Example
Calibration Panels	605, Comscore People Panel, iSpot TV, Nielsen ONE, TVision, etc.
Brand Lift Studies	Ipsos, Kantar, Lantana, Platform solutions (Google, Meta, Amazon DSP, Spotify), Upwave, YouGov, etc.
Conversion & Incremental Lift Studies	INCRMNTL, Google/Meta Conversion Lift tools, etc.
Multi-Touch Attribution (MTA)	Neustar Marketshare, Nielsen VisualIQ, Rockerbox, etc.
Social Media Listening	Brandwatch, Hootsuite, Sprinklr, etc.
Out-of-Home Measurement (OOH)	Clear Channel, Conversant, Outfront, TransitScreen, etc.
Contextual Advertising	Criteo Contextual, GumGum, Proximic (Comscore), etc.
Media Mix Models (MMM)	Analytic Edge, Mass Analytics, Meta Robyn (Open Source), MetricWorks, etc.
Panel-Based Ad Ratings	Comscore Campaign Ratings, Nielsen TAR/DAR, etc.
Ad Verification Solutions	DoubleVerify, Integral Ad Science, Oracle Moat, etc.
ID-Based Targeting & Identity Solutions	Blockgraph, COREID, ID5, LiveRamp (RampID), etc.
Consent Management Platforms (CMPs)	Didomi, Osano, OneTrust, Qonsent, etc.
Collaborative Data Pools	N/A – enabled via Secure Cloud & Clean Room solutions
Data Clean Rooms	Anonym, AWS Bastion, Databricks, Epsilon PeopleCloud, Habu, InfoSum, Snowflake etc.
Privacy-Forward Industry Frameworks	Apple SKAdNetwork & ITP, Google Privacy Sandbox, Meta/Mozilla IPA Proposal
Attention-Based Advertising	Adelaide, Lumen, agency services, participating DSPs e.g., TradeDesk, Avocet
Retail Media Integration	Retail Media Networks e.g., Walmart, Amazon, etc.
Data Augmentation (2nd-Party)	N/A – ad hoc dependent on use case and KPIs
Seller-Defined Audiences (SDA)	IAB Tech Lab SDA
Addressable CTV	Various delivery platforms: OTT e.g., Pluto TV, Netflix, etc.; Managed TV via telcos; ServerSide Ad Insertion

Solutions Heatmap Details

Blended Viability Score Methodology

Criteria	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Denominator (Viability Score Calculation)
Scoring Coefficient	**[1x]** *To be adjusted by readers for their specific use case(s)*	**1.5x**	**1.5x**	**1x**	**0.75x**	**4.75** *Optional: add custom Utility score to denominator*

Scoring Example 1: ***Ad Verification Solutions*** *(Baseline Without Utility)*	*N/A*	2 (Regulatory Score) * 1.5 (Coefficient) = 3	1.5 (Platform Score) * 1.5 (Coefficient) = 2.25	2.5 (Efficiency Score) * 1 (Coefficient) = 2.5	3 (Industry Score) * .75(Coefficient) = 2.25	10 (Total Score) / 4.75 (Denominator) **= 2.10 (Blended Viability Score)** **=**  (See: Viability Scoring scale)
Scoring Example 2: ***Ad Verification Solutions*** *(With Utility Score Added by Reader)*	*3 (Utility Score by Reader) * 1 (Coefficient) = 3*	2 (Regulatory Score) * 1.5 (Coefficient) = 3	1.5 (Platform Score) * 1.5 (Coefficient) = 2.25	2.5 (Efficiency Score) * 1 (Coefficient) = 2.5	3 (Industry Score) * .75 (Coefficient) = 2.25	13 (Total + Utility) / 5.75 (Denominator) **= 2.26 (New Blended Viability Score)** **=**  (See: Viability Scoring scale)

Established Solutions – Details

Use Case / Category	Solution	Description	Evolution Highlights	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Overall Viability
Measurement	**Panel-Based Ad Ratings**	Panel-based metrics used to evaluate ad campaign reach and impact in order to deliver a holistic and non-overlapping assessment of performance on TV and digital media.	TAR/DAR have been adopted by platforms (e.g., Meta, Google) to provide traditional TV measurement equivalency to brands and agencies when planning and optimizing online video campaigns. Other examples include ComScore Campaign Ratings (CCR).		29	30	31	32	
Planning/ Activation	**MVPD Addressable**	MVPD (Multichannel Video Programming Distributor) addressable TV enables advertisers to target specific ads to different viewers through a multichannel video service like cable or satellite TV, usually leveraging data from set-top boxes and ad insertion technology.			33	34	35	36	

[29] Generally not using PI, although any use of cookies and other tracking technologies in the process can still be subject to regulatory oversight.

[30] Data involved generally originates from panel participants plus extrapolation, lowering exposure to platform data and policy shifts.

[31] Supported by an established vendor ecosystem, although gaining full measurement utility from ad ratings is resource-intensive.

[32] Ratings are generally industry standard for brands investing in the TV advertising space.

[33] Generally based on aggregated audience insights and linear TV ratings not reliant on PI, although any use of cookies and other tracking technologies in the targeting process can still raise privacy concerns subject to regulatory oversight.

[34] Low overall dependency on activating based on signals and identifiers impacted by platform policies.

[35] Traditional linear TV systems often lack addressability tooling, upgrading this infrastructure can be a significant cost and technical undertaking.

[36] Dependent on region, but generally high in markets with advanced broadcasting technologies and infrastructures such as North America and Europe.

Use Case / Category	Solution	Description	Evolution Highlights	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Overall Viability
Measurement	**Brand Lift Studies**	Research analyses to measure the effectiveness of an advertising campaign via metrics like ad recall, brand lift, purchase intent through pre- and post-campaign surveys and experiments.	Brand lift experiment tools have been built directly into ad UIs by major ad platforms, DSPs and Retail Media Networks to facilitate experimentation.		37	38	39	40	
Planning/ Activation	**Private Marketplaces (PMPs) – Data at SSP Level**	Exclusive digital ad inventory marketplaces where advertisers bid on premium inventory from publishers. Solutions with data at SSP level use publisher-side data to optimize inventory and pricing, focusing on maximizing the value of publisher assets.			41	42	43	44	

[37] Generally offer aggregate awareness signals based on polling results without reporting on individual users – not a high-scrutiny regulatory area.

[38] Platform-driven signal loss might impact experiments and lift reading accuracy (blind to certain users/devices), but can still get access to addressable inventory.

[39] Usually integrated into platform and vendor UIs, but prone to set up errors (limited sample, short duration, etc.) increasing cost and affecting accuracy.

[40] Widespread use by brands, agencies and offered as a measurement tool by most large platforms/ad networks and built into agency services

[41] SSPs acting as facilitators of publisher inventory sales requires caution about data passed in the bid stream, advertisers using 1P data.

[42] SSP involvement in leveraging data capabilities, and the implied cross-publisher data pooling create higher risk of affect by platform policies.

[43] Generally more complex to utilize than open market RTB, due to several implied factors – setup, negotiation, tech integration, price/inventory control, etc.

[44] PMPs as a whole are on the rise as of 2023, given industry shifts and added focus on transparency and quality.

Use Case / Category	Solution	Description	Evolution Highlights	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Overall Viability
Planning/ Activation	**Private Marketplaces (PMPs) – Data at Ad Server Level**	In contrast to the above, this flavor of PMP utilizes data from the ad server to incorporate both publisher and advertiser insights, allowing for targeted and efficient ad placements.			45	46	47	48	
Measurement	**Conversion & Incremental Lift Studies**	Ensemble of approaches to evidence the sales and ROAS impact of specific campaigns, tactics and channels, by demonstrating conversion outcomes and/or statistically-significant conversion lift versus BAU.			49	50	51	52	

[45] In this scenario utilizing data at the ad server level, tighter integration of first-party data provides additional regulatory scrutiny durability.

[46] Given integration at the ad server level, there is more direct alignment with the publisher's first-party audience data and less intermediation in the process.

[47] See: PMP at SSP level footnote (34)

[48] See: PMP at SSP level footnote (35)

[49] Test/control data for experiments requires an understanding of users, which can be negatively impacted by disappearing device ids, cookies and other signals.

[50] Similar to 39 (Brand Lift Studies)

[51] Well-supported in platform tooling and ad tech vendor functionality, but complex to execute at scale and without experiment errors.

[52] Widely adopted in the advertising industry, although generally by larger brands and agencies with sufficient resources for orchestration and analysis.

Use Case / Category	Solution	Description	Evolution Highlights	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Overall Viability
Multi-Use	**Media Mix Models (MMM)**	Statistical analysis technique used to quantify the impact of various marketing inputs and "priors" (pre-existing historical insights) on sales or other performance indicators across marketing channels.	MMM has been augmented with **Geo-Lift calibration** to more accurately represent incrementality while reducing click/ view/sales data needed to design and run experiments, benefitting privacy.		53	54	55	56	
Measurement	**Multi-Touch Attribution (MTA)**	Method used to evaluate the impact of each touchpoint in a customer's journey towards a conversion, generally achieved by deduplicating outcomes from each marketing channel through cross-device tracking and identity resolution to get a more accurate view of their relative contribution.	MTA has evolved alongside regulations and recent industry shifts affecting identifiers needed to deduplicate conversions. **Data use is different between MTA digital-only, and when factoring-in linear TV.**		57	58	59	60	

[53] Generally not reliant on PI and user-level data for model inputs, lessening the risk of regulator scrutiny and one of the strengths of this approach.

[54] Platform policies curb availability and utility of data fed to media mix models, thus possibly affecting accuracy. Platforms offer their own MMM pipelines.

[55] Reliant on data science expertise and quality data inputs, lighter and faster approaches have been developed recently (incl. by specialized vendors).

[56] Historically a landmark solution in measurement toolboxes, recognized for its go-forward durability.

[57] Highly dependent on cross-device identifiers for deduplication e.g., accuracy; regulators weary of cross-device tracking and use with some requiring user choice.

[58] Data required for MTA (especially by 3rd parties) viewed by platforms as linking profiles, most affected by signal loss (ex: last-touch attribution vendors).

[59] Usually high technological and vendor overhead; costly to implement; affected by privacy-related regulation and new platform policies re: identifiers.

[60] High adoption in certain verticals (Gaming, Ecommerce), client segments (Enterprise) and by mobile app developers, though future is in question.

Use Case / Category	Solution	Description	Evolution Highlights	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Overall Viability
Multi-Use	**Ad Verification Solutions**	Solutions and tools designed to independently assess the viewability and suitability of ad impressions ("post-bid"), validating that ads reached the intended target demographics or geos and didn't appear alongside sensitive content, and take remedial action based on those insights ("pre-bid" or optimization).	Third-party verification vendors are increasingly linking post-bid verification with pre-bid optimization (including based on **Attention**), and developing data augmentation applications with verification signals. Can also enable Contextual analysis and targeting based on impression-level placement data.		61	62	63	64	
Measurement	**Social Media Listening**	As defined here, referring to social media monitoring and linkage with other channel outcomes in order to gain holistic insights into campaign effectiveness, by connecting social mentions and other signals with TV campaigns.	AI evolutions provide additional tools to analyze data at scale and identify 2nd-screen engagement patterns.		65	66	67	68	

[61] Most verification data is at impression-level without PI, however applications based on verification data may rely on IP, user agent and thus under scrutiny.

[62] Platform policies aiming to curb IP access/use affect any data marrying/augmentation to pair verification with outcomes. Sensitiveness to data access by 3Ps.

[63] Deployment and overall operation is primarily reliant on established technology vendors, with onboarding incl. pixeling and other actions needed to enable.

[64] Generally well-represented and accredited by various industry bodies, especially at the top end (large advertisers).

[65] Performed in similar fashion to MTA to reconcile devices around a single user and measure 2nd-screen behavior – affected by similar privacy scrutiny.

[66] Platform policies aim to specifically curb the type of user profile reconciliation required to enable social media listening (stitching TV viewership to devices where social posts occur).

[67] Only achievable at-scale via specialized vendors with dedicated API integrations and pattern/language analysis capabilities.

[68] Many large advertisers use forms of social media listening to support national brand campaign activations and gauge their impact.

Use Case / Category	Solution	Description	Evolution Highlights	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Overall Viability
Multi-Use	**IVT Solutions (Fraud)**	Solutions and tools designed to detect and prevent invalid traffic (IVT), such as bots and fraudulent clicks, ensuring genuine user engagement and protecting advertising spend.			69	70	71	72	
Measurement	**Out-of-Home Measurement (OOH)**	TV viewership measurement solutions to gauge the effectiveness of ads served in public ("out-of-home") locations e.g., bars, restaurants, gyms.	Solutions like Tunity address challenges such as public locations often having muted TV with sound off for reporting purposes.		73	74	75	76	
Planning/ Activation	**Digital & Programmatic OOH**	Distinct OOH activation solutions designed to offer access to targeting and reach extension into out-of-home networks and locations at scale.	**Digital Out-Of-Home (DOOH)** offers programmatic activation capabilities.		77	78	79	80	

[69] Regulators are generally open to exceptions and carve-outs to allow continued protection against online fraud and criminals.
[70] Platform policies aiming to curb IP access/use directly affect IVT solutions utility, which are reliant on that signal to identify fraud patterns.
[71] Enabled by an established vendor ecosystem, but can be complex to deploy, consistently monitor and take action on insights.
[72] Generally a well-established industry solution category with relatively unambiguous standards to define online fraud.
[73] Generally, OOH signals are not at the person-level e.g., no PI involved; as it moves to digital, could eventually enable person-level tracking (higher risk).
[74] Main concern lies with the geo-based component and related signals needed to get measurement utility, which can get affected by platforms.
[75] Turnkey solutions exist for access to OOH locations for measurement, but location scouting and ROI reporting requirements can complicate adoption.
[76] Inherently a niche solution encompassing OOH placements only, but part of a well-established category available to advertisers who wish to activate.
[77] Similar to the distinct measurement component, generally not reliant on PI so less affected by regulatory scrutiny.
[78] See: OOH item above – Main concern lies with the geo-based component and related signals needed to get activation utility.
[79] Digital OOH has programmatic capabilities, allowing advertisers to dynamically launch and adjust campaigns based on various data triggers.
[80] Compared to OOH measurement, deploying DOOH will typically require more technology integrations e.g., to enable dynamic real-time content.

Use Case / Category	Solution	Description	Evolution Highlights	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Overall Viability
Multi-Use	**ID-Based Targeting**	Solutions enabling the identification of individuals or households across digital spaces for targeted advertising. Traditionally dependent on third-party cookies and device IDs, now adapting to new regulations and platform policies.	The changing identity landscape has spurred ID solutions to adopt new, privacy-conscious signals for user identification, moving beyond third-party cookies and device IDs for future resilience.		81	82	83	84	
Planning/ Activation	**Contextual Advertising**	Solutions designed to place ads based on the content being viewed, instead of known user behavioral data and profiles. This method respects user privacy by not relying on personal data for ad targeting.	**"Contextual 2.0"** is an evolution of traditional Contextual, where placement context is parsed programmatically to inform delivery in real-time, which can be further enhanced by AI.		85	86	87	88	

[81] At risk due to privacy regulations, though the use of PETs, clean rooms and consent strategies might play a role in future durability.

[82] Dependent on enabling solution and party's structural position to user (e.g., advertiser may not be able to activate consented data if can't access user signal).

[83] ID-based targeting benefits from a robust ecosystem of relatively turnkey vendor solutions, but deploying them effectively requires significant overhead.

[84] Broad industry adoption within the digital space, from in-house paid media teams to agencies and specialized vendors focused on optimization.

[85] Not reliant on pixel/cookie PI data or sensitive behavioral data and as such should generally be privacy-friendly in the eye of regulators.

[86] Basic contextual solutions are lower risk, although pooled approaches create more potential platform risks – possible (separate) commercial interest risk.

[87] Supported by established tech solutions e.g., verification vendors, but can be challenging to operate: high CPA, targeting imprecision, inventory limitations.

[88] Industry adoption of Contextual Advertising has been on a rising trajectory, especially as the industry moves towards more privacy-centric advertising.

Use Case / Category	Solution	Description	Evolution Highlights	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Overall Viability
Multi-Use	**Collaborative Data Pools**	Bespoke environments where viewer data from several participants such as broadcasters and advertisers is pooled in aggregate, anonymized, then shared among the group to improve audience targeting and ad effectiveness by augmenting their respective insights.	In some ways, Data Clean Rooms are an evolution of collaborative data pools, or in any case, play a key role in operationalizing them.		89	90	91	92	
Planning/ Activation	**Addressable CTV**	Solutions to deliver targeted ads at scale to specific viewers using internet-connected television devices, enabling personalization, often by employing programmatic technology in CTV context.			93	94	95	96	

[89] Theoretically secure, but inherently dependent on data security frameworks and enabling technology underneath. Power asymmetries to consider.

[90] Likely low platform appetite for pooled data frameworks, likely to place scrutiny and/or additional demands on participants.

[91] Inherently limited to participants and requiring significant partnerships and legal legwork to deliver utility, but select vendors can help facilitate deployment.

[92] Gaining interest as of 2023, but adoption is dependent on industry, overall nascent compared to more established data management and analytics technologies.

[93] Addressable CTV relies on granular data and signals to inform ad delivery and personalization, reaching into possible regulatory scrutiny territory (e.g., VPPA).

[94] Real-time audience segmentation and tailored ads typically require data points on which platform policies can have a significant curbing impact.

[95] Turnkey solutions exist to programmatically activate on CTV with relatively minimal setup requirements.

[96] Adoption is significantly growing as of 2023, driven by a combination of factors: growth in CTV viewership, targeting/personalization capabilities.

Emerging Solutions – Details

Use Case / Category	Solution	Description	Evolution Highlights	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Overall Viability
Multi-Use	**Consent Management Platforms (CMPs)**	Solutions and tools helping advertisers and publishers manage data collection consent and transparency, assisting with compliance in data used for targeted advertising. The category has been growing with the advent of GDPR, CCPA and other regulation frameworks.	Various CMPs have developed automated diagnosis solutions for brands, publishers to gauge compliance levels across environments and involved parties.		97	98	99	100	

[97] CMPs are key to consent strategies, but are only as good as how they are implemented and thus do not guarantee compliance in themselves. Regulators are also skeptical of whether consent can be obtained for thousands of parties in the programmatic ecosystem or whether a user understands use cases it opts out of (vs. use cases that continue post-opt out).

[98] Platforms can act as gatekeepers in consent optimization levers available e.g., Apple App Store's consent incentivization app guidelines.

[99] Major CMPs have invested in built-in consent popup builders and other turnkey functionality to facilitate roll out at scale, with built-in UI designers, etc.

[100] Adoption has become increasingly common among businesses that operate online, especially in regions with a higher data privacy regulation bar.

Use Case / Category	Solution	Description	Evolution Highlights	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Overall Viability
Multi-Use	**Data Clean Rooms**	Computing environment where participants can join and/or access granular or aggregated data without revealing individual PI, allowing analysis. Although designed and marketed to enhance data security and privacy, they do so at varying degrees (dependent on underlying designs and PETs), and are still bound to privacy requirements.	Data Clean Rooms are fast evolving in adoption level, applications, standards, and level of industry interoperability. Computing costs remain a concern, joining data sets in the current platform policy (restricted cookies & identifiers) and regulatory (new definitions of PI) environments creates a risk of low match rate.		101	102	103	104	
Multi-Use	**Privacy-Forward Industry Frameworks**	Proprietary platform-owned attribution frameworks designed to be privacy-forward and improve data use defensibility in light of leaks and increased regulatory scrutiny.	SKAdNetwork's imperfect signals have increasingly been integrated into platform modeling to enhance ML-driven ad ranking and delivery. Google Privacy Sandbox is another landmark platform framework.		105	106	107	108	

[101] Most clean rooms offer strong data security and technical (vs. contractual) control over use cases, access and sharing , but inputs are typically still PI and use cases still require careful evaluation. Mistakenly approaching clean rooms as inherently private can create significant risk.

[102] Implicit platform recognition of clean rooms' potential utility in the ecosystem, e.g., several have developed their own and/or integrated 3P clean rooms.

[103] High technological overhead and computing costs, disparate industry standards, fragmented vendor landscape (but improving with rising interoperability).

[104] Industry consensus about clean room utility and potential (source: stakeholder interviews) – Google, SambaTV, GroupM, etc. though standards still emerging.

[105] Caveat that while these frameworks leverage privacy-forward techniques, underlying platform owners themselves aren't immune to regulatory scrutiny.

[106] Promoted by platform themselves, although there is risk in said frameworks suddenly evolving e.g., previously-available data withheld, API changes, etc.

[107] Despite turnkey APIs and generally scalable data availability, incidents are still frequent and ad tech integration/utility remains a challenge.

[108] As of 2023, SKAN is increasingly used as a signal source by platforms and advertisers, and Google is engaging various ecosystem participants for Sandbox.

Use Case / Category	Solution	Description	Evolution Highlights	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Overall Viability
Planning/ Activation	**Contextual 2.0 (ML-Enabled)**	Emerging form of Contextual leveraging Machine Learning (ML) to parse content at scale and serve ads accordingly. Placement context is interpreted programmatically to inform delivery in real-time.			109	110	111	112	
Multi-Use	**Customer Data Platforms (CDPs)**	Solutions and tools that help advertisers and publishers collect, centralize and analyze customer data (primarily first-party data) from various sources to enable personalized interactions, efficiency improvements and other insights.			113	114	115	116	

109 By definition leveraging aggregated contextual data points that do not involve PI, though any ML-based content scraping might get regulator attention.
110 Not relying on PI for inputs provides added durability to platform policies, although reaching an audience based on such signals is not immune.
111 Reliance on machine learning provides additional scalability.
112 As reflected by its name, "Contextual 2.0" is an emerging solution on a rising trajectory, but from a low user base with standards still being updated.
113 1P data = lower risk but VPPA and other regulations come into play with sharing. Plus technical deployment challenge.
114 Additional challenges deploying first-party data from CDP pipelines in light of shifting platform policies.
115 Data integration and flows implied in CDP deployment are a non-trivial technical undertaking for most organizations.
116 CDPs are reaching significant adoption, especially by larger organizations investing in further data-driven decision-making and in light of 1P data utility.

Use Case / Category	Solution	Description	Evolution Highlights	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Overall Viability
Planning/ Activation	**Seller-Defined Audiences (SDA)**	Solution based on IAB standards and designed to help publishers monetize their first-party data by creating audience cohorts that can then be passed on to demand partners (i.e. DSPs) via the OpenRTB protocol and Prebid. Privacy-friendly alternative to ID-based audience targeting.			117	118	119	120	
Planning/ Activation	**Attention-Based Advertising**	Solutions and tools that leverage a read of consumer attention obtained via ad interaction analysis *(what the consumer is viewing, where, for how long),* as a signal to help advertisers and tech providers develop more effective ads planning and delivery optimization.	AI-based models help render Attention-based measurement and optimization more actionable, faster. Can be a challenging signal to plan or optimize for, as the relationship between creative, attention and sales outcomes is inconsistent and lacks standardized definitions.		121	122	123	124	

117 SDAs work off of anonymized first-party data sets and cohorting, ensuring a high level of baseline durability to privacy regulations.
118 Dependent on data use cases and deployment, could still get impacted by platform-driven signal loss.
119 Still-nascent ecosystem integration and adoption means a limited scope of supporting vendors and ecosystem participants for the time being.
120 First proposed in March 2021, as such still in early industry evaluation and adoption phase.
121 Attention signals are collected at impression/ad-level (without exposing users), but Attention-based activation requires data linking, which carries privacy risk.
122 Activation and optimization based on Attention signals might go to the user level, creating additional vulnerability to shifting platform policies.
123 Various solutions are working on integrating Attention signals for advertising, but Attention-based actionability as a standalone KPI/metric remains a challenge.
124 *"[Attention is generating interest], However, while [its] theoretical benefits [...] are well understood, it is less clear how media buyers are capitalizing [today]"*

Use Case / Category	Solution	Description	Evolution Highlights	Utility	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Adoption	Overall Viability
Planning/ Activation	**Retail Media Network Integration**	Solutions and tools that let advertising ecosystem participants integrate with Retailer platforms to gain advertising opportunities through a more effective understanding of consumers, and more effective targeting based on their shopping behavior and preferences.	Most large online retailers have recently built, or are in the process of building their retail media offering. Notable concern with their inherently closed-loop nature, although the use of solutions like Clean Rooms can help facilitate insights reporting and broader ecosystem integration.		125	126	127	128	
Multi-Use	**Data Augmentation Partnerships (2nd-Party)**	Solutions based on data collected by one entity (responsible for ensuring security and consent) that is then shared or sold to another entity directly, typically for enhancing marketing efforts and ad targeting.			129	130	131	132	

[125] RMNs generally mobilize first-party consented user data to offer advertising services, although this process isn't immune to regulatory concerns.
[126] Platform-related signal loss can directly affect measurement visibility into, and integration with RMN data.
[127] Large RMNs like Walmart Connect offer turnkey onboarding and started integrating into the vendor ecosystem, but haven't reached broad self-service functionality.
[128] Amazon, Walmart, and new entrants are growing rapidly (~2x other online channels), but still #4 behind Search, Social, TV; primarily adopted by large brands.
[129] Inherently falling within the realm of data (re)sales, which under specific regulation frameworks might de facto be problematic.
[130] Can inherently fall under scope of platform policy shifts given data stitching processes involved.
[131] Requires sophisticated data integration technology and a robust contractual & legal framework to be viable.
[132] Widely adopted by major technology companies, platforms, and Fortune 500 advertisers.

Enabling Technologies & Techniques – Details

Use Case / Category	Technology or Technique	Description	Related Solutions	Evolution Highlights	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Standardization	Overall Viability
Multi-Use	**AI/ML Conversion Modeling**	Advanced attribution models using AI combined with statistical modeling and other techniques to determine when an ad was seen and led to a specific conversion, in absence of direct (deterministic) signals e.g. due to cookie and MAID restrictions.	• Conversion Modeling is increasingly built into any measurement or targeting solution that previously relied on deterministic data now less available as a result of platform policy shifts.	Modeling is on the rise to fill gaps in attribution from signal loss (cookie, device identifiers no longer available), assisted by AI	133	134	135	136	

[133] Reliant on statistical models theoretically resilient in the face of signal loss, though still dependent on a layer of deterministic data.

[134] Data feeding into models, which is often user-level is still bound to shifting platform policies that may reduce available signals.

[135] Turnkey solutions exist (custom bidding, platform-owned – Google modeled conversion) but require large data sets and actionability can be a challenge.

[136] Widely adopted in the media and tech industry (e-commerce, SaaS, etc.), accelerated adoption by ad networks due to privacy and industry shifts since 2021.

Use Case / Category	Technology or Technique	Description	Related Solutions	Evolution Highlights	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Standardization	Overall Viability
Measurement	**Statistical Sampling (Panels)**	Technique used to extrapolate viewing behaviors, preferences, and trends of a larger population, based on data obtained from households equipped with measurement devices, to aid in the optimization of advertising strategies.	• Panels	As primarily a probabilistic measurement approach, statistical sampling is generally more durable to regulatory and platform shifts.	137	138	139	140	
Measurement	**Set-Top Box Data (STB)**	Second-by-second household viewership data collected by cable providers, providing additional granularity over linear TV measurement. STBs enable content from cable/satellite to be displayed on TV.	• Panels • Attribution/ Conversion Modeling • Cross-Channel Measurement	STBs have evolved from cable-based & provided, to Smart Internet STBs (OTT Smart TV Box e.g., Apple TV) reflecting the shift away from cable TV.	141	142	143	144	

[137] Meters require explicit user/household consent, statistical sampling is inherently probabilistic – high regulatory defensibility.
[138] Seed data collected via meters is generally resilient to platform policy shifts.
[139] Mostly low efficiency and high-cost due to reliance on metering, which requires careful sampling and household outreach.
[140] Historically the preferred traditional TV measurement approach and standard, highly standardized as a result.
[141] Theoretically with the ability to get consent / provide transparency. However, leaks and data sales are possible issues. Could combine with other account data.
[142] STB data collection inherently captures individual information, including PI signals being curbed, but platforms have low gatekeeping oversight on the process.
[143] Coverage limited by hardware adoption/purchases and deployment, cost considerations as barrier to entry.
[144] Highly standardized in context of TV measurement, though contingent on specific hardware and thus not a holistic solution.

Use Case / Category	Technology or Technique	Description	Related Solutions	Evolution Highlights	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Standardization	Overall Viability
Measurement	**Calibration Panels**	Panels track trends and opinions over time from selected respondents, commonly for monitoring TV and video viewership. This involves using devices like People Meters in sampled households to represent the broader population.	• MMM • Ad Ratings • Modeling	Panels have evolved to offer more precise, currency-grade data, providing detailed insights and serving as a **calibration tool within broader big data measurement strategies.** Attention-based panels e.g., TVision.	145	146	147	148	

[145] Only opt-in participants; usually not person-level; layer of statistical analysis performed to extrapolate insights from sample, lower regulatory scrutiny.
[146] Minimal platform policy shift impact on the future-looking durability of panels, given tooling, enablers, and statistical sampling approach.
[147] Historically low: dependency on sizable panel pools for statistical analysis, STB footprint, high non-response rates – overall scalability challenge.
[148] Historically the linear TV measurement standard, indicating a high level of adoption and standardization.

Use Case / Category	Technology or Technique	Description	Related Solutions	Evolution Highlights	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Standardization	Overall Viability
Measurement	**Automatic Content Recognition (ACR)**	Technology allowing automated recognition of data usually sourced from Smart TVs, tracking what content and ads are being viewed in real-time. Involved watermarking & Acoustic Fingerprinting for the audio recognition component.	• OOT solutions • Ad Ratings	Examples: Samba TV, Shazam, Inscape, Nielsen DAR (which has an ACR component option)	149	150	151	152	
Multi-Use	**Content Tagging & IDs**	Content tagging & IDs facilitate precise tracking and targeting of TV and video content, enhancing measurement accuracy and enabling tailored audience activation.	• Any measurement solution • CDPs • Addressable TV (at large)	ACR (see above), as a more passive enabling technology version of proactive content tagging	153	154	155	156	

[149] SambaTV interview: "ACR data 100% opt-in, SambaTV is 1P owner" – however any title content paired with Personal Information (PI) creates risk (see VPPA).
[150] Recognition technology provides data and isn't directly affected by platform policies, but platforms could still take steps to curb applications with said data.
[151] ACR is serviced by an established roster of vendors, however deployment is complex across infrastructure requirements, QA, monitoring, and compliance.
[152] Well-adopted by major publishers and as an enabling technology solution by advertisers for measurement purposes via leading market providers.
[153] Tagging content as a standalone practice has no adverse regulatory implications, however any content title paired with PI risks VPPA infringement in the US.
[154] API availability to platform content metadata creates potential risks to the tagging process, and its accuracy.
[155] Vendor solutions that facilitate/automate content tagging exist, however, in many organizations it remains a manual process (due to lack of resources, etc.).
[156] Widely adopted practice in the TV advertising space, although standardized definitions can vary and pose a challenge for consistency across vendors.

Use Case / Category	Technology or Technique	Description	Related Solutions	Evolution Highlights	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Standardization	Overall Viability
Multi-Use	**CTV/OTT SDKs & Analytics**	Software Development Kits (SDKs) Integrated into apps e.g. Roku, FireTV, etc. are key to enabling various advertising-related use cases: Fraud, Identity resolution, Consent management, Sandbox/On-device processing, Attribution insights, etc. by tracking and storing app interaction signals.	• Any measurement solution with a mobile & CTV component • Targeting solutions e.g. powering retargeting • Fraud prevention • MTA • Consent Management	Examples: Android SDK, Unity, AppsFlyer, Google Firebase, Meta SDK, OneSignal (push notifications)	157	158	159	160	

[157] Dependent on SDK implementation: can be configured to be fully compliant, but often capture device parameters that might cause regulatory scrutiny.

[158] 3rd-party SDKs are generally highly scrutinized by platforms as a possible liability risk (e.g., SDKs in kids apps, Apple App Store policies).

[159] SDKs are industry standard, but technical implementation usually requires coding – though no-code options and ample documentation exists.

[160] Widely-accepted industry standard within the mobile app ecosystem, equivalent to web pixels.

Use Case / Category	Technology or Technique	Description	Related Solutions	Evolution Highlights	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Standardization	Overall Viability
Planning/ Activation	**First-Party Data Activation**	Process of collecting and mobilizing first-party data to power and enhance targeted ad solutions, without relying or infringing on external data sources. Marrying First-Party Data with other data sets and vendor 3rd-Party data to augment audience and performance measurement has additional privacy implications.	• Most measurement solutions • Activation solutions, either direct or via data augmentation and partnerships		161	162	163	164	
Planning/ Activation	**Server-Side Ad Insertion (DAI/SSAI)**	Technology that customizes ads and stitches them seamlessly into a single video stream, enabling dynamic content personalization and instantaneous load times in a video advertising context (e.g. CTV).	• Addressable CTV		165	166	167	168	

[161] Generally considered privacy-forward as it's collected with consent at the source, however ultimate compliance depends on which data was collected, and how.
[162] First-party data, while collected directly by an organization from its audience, isn't immune to platform policy compliance e.g. adherence to collection rules, etc.
[163] Dependent on usage: easy to leverage by original data collectors, but higher friction for 3rd parties aiming to marry it with their own data sets.
[164] The adoption of first-party data solutions has been gaining traction, especially since 2018 with the introduction of GDPR and Apple's ITP.
[165] While SSAI can function without mobile identifiers, many implementations use them to personalize ad delivery and report on ad views. See VPPA concerns.
[166] Dependency on platform policy regarding device IDs, but platforms may not have as much gatekeeping power for CTV devices.
[167] SSAI is a sophisticated technology with many integration, content preparation, compatibility, QA, and monitoring requirements for successful implementation.
[168] SSAI remains a relatively emerging technology; streaming technologies and protocols (like HLS, DASH) evolve and SSAI solutions need to stay updated.

Use Case / Category	Technology or Technique	Description	Related Solutions	Evolution Highlights	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Standardization	Overall Viability
Planning/ Activation	**Privacy-Enhancing Techniques**	Mathematical frameworks utilized for the obfuscation, encryption and/ or noise injection into sensitive and personal data. Can provide additional privacy guarantees by allowing data to be analyzed without revealing sensitive information about any individual in a dataset. **Examples: Differential privacy (DP), Homomorphic Encryption (HE), Private-Set Intersection (PSI).**	• Measurement and Activation solutions	Increasingly deployed by platforms and AdTech to add privacy guarantees to data analysis. A key concern is preserving measurement/ activation utility (ensuring accuracy) despite the inherent obfuscation of individual data.	169	170	171	172	

[169] By adding noise into sensitive data sets, ensures no exact value can be pinpointed, protecting (with mathematical guarantees) anonymity of individuals within.
[170] In-use by platforms themselves, using DP can facilitate compliance with platform policies – but not 100% immune to human error and misuse.
[171] Requires data science / privacy engineering expertise to implement, though various vendor solutions and open-source resources are available.
[172] Based on well-documented research and principles, however, utility and standards for planning and activation use cases are still being refined.

Use Case / Category	Technology or Technique	Description	Related Solutions	Evolution Highlights	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Standardization	Overall Viability
Planning/ Activation	**Privacy-Enhancing Technologies**	Ensemble of technologies that allow the storage, analysis, matching of data for advertising purposes e.g. targeted ads, in a way that doesn't expose individual PI to any of the involved parties. **Examples: Secure Multi-Party Computation (sMPC), Trusted-Execution Environments (TEEs), etc.**	• Mainly Activation solutions	Increasingly used by platforms to securely gain access to sensitive advertiser data for ML training, and in the context of Data Clean Rooms for data sharing. Supported by IPA and Apple's PAM	173	174	175	176	

[173] Enables different parties to work together to obtain a result, without learning anything about each other's inputs apart from what can be inferred from the result.
[174] Powers certain platform integrations and applications, can support deploying clean rooms, not 100% immune to error and leakage.
[175] While TEEs and particularly sMPC offer strong privacy guarantees, their deployment complexity, computation cost, and other overhead, have limited adoption.
[176] Increasingly being deployed in the media and advertising space, in context of clean room integrations and deployed by platforms to offer secure lift analysis.

Use Case / Category	Technology or Technique	Description	Related Solutions	Evolution Highlights	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Standardization	Overall Viability
Multi-Use	**Zero-Trust Frameworks (incl. Blockchain)**	Zero Trust describes security frameworks requiring all users inside/outside an organization to be authenticated, authorized, and continuously validated before being granted or keeping access to data. Using blockchains can bring an additional layer of security if executed properly.			177	178	179	180	

[177] Enables different parties to work together to obtain a result, without learning anything about each other's inputs apart from what can be inferred from the result.
[178] Powers certain platform integrations and applications, can support deploying clean rooms, not 100% immune to error and leakage.
[179] While TEEs and particularly sMPC offer strong privacy guarantees, their deployment complexity, computation cost, and other overhead, have limited adoption.
[180] Increasingly being deployed in the media and advertising space, in context of clean room integrations and deployed by platforms to offer secure lift analysis.

Use Case / Category	Technology or Technique	Description	Related Solutions	Evolution Highlights	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Standardization	Overall Viability
Multi-Use	**Identity Solutions**	ID solutions allow AdTech companies to identify users across different websites and devices, by creating deterministic profiles of known users and their interactions. Universal IDs can be created using probabilistic data (e.g., IP address, browser type and model, and user-agent string) or deterministic data (e.g., an email address or phone number), or both, to produce an ID while abiding by regulations and policies.	• Involved in many emerging flavors of targeting solutions	Rising in response to third-party cookie/ID deprecation, but raise similar privacy concerns and generally have lower match rates due to ecosystem fragmentation (number of participants in each solution)	181	182	183	184	

[181] User/device identifiers have been a primary focus of regulatory action since GDPR was enacted; universal ID solutions aren't immune to regulatory scrutiny.
[182] Universal IDs attempt to remedy platform shifts (e.g., cookie deprecation). Can be more resilient when combined with 1P data, but scrutiny will be significant.
[183] Established solutions exist facilitation adoption, however identity graphs and their required data marrying are inherently complex and costly to integrate.
[184] Various vendor solutions compete, with different approaches and security guarantees leading to a level of standards fragmentation.

Use Case / Category	Technology or Technique	Description	Related Solutions	Evolution Highlights	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Standardization	Overall Viability
Measurement	**Sentiment Analysis**	Solutions leveraging machine learning and natural language processing to parse consumer reactions to ad campaigns and brands across specific properties e.g. social media comments, then develop user sentiment reports to help gauge their effectiveness.	• Social Media Listening	Further evolution potential enabled by the rise of more powerful AI models to detect patterns.	185	186	187	188	
Multi-Use	**Privacy Controls Device/ Platform/ Provider Level**	Tools and settings that can be implemented by device manufacturers, platform providers, and service providers to offer users better control managing and protecting their data and privacy.	• CMPs • CDPs • Any targeting solution		189	190	191	192	

[185] Leverages increasingly powerful AI/ML to analyze sentiment expressed in social posts and ads, generally no requiring individual user data as inputs.
[186] Sentiment input data is generally readily available via platform APIs, though it inherently isn't immune to future shifts.
[187] Parsing and automation can be obtained through specialized vendors, but taking optimization action beyond sentiment readings is generally challenging.
[188] Sentiment analysis is an established approach, but application of insights it generates are varied and can lack standards.
[189] Inherently a privacy-oriented feature, allowing consumers to set their privacy preferences, including opt-in and out and data deletion at various levels.
[190] Generally intersects with platform interests to implement and ensure transparency and control.
[191] Dependent on app and site portfolio, implementation can scale from straightforward to complex for large publishers with many properties (for instance).
[192] Generally supported by well-defined industry standards and regulatory literature, adopted by many large advertisers, publishers, platforms.

Use Case / Category	Technology or Technique	Description	Related Solutions	Evolution Highlights	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Standardization	Overall Viability
Planning/ Activation	**On-Device Segmentation and Auction**	Process where data required for audience segmentation and ad auctions is kept and processed strictly on the user's device (with the device effectively acting as a TEE of sorts), to prevent any leakage or exposure of the underlying user data.	• Platform Privacy-Oriented Frameworks e.g. Google Privacy Sandbox		193	194	195	196	
Planning/ Activation	**Trusted-Execution Environments (TEE)**	Any intentionally isolated hardware or software environment dedicated to secure data processing, to prevent data leakage to unauthorized parties.			197	198	199	200	

[193] Processing any sensitive data on-device to prevent leakage, protecting privacy. Regulators may have questions but are open to being convinced of protections.
[194] Process is reliant on platform allowance or performed by platforms themselves, which can opt to limit APIs and scope of applications in the future.
[195] Emerging technique with numerous work-in-progress activation use cases and best practices.
[196] Standards still emerging and advertising utility being evaluated by publishers and advertisers (e.g., technique involved in Google PAIR).
[197] Segregated environments for computation to preserve security (on-device, such as employed in Google's PAAPI is a form of TEE).
[198] Generally an emerging, preferred platform technique although access durability to outputs raises future questions.
[199] Likely computationally-intensive and costly to leverage, due the additional layer of data in and out processing with the TEEs.
[200] Emerging with still relatively minimal ecosystem adoption.

Use Case / Category	Technology or Technique	Description	Related Solutions	Evolution Highlights	Regulatory Scrutiny Risk	Platform Policy Risk	Efficiency – Deployment & Operation	Industry Standardization	Overall Viability
Measurement	**Surveys**	Process of gathering direct feedback from specific audiences (consumers, households, groups), helping brands understand consumer preferences, campaign outcomes, and refine planning and activation practices.	Surveys have progressively become integrated into digital ad platform campaign management flows.		201	202	203	204	205

[201] Surveys inherently provide fully consented insights, as participation requires voluntary action by surveyed cohorts.
[202] Platform policies generally do not affect ecosystem participants' ability to survey a given population, as long as they have a contact method for outreach.
[203] Conducting *insightful* surveys at scale is generally time- and cost-intensive, from defining survey questions, to gathering contact info, to delivery and collection.
[204] Surveys have been industry standard for decades or more, with well-established best practices, service providers and tooling.
[205] Widely adopted by brands and other ecosystem constituents to get steering feedback from their audiences.

Authors & Contributors

ThinkMedium

Dennis Buchheim, President
Rachel Galvin, Advisor
Hannah Pavalow, Advisor
James Rothwell, Senior Advisor
Alex Roucourt, Advisor

Shullman Advisory

Fiona Campbell-Webster, Advisor
Julia Shullman, President

CIMM & 4A's

Kevin Freemore, SVP, Media, Technology, Data, 4A's
Ashwini Karandikar, EVP, Media, Technology, Data, 4A's
Tameka Kee, Deputy Managing Director, CIMM
Alison Pepper, EVP, Government Relations & Sustainability, 4As
Jon Watts, Managing Director, CIMM

Steering Group Members

David Algranati, Chief Product Officer, Comscore
Andy Dale, General Counsel & Chief Privacy Officer, Open AP
Rachel Glasser, Chief Privacy Officer, Magnite
Claudio Marcus, Independent Industry Expert
Yee Pang, Group Director, Research & Measurement, GroupM
Bharad Ramesh, Executive Director, Research & Investment Analytics, GroupM
Noga Rosenthal, General Counsel & Chief Privacy Officer, Ampersand

WIth thanks to interviewees from A+E, Ampersand, Blockgraph, Comscore, Dish, Infosum, Nielsen, Google, GroupM, Paramount, Philo, Qonsent, Samba TV, and VideoAmp.