TV 3.0 Privacy Management: Signaling, Enforcement and Rights Control

Marcelo F. Moreno,

Eduardo Barrére

Débora C. Muchaluat-Saade

CITE THIS ARTICLE

Marcelo F. Moreno, Eduardo Barrére and Débora C. Muchaluat-Saade; 2025. TV 3.0 Privacy Management: Signaling, Enforcement and Rights Control. SET INTERNATIONAL JOURNAL OF BROADCAST ENGINEERING. ISSN Print: 2446-9246 ISSN Online: 2446-9432, doi: 10.18580/setijbe.2025.6 web link: https://dx.doi.org/10.18580/setijbe.2025.6

SET INTERNATIONAL JOURNAL OF BROADCAST ENGINEERING – SET IJBE V.11, 2025, Article 6 | 11 p
© 2025 SET – Brazilian Society of Television Engineering | ISSN (Print): 2446-9246 | ISSN (Online): 2446-9432

TV 3.0 Privacy Management: Signaling, Enforcement and Rights Control

Marcelo F. Moreno, Associate Professor, UFJF, Eduardo Barrére, Full Professor, UFJF and
Débora C. Muchaluat-Saade, Full Professor, UFF

Abstract— The integration of broadband connectivity and application-oriented services in TV 3.0 introduces new requirements for platform-level governance of personal data processing. Existing broadcast and smart TV ecosystems typically delegate privacy signaling and viewer preference handling to applications, offering limited guarantees of enforcement. TV 3.0 addresses this limitation by incorporating a native Privacy Manager within the Application-oriented Platform (AoP), responsible for interpreting declarative privacy signaling, managing viewer agreements across multiple lawful bases, and mediating access to privacy-scoped system resources. This paper presents the architecture, signaling model, and enforcement mechanisms of privacy management in TV 3.0, including the Privacy Record Request Description (PRRD), standardized privacy records and receipts, automated privacy interface rendering, and runtime mediation of sensitive APIs. Privacy governance is implemented as an intrinsic middleware capability of TV 3.0, independent of application logic and external enforcement mechanisms.

Index Terms— Broadcast Technology, Personal Data, Privacy Protection, Software Architecture

I. INTRODUCTION

THE evolution of digital television toward application-oriented and broadband-integrated services introduces new architectural requirements for the governance of personal data processing at the receiver level. TV 3.0 specifies a next-generation broadcast platform in which interactive services are natively integrated with Internet connectivity, enabling user interaction, personalization, and service adaptation within a standardized execution environment [1]. As the television receiver evolves into an execution environment that mediates between broadcast signaling, application logic, and device-level resources, the handling of viewer-related information becomes a foundational platform responsibility.

As interactive television platforms evolve, the receiver increasingly mediates between broadcast signaling, application logic, and device-level resources. This shift raises fundamental questions regarding how data processing intentions are declared, how viewer choices are captured, and how resulting restrictions are enforced across shared middleware interfaces. Regulatory frameworks such as Brazil’s Lei Geral de Proteção de Dados Pessoais (LGPD) define principles including lawful bases for processing, transparency, purpose limitation, and accountability, which act as constraints on system design rather than matters of legal interpretation [2]. Studies of smart TV usage further indicate that privacy expectations are shaped by the shared and persistent nature of television devices, reinforcing the need for platform-level mechanisms that operate consistently across applications and users [3].

In many existing broadcast-interactive and smart TV ecosystems, privacy handling remains primarily delegated to applications. In standards such as HbbTV [4] and ATSC 3.0 [5], applications are responsible for presenting privacy notices, collecting viewer choices, and enforcing declared preferences within their own execution context. Empirical analyses of connected TV environments show that this approach leads to heterogeneous implementations, fragmented records, and limited technical guarantees that viewer preferences are indeed respected across system boundaries [6], [7]. Similar limitations have been observed in web and streaming ecosystems, where in-application banners and checkbox-based mechanisms rely on voluntary compliance and provide limited auditability or technical enforcement at the platform level [8], [9].

The TV 3.0 Application-oriented Platform (AoP) addresses these limitations by defining privacy governance as a native middleware capability. The platform incorporates a dedicated Privacy Manager that operates independently of Broadcaster Applications and mediates privacy-related interactions between service-layer signaling, viewer interfaces, and access to sensitive system resources. The definition of this platform results from a coordinated research and development effort [10] conducted within the Brazilian Digital Television System Forum (SBTVD Forum) and consolidated through technical standardization activities [11]. Within this process, privacy management is treated as a design-time architectural requirement rather than a post-deployment concern. This architecture integrates standardized information structures for privacy records and receipts, based on ISO/IEC 27560 [12], together with machine-readable semantic vocabularies for data processing purposes, lawful bases, and personal data categories [13], [14]. The AoP establishes a unified enforcement layer by placing privacy management within the middleware, independent of application-specific behavior.

The objective of this paper is to present the architecture, signaling model, and enforcement mechanisms defined for privacy management in TV 3.0. The paper describes how data processing intentions are expressed through structured service-layer signaling, how viewer interactions are automatically rendered and recorded by the platform, and how the resulting privacy state governs application access to personal data at runtime. Privacy governance is treated as an intrinsic capability of TV 3.0 AoP, reflecting the outcome of a research-driven standardization process and providing a technically enforceable foundation for regulated data processing in application-oriented broadcast environments.

This paper is organized as follows. Section II reviews the regulatory and technical background relevant to privacy management in application-oriented broadcast platforms and discusses related work. Section III introduces the role of the Privacy Manager within TV 3.0 AoP. Section IV presents the specification of the Privacy Record Request Description

This work was supported in part by Brazilian Ministry of Communications (MCom), SBTVD Forum and the National Research and Education Network (RNP), under TV 3.0 Project - Phase 3.

https://set.org.br/ijbe/ doi:10.18580/setijbe.2025.6 Web Link: https://dx.doi.org/10.18580/setijbe.2025.6

(PRRD) used for declarative privacy signaling. Section V describes the privacy workflow and the automated rendering of user interfaces. Section VI details the lifecycle of privacy records and receipts. Section VII explains the runtime enforcement model for mediating access to sensitive APIs, and Section VIII discusses cross-service privacy registry and preference management. Section IX concludes the paper and outlines directions for future work.

II. BACKGROUND AND RELATED WORK

This section establishes the regulatory and technical context that underpins the privacy management architecture defined for TV 3.0. It first outlines the data protection principles that act as design constraints for interactive broadcast platforms, with emphasis on lawful bases, purpose limitation, and accountability. It then reviews how privacy signaling and viewer preference handling are addressed in existing broadcast and smart TV standards, highlighting their reliance on application-level mechanisms. Finally, the section introduces standardized information models and semantic vocabularies for privacy records and data processing declarations, and situates the TV 3.0 approach within this landscape through an architectural comparison of platform- and application-centric privacy governance models.

A. Regulatory and Design Constraints for Privacy Management

The design of privacy management mechanisms in TV 3.0 is constrained by data protection frameworks that define the conditions under which personal data may be processed. In the Brazilian context, LGPD establishes a set of principles and requirements applicable to any processing of personal data, including processing performed in connection with broadcasting services enabled by broadband connectivity [2]. Comparable principles are present in other data protection frameworks, such as the General Data Protection Regulation (GDPR)[2] of the European Union, reinforcing the relevance of these constraints beyond a single jurisdiction.

A central element of these frameworks is the requirement that each data processing activity be associated with a clearly defined purpose and a corresponding lawful basis. Lawful bases may include, among others, consent, legitimate interest, or compliance with legal or regulatory obligations. The applicability of a given lawful basis depends on factors such as the nature of the data involved, the intended purpose of processing, and the operational context of the service. The selection and justification of the appropriate lawful basis are the responsibility of the data controller, which in the TV 3.0 ecosystem corresponds to the broadcaster offering the service. Platform mechanisms are therefore required to support the declaration of purposes and lawful bases without embedding assumptions about their legal validity.

From a system design perspective, this requirement implies that privacy management mechanisms must support multiple lawful bases concurrently and allow different purposes to be associated with different processing conditions. In particular, consent represents one possible lawful basis among others and must be treated as such within the platform architecture. While consent-based processing requires mechanisms for explicit viewer agreement, withdrawal, and documentation, other lawful bases may impose different requirements on transparency and control. A platform-level privacy subsystem must therefore be capable of distinguishing between these cases while remaining agnostic to the legal interpretation underlying the broadcaster's declarations.

In addition to lawful basis selection, regulatory frameworks emphasize principles such as purpose limitation, data minimization, transparency, and accountability. These principles translate into technical requirements for structured declaration of processing intentions, clear communication to the viewer, and the ability to document and demonstrate how viewer-related data is handled over time. Importantly, these requirements cannot be fully addressed through user interface elements alone. They require platform support for consistent signaling, persistent records of viewer decisions, and enforceable restrictions on access to personal data in accordance with the declared processing context.

Within this paper, regulatory frameworks such as LGPD and GDPR are treated strictly as sources of design constraints that inform system architecture. No attempt is made to interpret legal obligations or to assess compliance. Instead, the focus is on how a broadcast platform can be structured to support explicit declaration of purposes and lawful bases, viewer-facing transparency, and technical enforcement capabilities in a manner consistent with the expectations imposed by contemporary data protection regimes.

B. Privacy Management in Existing Broadcast and Connected TV Platforms

Existing interactive broadcast and connected television platforms address privacy management primarily at the application level. In these environments, interactive services are delivered through applications executed on the receiver, and privacy-related interactions, such as the presentation of notices, collection of viewer choices, and handling of preferences, are implemented within application logic rather than as native platform functions. As a consequence, responsibility for privacy signaling, user interface behavior, and enforcement is distributed across individual services, with limited coordination or consistency at the receiver level.

In interactive broadcast systems based on HbbTV [4], applications are responsible for presenting privacy-related information and collecting viewer choices, while the underlying platform focuses on service signaling, application execution, and lifecycle management. Although HbbTV defines mechanisms for hybrid broadcast–broadband service delivery, it does not specify standardized platform-level mechanisms for privacy signaling, record generation, or enforcement. These aspects are left to applications' logic, resulting in service-specific approaches to privacy handling. Empirical analyses of HbbTV deployments further indicate that this application-centric model leads to heterogeneous

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). OJ L 119, 4.5.2016, pp. 1–88.

practices and limited technical guarantees regarding how viewer-related data is accessed and processed [6], [7].

A comparable approach is observed in ATSC 3.0 interactive content [5] and service delivery [15] standards. They provide detailed mechanisms for application signaling, execution, and synchronization, but do not assign privacy governance responsibilities to the middleware. Privacy notices, viewer preference handling, and any resulting access restrictions are implemented within applications, without a standardized platform-level mechanism for interpreting privacy declarations or mediating access to personal data. As a result, the receiver platform does not maintain a unified representation of viewer privacy preferences across services.

Similar architectural patterns are observed in connected and streaming television platforms. Privacy management in these systems is typically implemented through in-application dialogs, banners, or checkbox-based interfaces that rely on voluntary compliance by applications and services. Empirical studies have shown that such mechanisms provide limited auditability and do not ensure that declared viewer preferences are consistently enforced across system interfaces or over time [6], [7] particularly when privacy handling is implemented through user interface mechanisms without platform-level mediation [8]. These findings highlight the absence of a stable platform mechanism for enforcing viewer privacy preferences.

Taken together, these platforms share a common architectural characteristic: privacy management is treated as an application responsibility rather than a platform capability. While this approach allows service-specific flexibility, it does not provide standardized signaling, persistent records of viewer decisions, or middleware-level enforcement. This background motivates the design choice in TV 3.0 to define privacy governance as a native function of TV 3.0 AoP, enabling consistent interpretation of privacy declarations and technical enforcement independent of application logic.

C. Standardized Privacy-related Records and Vocabularies

Several standardization efforts provide foundational elements for representing privacy-related information in a structured and interoperable manner. These efforts focus on information modeling and semantics, rather than on system architecture or enforcement, and are thus complementary to platform-level privacy management designs.

ISO/IEC 27560 defines standardized information structure for consent records and receipts, specifying how user decisions can be represented, identified, timestamped, and linked to declared processing contexts [12]. It establishes a common model for documenting consent-related events, enabling portability and auditability of consent information across systems. Its scope is intentionally limited to consent, which is a lawful basis that explicitly requires recording and demonstrability under data protection frameworks. Other lawful bases do not generally impose the same requirement for user-facing records, making this focus both deliberate and appropriate. However, as a consequence of this scope choice, ISO/IEC 27560 does not address how records related to non-consent lawful bases should be represented, nor how mixed scenarios involving multiple lawful bases should be handled within a single processing context.

Complementing record structures, W3C Data Privacy Vocabulary (DPV) 2.0 provides a controlled vocabulary for expressing data processing purposes, lawful bases, processing operations, and related concepts in a machine-readable form [13]. The associated Personal Data Categories (PD) vocabulary defines standardized terms for classes of personal data, supporting consistent identification of the types of information involved in processing activities [14]. Together, these works enable semantics and interoperability when describing privacy-relevant declarations across different systems and application domains.

While DPV and PD provide a flexible semantic foundation, their current scope reflects an early stage of formalization for complex privacy lifecycles. In particular, the vocabularies are limited in their ability to express temporal and state-based aspects of lawful bases beyond consent, such as opt-in and opt-out conditions associated with legitimate interest, expiration of processing authorizations, or revocation semantics that differ from consent withdrawal. These limitations are not specific to Broadcaster Applications and reflect broader challenges in modeling dynamic privacy states across heterogeneous systems.

Importantly, neither ISO/IEC 27560 nor W3C vocabularies prescribe how privacy information is collected, how user interfaces are rendered, or how access to personal data is technically enforced. Their role is to provide standardized representations that can be integrated into domain-specific architectures. As such, they serve as essential building blocks for privacy management solutions that require interoperability, auditability, and semantic consistency, while leaving enforcement strategies and platform responsibilities to be defined by the systems.

D. TV 3.0 Architectural Positioning

The preceding subsections have outlined the regulatory constraints applicable to privacy management in interactive broadcast systems, reviewed how existing platforms handle privacy at the application level, and introduced standardized information models and vocabularies that support structured privacy declarations. This subsection consolidates those observations by positioning the TV 3.0 privacy framework [1] within the architectural landscape of interactive broadcast and connected television platforms and summarizing the resulting architectural distinctions.

TV 3.0 defines privacy management as a native function of the AoP. At an abstract level, this positioning is characterized by the use of standardized signaling to declare data processing intentions, the platform-controlled presentation of privacy interfaces, the generation of persistent records documenting viewer decisions, and the mediation of access to privacy-scoped system resources by the middleware. These characteristics are introduced here solely to establish a common basis for comparison; their specification and operational behavior are detailed in subsequent sections.

Table I summarizes how this architectural positioning contrasts with approaches observed in existing interactive broadcast platforms and in application-centric connected

TV and streaming services. Rather than focusing on specific mechanisms, the comparison highlights the allocation of responsibility between applications and the execution environment. This summary highlights that the contribution of TV 3.0 lies not in redefining regulatory principles or privacy semantics, but in reassigning responsibility for privacy governance to the execution environment. By doing so, the platform establishes a consistent foundation for signaling, record-keeping, and enforcement that complements existing regulatory and semantic standards, while avoiding dependence on application-level opaque implementations.

TABLE I
Comparative Overview of Privacy Management Approaches

Aspect	HbbTV [4]	ATSC 3.0 [5]	Web / Streaming	TV 3.0 [1]
Location of privacy governance	Application logic			Platform middleware
Privacy signaling	Service-specific, ad hoc			Standardized, platform-interpreted
Control of privacy UI	Application-defined			Platform-defined
Representation of viewer choices	Implicit or service-specific			Structured platform records
Persistence of privacy state	Service-dependent			Maintained by the platform
Enforcement of restrictions	Application-implemented			Middleware-mediated
Support for auditability	Limited			Platform-supported

III. PRIVACY MANAGEMENT IN TV 3.0 AOP

TV 3.0 AoP defines privacy management as a system-level function integrated into the middleware that mediates the execution of broadcast services and applications. Within this architecture, the Privacy Manager operates as a native platform component responsible for interpreting privacy declarations, collecting viewer decisions, and maintaining auditable records. Figure 1 summarizes TV 3.0 privacy management workflow, illustrating the sequence from standardized privacy signaling to the generation and storage of privacy artifacts. The numbered steps shown in the figure are referenced throughout this section.

The workflow begins when a broadcaster transmits a Privacy Record Request Description (PRRD) as part of the SLS of a TV 3.0 service (①). The PRRD declaratively specifies the broadcaster's intended processing of personal data, including purposes and associated lawful bases and data. The Privacy Manager monitors the signaling stream to identify PRRD announcements/updates in the current service.

Privacy management is activated when the viewer selects a broadcast service (②). Service selection establishes the execution context in which Broadcaster Applications may run and personal data access may be requested. Upon service selection, the Privacy Manager retrieves and validates the PRRD associated with the selected service and determines whether it represents a new request or a modification of a previously processed declaration.

When viewer interaction is required, the Privacy Manager automatically renders a privacy management interface that is superimposed over the currently active Bootstrap or Broadcaster Application (③). The structure, behavior, and available controls of this interface are fully derived from the PRRD content and are not subject to modification by the broadcaster, ensuring consistent presentation across services.

Through the rendered interface, the viewer reviews the declared data processing purposes and expresses their privacy choices (④). The Privacy Manager captures these choices in a structured form, preserving their association with the corresponding purposes and the active viewer profile.

After the viewer submits their selections, the Privacy Manager generates a structured privacy record that incorporates the broadcaster's declared processing intentions together with the viewer's decisions and securely delivers this record to the broadcaster using the delivery endpoint specified in the PRRD (⑤). This record provides the broadcaster with a verifiable representation of the viewer's current privacy state broadcaster with a verifiable representation of the viewer's current privacy state..

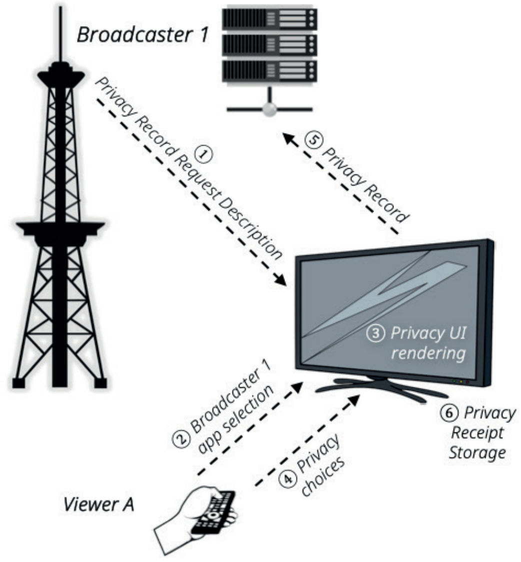

Broadcaster 1
① Privacy Record Request Description
⑤ Privacy Record
③ Privacy UI rendering
② Broadcaster 1 app selection
④ Privacy choices
⑥ Privacy Receipt Storage
Viewer A

Fig. 1. Privacy management workflow in TV 3.0 AoP, from PRRD signaling to privacy record delivery and local receipt storage [1]

Upon successful delivery of the privacy record, the Privacy Manager generates a corresponding privacy receipt and stores it locally in non-volatile memory (⑥). The receipt mirrors the content of the delivered record and maintains an event-based history of viewer decisions, enabling subsequent review or withdrawal of preferences. The receipt remains persistently associated with the active viewer profile.

Based on the privacy state expressed in the most recent privacy receipt, the Privacy Manager enables enforcement within the AoP. When Broadcaster Applications attempt to access personal data or privacy-scoped platform APIs, the Privacy Manager mediates these requests and conditionally grants or denies access according to the recorded viewer choices. Updates to preferences are immediately reflected in enforcement behavior, ensuring that expressed decisions are translated into technically binding operational constraints.

IV. PRIVACY RECORD REQUEST DESCRIPTION (PRRD)

The Privacy Record Request Description (PRRD) is the mechanism through which TV 3.0 services formally declare their intended processing of viewers' personal data. Technically, PRRD is defined as an XML fragment embedded in the Service Layer Signaling (SLS), following the fragment-based signaling model established in ATSC A/331 [16]. As such, PRRD is transmitted as part of the broadcast signaling flow and interpreted directly by TV 3.0 AoP, independently of Broadcaster Applications' logic. All elements and attributes discussed in this section therefore refer to XML constructs defined within the PRRD fragment.

Rather than redefining privacy semantics, the PRRD specification builds upon established international standards. ISO/IEC 27560 [12] provides the conceptual foundation for structured records and receipts documenting data processing decisions, while W3C DPV [13] and PD [14] vocabularies supply standardized identifiers for lawful bases, processing purposes, personal data categories, and actor roles. These vocabularies are reused as semantic building blocks and integrated into broadcast service signaling and platform-level interpretation, addressing TV 3.0 specific requirements.

At a conceptual level, PRRD represents a service-scoped, machine-readable declaration of data processing intentions issued by the broadcaster. Its role is to establish the processing context that enables the Privacy Manager to determine whether viewer interaction is required, how management interfaces are rendered, and which enforcement rules apply once decisions are expressed. PRRD precedes and conditions the generation of privacy records and privacy receipts; it does not record viewer choices, but instead defines the purposes, lawful bases, and data categories against which those choices are later evaluated and enforced.

An illustrative PRRD instance is provided in Listing 1, demonstrating the declaration of a service usage analytics purpose, associated personal data categories, lawful basis, jurisdiction, participating parties, and delivery endpoint. The specific values used in this example are provided solely for illustration. The selection of processing purposes and corresponding lawful bases remains the responsibility of each broadcaster and depends on its legal interpretation, practices, and the nature of the data involved. The PRRD mechanism itself is agnostic to particular purposes or legal bases and is designed to support a broad range of data processing declarations within applicable data protection frameworks.

Each PRRD instance is uniquely identified by a versioned schema reference (PRRD@schemaVersion), allowing the Privacy Manager to distinguish between new and previously processed declarations. Any modification to declared purposes, lawful bases, personal data categories, recipients, retention parameters, or other semantically relevant elements results in a new version identifier. This versioning mechanism ensures that viewer decisions are always associated with the precise processing context in effect at the time of interaction and provides a deterministic trigger for re-evaluating privacy choices when that context changes.

PRRD organizes privacy information through one or more piiProcessing elements, each corresponding to a specific language (piiProcessing@language). Each piiProcessing block encapsulates all textual and presentational content required to render the privacy management interface in that language, including references to the applicable privacy notice (piiProcessing@privacyNotice), a broadcast-accessible copy (piiProcessing@broadcastNotice), the secure endpoint for privacy record delivery (piiProcessing@deliveryUrl), and the initial disclaimer displayed in simplified privacy views (initialDisclaimer). When multiple languages are provided, these blocks remain semantically equivalent, differing only

```
<?xml version="1.0" encoding="UTF-8"?>
<PRRD xmlns= "tag:sbtvd.org.br,2025:XMLSchemas/TV30/AppSignaling/
PRRD/1.0/"
   xmlns:dpv="https://w3id.org/dpv#"
   xmlns:pd="https://w3id.org/dpv/pd#"
   schemaVersion="PRRD-1.0-BCAST-20251101">
  <piiProcessing language="en-US"
     privacyNotice=
       "https://broadcaster.com.br/privacy/tv30/20251101"
     broadcastNotice=
       "http://broadcaster.com.br/appCtx1/priv20251101.html"
     deliveryUrl=
       "https://privacy.broadcaster.com.br/tv30/records">
    <initialDisclaimer>
      Broadcaster requests to process viewer-related data for specific purposes. You
can review/manage these options now.
    </initialDisclaimer>
    <purposes>
      <purpose id="audienceMeasurementPurpose"
              type="dpv:ServiceUsageAnalytics"
              lawfulBasis="dpv:Consent">
        <piiInformation>
          <pii type="pd:Profile" optional="false">
        Viewer profile identifier
          </pii>
          <pii type="pd:DeviceBased" optional="true">
        Device identifier for service usage measurement
          </pii>
          <pii type="pd:Behavioral" optional="false">
        Interaction and navigation events within the service
          </pii>
          <piiControllers>
            <partyId>BROADCASTER</partyId>
          </piiControllers>
          <storageLocations>BR</storageLocations>
          <retentionPeriod>P6M</retentionPeriod>
          <jurisdiction>BR</jurisdiction>
          <recipientThirdParties>
            <partyId>MEDIARESEARCH</partyId>
          </recipientThirdParties>
          <withdrawalMethod>TV30AoP-privacyManager
          </withdrawalMethod>
          <authorityParty>ANPD</authorityParty>
        </piiInformation>
      </purpose>
      <!-- Other purpose elements may appear here -->
    </purposes>
  </piiProcessing>
  <!-- Other piiProcessing elements may appear here -->
  <partyIdentification>
    <party id="BROADCASTER" type="dpv:DataController">
      <partyName>Broadcaster</partyName>
      <partyAddress> Rio de Janeiro, RJ, Brazil</partyAddress>
      <partyContact>mailto:privacy@broadcaster.com.br
      </partyContact>
    </party>
    <party id="MEDIARESEARCH" type="dpv:DataProcessor">
      <partyName>Media Research Institute</partyName>
      <partyAddress> São Paulo, SP, Brazil</partyAddress>
      <partyContact>mailto:dpo@mediaresearch.org.br
      </partyContact>
    </party>
    <party id="ANPD" type="dpv:DataProtectionAuthority">
      <partyName>
        Autoridade Nacional de Proteção de Dados (ANPD)
      </partyName>
      <partyAddress>Brasília, DF, Brazil</partyAddress>
      <partyContact>https://www.gov.br/anpd/</partyContact>
    </party>
  </partyIdentification>
</PRRD>
```

List. 1. Example of a Privacy Record Request Description (PRRD) instance, declaring a service usage analytics purpose.

in localization.

Within each piiProcessing block, processing intentions are declared through one or more purpose elements. Each purpose represents a distinct data processing activity and is uniquely identified (purpose@id). The natural-language content of the purpose element describes the intended processing in a manner sufficiently clear to allow the viewer to understand its scope. Purposes are further classified using standardized vocabulary terms (purpose@type) drawn from W3C DPV. Typical purpose types include, among others, dpv:ServiceUsageAnalytics, dpv:ServiceOptimisation, dpv:PersonalisedAdvertising, dpv:AccountManagement, dpv:TargetedAdvertising, dpv:PoliticalCampaign, dpv:CommercialPurpose and dpv:AgeVerification. These classifications complement the textual description and support consistent interpretation and platform-level optimization of the privacy management interface.

The legal justification for each purpose is explicitly declared through the purpose@lawfulBasis attribute, which also adopts DPV terms, including dpv:Consent, dpv:LegitimateInterest, dpv:PublicInterest, among others. The differentiation between consent-based and non-consent-based processing is therefore expressed entirely through this attribute. While the Privacy Manager relies on this declaration to determine interface behavior, the selection of the lawful basis itself remains the responsibility of the broadcaster and reflects its own legal assessment.

For each declared purpose, PRRD specifies the categories of personal data involved through one or more pii elements within the piiInformation structure. Each pii element combines a human-readable description with a standardized classification (pii@type) based on W3C PD vocabulary. Examples of such categories include pd:Profile, pd:UID, pd:DeviceBased, pd:TVViewingBehavior, pd:Tracking, pd:Behavioral, pd:Preference and pd:Location. The optionality of each pii is explicitly indicated (pii@optional), allowing the platform to distinguish between mandatory and optional data within an authorized purpose and to apply corresponding access controls.

Additional contextual elements included in the PRRD provide transparency and support rights awareness. These include declared storage locations, retention periods, applicable jurisdiction, identification of third-party recipients, withdrawal mechanisms, and supervisory authorities. PRRD also identifies all parties involved in the processing through a dedicated identification structure (partyIdentification), where broadcasters, processors, recipients, and authorities are declared with explicit roles (party@type) using standardized DPV actor types such as dpv:DataController, dpv:DataProcessor, dpv:Recipient, dpv:ServiceConsumer and dpv:DataProtectionAuthority.

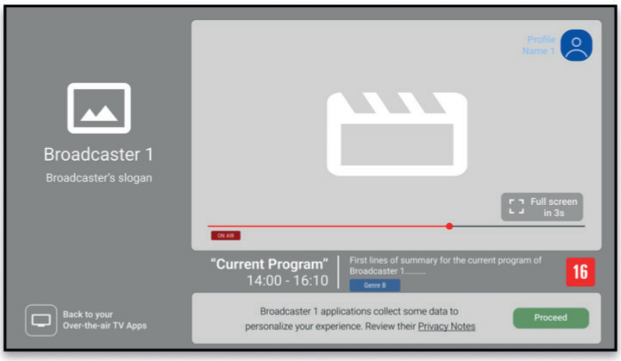
As a definition of privacy intent embedded in broadcast signaling, PRRD establishes a clear separation between the declaration of processing intentions and the recording of viewer decisions. This separation enables consistent, auditable, and platform-level privacy governance within TV 3.0, while remaining independent of application-specific implementations and opaque processing logic.

V. PRIVACY WORKFLOW AND UI RENDERING

Upon reception and validation of a PRRD announced in SLS, TV 3.0 AoP activates the Privacy Manager to mediate the viewer interaction associated with the declared data processing intentions. The Privacy Manager first verifies the structural validity and version of the PRRD instance and determines whether it represents a new declaration or an update to a previously processed request. This evaluation conditions whether viewer interaction is required or whether existing recorded preferences remain applicable.

When viewer interaction is required, the Privacy Manager automatically renders a privacy management user interface that is superimposed over the currently active Bootstrap Application or Broadcaster Application. The generation of this interface is entirely driven by the content of the validated PRRD and is executed by the platform itself. Broadcaster Applications neither define nor modify the layout, behavior, or control logic of the interface, ensuring that privacy interaction remains independent of applications choices.

The Privacy Manager applies a deterministic decision logic to select between two interface modalities. If the PRRD declares no purposes whose lawful basis is consent, a simplified interface is presented. This view displays the initial disclaimer provided in the PRRD, a reference to the full privacy notice, and a single continuation action that returns control to the underlying application. In this case, no granular viewer choice is required, as all declared purposes rely on lawful bases that do not mandate explicit opt-in under the applicable regulatory framework. Figure 2 presents a wireframe representation of the simplified privacy management interface generated by the Privacy Manager and overlaid on a Bootstrap Application.

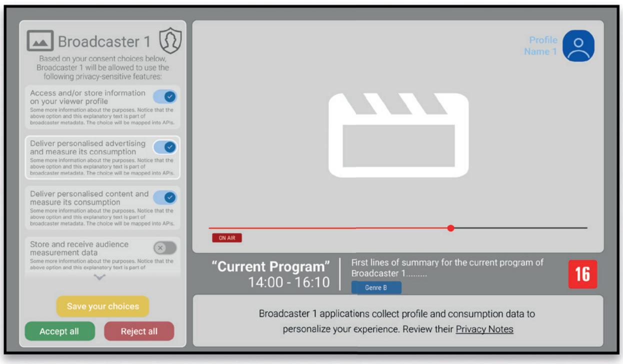


Broadcaster 1 applications collect some data to personalize your experience. Review their Privacy Notes

Fig. 2. Example wireframe of the simplified privacy management interface generated by the TV 3.0 Privacy Manager and superimposed over a Bootstrap Application when the PRRD contains no consent-based purposes.

Conversely, if at least one declared purpose relies on consent as its lawful basis, a detailed privacy management interface is presented. This interface includes an initial disclaimer, access to the full privacy notice, and explicit control options allowing the viewer either to accept all purposes or to manage them individually. The availability of these options is derived directly from the lawful basis metadata associated with each purpose in the PRRD.

When the viewer chooses to manage preferences individually, the Privacy Manager presents a secondary view listing all declared purposes. Figure 3 presents a wireframe representation of such a view. Each purpose is rendered with a dedicated toggle control that reflects its current authorization state. The default state of each toggle is determined by the lawful basis declared for the corresponding purpose. Purposes based on consent are initialized in a denied state, requiring explicit viewer action to authorize processing. Purposes based on other lawful bases, such as legitimate interest, are initialized in an allowed state, while still remaining visible to the viewer for transparency and review.



Based on your consent choices below, Broadcaster 1 will be allowed to use the following privacy-sensitive features:

Access and/or store information on your viewer profile ☑
Some more information about the purposes. Notice that the above option and this explanatory text is part of broadcaster metadata. The choice will be mapped into APIs.

Deliver personalised advertising and measure its consumption ☑
Some more information about the purposes. Notice that the above option and this explanatory text is part of broadcaster metadata. The choice will be mapped into APIs.

Deliver personalised content and measure its consumption ☑
Some more information about the purposes. Notice that the above option and this explanatory text is part of broadcaster metadata. The choice will be mapped into APIs.

Store and receive audience measurement data ☒
Some more information about the purposes. Notice that the above option and this explanatory text is part of

"Current Program"
14:00 - 16:10

First lines of summary for the current program of Broadcaster 1.........

Broadcaster 1 applications collect profile and consumption data to personalize your experience. Review their Privacy Notes

Fig. 3. Privacy management interface listing PRRD-declared purposes and their corresponding per-purpose controls, with default states determined by the lawful basis associated with each purpose.

This differentiated default behavior operationalizes regulatory distinctions without embedding legal interpretation logic into the user interface itself.

Throughout the interaction, the Privacy Manager ensures that viewer choices are collected unambiguously. Each interaction results in the creation of structured events associated with the relevant purposes, which are subsequently incorporated into the privacy record and mirrored in the locally stored privacy receipt. These events preserve temporal information and allow later revisions, ensuring that the full history of viewer decisions remains traceable.

In addition to automatic invocation triggered by new or updated PRRDs, the Privacy Manager supports manual access initiated by the viewer at any time. When invoked with an active DTV service, the Privacy Manager directly loads and displays the existing privacy receipt associated with that broadcaster, if available. In the absence of a prior receipt, the interaction proceeds as a first-time request, using the current PRRD as the governing declaration.

VI. PRIVACY RECORDS AND RECEIPTS LIFECYCLE

The Privacy Manager materializes viewer privacy decisions through the generation of structured privacy records and privacy receipts, which together form the evidentiary layer of privacy governance in TV 3.0. These artifacts are created after viewer interaction with the privacy management interface and are derived directly from the corresponding PRRD, preserving continuity between declared processing intentions and recorded decisions.

A representative privacy record instance is shown in Listing 2, illustrating how viewer choices are captured as structured events associated with specific processing purposes. The example supports the discussion that follows and is provided for explanatory purposes only. The concrete purposes, legal bases, data categories, and actors appearing in the listing do not imply normative requirements; broadcasters remain responsible for defining these elements according to their own legal assessments, organizational practices, and applicable regulatory constraints.

At a structural level, a privacy record is represented as a structured XML document that mirrors the PRRD while extending it with decision-related information. The root element (privacyRecord) retains the same schema version identifier (privacyRecord@schemaVersion) used in the PRRD, binding the recorded decisions to the exact declarative context under which they were collected. Each privacy record is uniquely identified (privacyRecord@id) and explicitly associated with the active viewer profile (privacyRecord@piiPrincipalId), enabling unambiguous reference for audit, compliance and dispute resolution.

The privacy record preserves the declarative components inherited from the PRRD. The piiProcessing elements remain unchanged and continue to describe the declared purposes, lawful bases, personal data categories, retention parameters, and jurisdictional context. Likewise, the partyIdentification section is reproduced to explicitly identify the entities involved in the processing, including data controllers, data processors, and supervisory authorities.

```
<?xml version="1.0" encoding="UTF-8"?>
<privacyRecord xmlns= "tag:sbtvd.org.br,2025:XMLSchemas/TV30/AppSignaling/
PRRD/
privacyRecord/1.0/"
  xmlns:dpv="https://w3id.org/dpv#"
  xmlns:pd="https://w3id.org/dpv/pd#"
  schemaVersion="PRRD-1.0-BCAST-20251101"
  id="b3c6a8c2-9f4e-4b6f-a4c9-7f1c9a2f0e11"
  piiPrincipalId="550e8400-e29b-41d4-a716-446655440000">
 <!-- All piiProcessing elements from PRRD -->
 <piiProcessing>
  ...
 </piiProcessing>
 <!-- The partyIdentification element from PRRD -->
 <partyIdentification>
  ...
 </partyIdentification>
 <!-- Viewer decision events -->
 <eventInformation>
  <!-- Explicitly consent for audienceMeasurementPurpose -->
  <event
    type="dpv:ExplicitlyExpressedConsent"
    time="2025-11-01T22:15:00Z"
    validityDuration="P6M">
   <entityId>550e8400-e29b-41d4-a716-446655440000
   </entityId>
   <purposeId>audienceMeasurementPurpose</purposeId>
   <eventState>dpv:ConsentGiven</eventState>
  </event>
  <!-- Implicitly remains opted-in for appTelemetry -->
  <event time="2025-11-01T22:15:00Z">
   <entityId>550e8400-e29b-41d4-a716-446655440000
   </entityId>
   <purposeId>appTelemetry</purposeId>
   <eventState>tv30:AnyOptIn</eventState>
  </event>
 </eventInformation>
</privacyRecord>
```

List. 2. Example of a Privacy Record instance, documenting two recorded decision events for declared data processing purposes

Viewer decisions are expressed through an event structure contained within eventInformation. Each event is linked to a specific purpose (purposeId) and records its lifecycle state (eventState). Temporal metadata (event@time) is included to establish when the decision took effect, and optional validity constraints (event@validityDuration) may be specified where temporal limitation is relevant, particularly for consent-based processing.

For purposes whose lawful basis is consent, the Privacy Manager records events using standardized consent lifecycle states defined in W3C DPV, such as dpv:ConsentGiven, dpv:ConsentWithdrawn, or dpv:ConsentExpired. These states determine whether the associated processing remains valid and directly influence enforcement decisions at runtime. In such cases, the event may also include an optional event@type attribute to qualify the form of consent expression, when applicable.

For purposes relying on lawful bases other than consent, a distinct lifecycle model applies. As illustrated in Listing 2, when a purpose based on legitimate interest remains enabled through its default state, the corresponding event records an opt-in condition using TV 3.0-specific lifecycle states (e.g., tv30:AnyOptIn). This distinction preserves semantic correctness while allowing all processing purposes to be represented within a unified event framework.

Each event also includes an explicit actor reference (entityId), identifying the entity whose action resulted in the recorded state. This identifier captures whether the state change originated from the viewer, the broadcaster, or the platform itself, depending on the nature of the transition. Explicit attribution strengthens the evidentiary value of the record by making the provenance of each decision auditable.

Once generated, the privacy record is securely delivered to the broadcaster using the endpoint declared in the originating PRRD. TV 3.0 AoP manages delivery attempts and ensures that records are retained locally until successful transmission occurs. Broadcasters store the received records as part of their compliance documentation, enabling verification of lawful processing over time.

In parallel with record delivery, the Privacy Manager generates a privacy receipt, which serves as the viewer-facing counterpart of the privacy record. The receipt is also encoded as a structured XML document whose root element is privacyReceipt, and whose internal structure mirrors that of privacyRecord, including the replicated piiProcessing, partyIdentification, and eventInformation elements. This structural symmetry ensures that the receipt reflects the same purposes, actors, and decision events recorded and transmitted to the broadcaster.

Despite this mirroring, the privacy receipt differs from the privacy record in two important respects. First, the receipt is retained locally within the receiver's non-volatile memory and is not transmitted as part of the broadcast–broadband exchange. Second, the privacyReceipt element includes additional contextual information, such as the delivery endpoint associated with the originating PRRD, enabling re-delivery of revised privacy records without requiring renewed signaling. These distinctions position the receipt as a persistent, viewer-accessible artifact that supports review, modification, and verification of past decisions.

Whenever viewer preferences are revised, new decision events are appended to the locally stored receipt, and an updated privacy record is generated and delivered to the broadcaster. In this way, the privacy receipt maintains a complete and continuous history of privacy interactions from the viewer's perspective, while remaining synchronized with the broadcaster-held record.

VII. ENFORCEMENT MODEL AND SENSITIVE API CONTROL

TV 3.0 AoP enforces viewer privacy decisions at runtime through the mediation of sensitive platform APIs. This enforcement model ensures that privacy preferences recorded in privacy records and receipts are translated into concrete technical constraints governing data access. Enforcement is continuous, service-scoped, and applies uniformly to all Broadcaster Applications.

At the core of this model lies a binding between declared processing purposes, categories of personal data, and the platform APIs that expose such data. When a Broadcaster Application requests access to a sensitive API, the AoP evaluates the request against the current privacy state associated with the active viewer profile and service context. This evaluation considers the declared purpose of the request, the categories of personal data implicated by the API, and the lifecycle state recorded in the privacy receipt. Access is granted only when the recorded state permits processing for that purpose and data category; otherwise, the request is denied by the middleware. The enforcement logic is intentionally independent of the lawful basis declared by the broadcaster, preserving a clear separation between technical access control and legal responsibility.

Audience measurement provides a concrete example of this enforcement logic. TV 3.0 AoP supports dedicated APIs that allow broadcasters to request audience measurement data collection sessions without embedding tracking logic directly into applications or content. Instead, the responsibility for data collection is delegated to the AoP, which autonomously gathers the relevant data, compiles reports, and delivers them to the broadcaster. Crucially, the use of this API is conditioned on the existence of a valid privacy state authorizing processing for a purpose declared with a dpv:ServiceUsageAnalytics type in the PRRD.

When an application attempts to initiate an audience measurement session, TV 3.0 AoP first verifies whether the corresponding purpose is authorized for the active viewer and service. If the purpose relies on consent, the platform checks that a valid consent state, such as dpv:ConsentGiven or dpv:RenewedConsentGiven, is present in the privacy receipt. If consent has been refused, withdrawn or expired, the API request is denied, and no data collection is initiated. This decision is enforced entirely at the platform level, without reliance on application-level checks or self-declaration.

For purposes relying on lawful bases other than consent, the enforcement model follows the same structural pattern, but relies on TV 3.0-specific lifecycle states. When such a purpose is declared in the PRRD, the authorization state is recorded in the privacy receipt as tv30:AnyOptIn, reflecting that processing is permitted without requiring an explicit affirmative action from the viewer. Subsequent viewer interactions may generate state transitions such as tv30:AnyOptOut, tv30:AnyExpired, or tv30:AnyRevoked.

During runtime, TV 3.0 AoP evaluates API access requests by matching the declared purpose and requested data types against the current lifecycle state recorded in the privacy receipt. Access is granted only when the recorded state authorizes processing, ensuring that enforcement semantics for non-consent purposes remain as traceable and reversible as those applied to consent-based purposes.

Once authorized, audience measurement data collection proceeds within a tightly scoped context defined by the pair ⟨service-globalServiceID, viewer-id⟩. This context binding ensures that data collection is unambiguously linked to a specific broadcaster and viewer authorization. Any disruption to this context, such as service changes, profile switches, or receiver interruptions, causes TV 3.0 AoP to pause the session automatically. When the original context is restored, the session may resume, preserving continuity while preventing unauthorized collection across contexts.

From the application's perspective, enforcement is opaque but deterministic. Applications interact with stable platform APIs and receive either authorization or denial responses. They are neither involved in the mechanics of data collection nor capable of bypassing TV 3.0 AoP's mediation logic.

This coupling of declarative intent (PRRD), recorded decisions (privacy records and receipts), and runtime API mediation establishes a closed-loop enforcement model in TV 3.0 privacy management.

VIII. CROSS-SERVICE PRIVACY REGISTRY MANAGEMENT

Beyond managing privacy interactions within the context of an active TV 3.0 service, AoP maintains a persistent registry of privacy-related artifacts across broadcaster services. This registry enables the Privacy Manager to retain awareness of previously announced PRRDs and associated privacy receipts, allowing viewer preferences to be revisited and modified independently of real-time service selection.

At a system level, the registry operates as a service-scoped index linking each broadcaster service identifier to its most recent PRRD version and the corresponding locally stored privacy receipt, when available. This structure allows TV 3.0 AoP to distinguish between services that have never declared data processing intentions, services that have declared intentions but for which no viewer decision exists, and services for which prior decisions have already been recorded. As a result, the Privacy Manager can determine whether an interaction represents a first-time request, a continuation of an existing privacy relationship, or a revision of previously expressed preferences.

Specifically, when the Privacy Manager is invoked without an active TV 3.0 service, it presents a dedicated view, listing only those broadcast services for which a privacy receipt already exists. This view allows the viewer to select a specific broadcaster and directly access its previously recorded privacy settings. Upon selection, the Privacy Manager loads the corresponding privacy receipt and renders the same standardized management interface used during in-service interactions, enabling the viewer to review prior decisions.

This cross-service access model ensures that privacy management is not bound to transient viewing contexts or application lifecycles. Instead, privacy preferences become persistent system-level state associated with the viewer profile and broadcast service. This design avoids repeated consent prompts, reduces interaction fatigue, and reinforces the perception of control across the TV 3.0 environment.

Any modification performed through this registry-based interaction results in the creation of new events in the privacy receipt, following the same lifecycle semantics described in Section VI. Updated privacy records are securely delivered to the corresponding broadcaster using the delivery endpoint, ensuring that changes initiated outside an active viewing session are propagated consistently and verifiably. From the platform's perspective, these updates are indistinguishable from in-session modifications, and enforcement behavior is updated immediately upon receipt modification.

Persistence and synchronization are central to the reliability of this registry. Privacy receipts are stored in non-volatile memory and remain available across power cycles, profile changes, and software updates. The registry maintains version associations between PRRDs and receipts, ensuring that viewer decisions are always evaluated against the correct declaration context. When a broadcaster updates its PRRD, the registry enables the Privacy Manager to detect version mismatches and re-initiate the workflow when necessary.

Security considerations apply uniformly across registry operations. Access to stored receipts is constrained to the active viewer profile, and all record deliveries to broadcasters are performed over authenticated and encrypted channels. The consolidation of privacy state management at TV 3.0 AoP level minimizes duplication of sensitive logic across applications and reduces the risk of inconsistent or unauthorized handling of viewer preferences.

IX. CONCLUSIONS AND FUTURE WORK

This paper presented TV 3.0 Privacy Framework as a platform-level solution that integrates legal compliance, technical enforcement, and viewer control. By embedding privacy signaling, decision collection, record generation, and runtime enforcement directly into TV 3.0 AoP, privacy management is moved from a voluntary, application-dependent feature to a mandatory middleware capability. This architectural shift establishes a stable enforcement point that ensures consistency of viewer experience, auditability of decisions, and effective control over access to personal data across all Broadcaster Applications.

The proposed design demonstrates how standardized privacy declarations, machine-readable records, and enforcement can coexist within a broadcast environment while remaining aligned with regulatory requirements such as LGPD and comparable international frameworks. The use of established vocabularies and consent record structures further reinforces interoperability and legal clarity, while the separation between broadcaster responsibility and platform enforcement preserves clear accountability boundaries.

Several directions for future work emerge from this architecture. First, privacy records accumulated by broadcasters open opportunities for structured knowledge acquisition, enabling improved governance, accountability reporting, and compliance analysis over time. Second, mechanisms for the secure delivery of privacy records to authorized third parties merit further investigation, particularly to support scenarios in which downstream services operate under the context of a broadcaster service and must apply equivalent privacy constraints.

An important complementary direction concerns the definition of conformance testing procedures for TV 3.0 receivers and platforms. Such procedures would allow objective verification that Privacy Manager implementations correctly interpret PRRD signaling, render standardized user interfaces, generate and store privacy records and receipts as specified, and enforce access restrictions on sensitive APIs in accordance with recorded privacy states. Conformance testing would also support harmonization across manufacturers by validating behavior under updates, profile changes, interrupted sessions, and preference revisions.

Further research is needed to assess how viewers understand and interact with privacy management interfaces in receivers, including empirical studies on comprehension, trust, and long-term preference management. Finally, extensions of the Privacy Manager concept to cross-device and multi-platform scenarios remain a promising direction, particularly as broadcast services increasingly span heterogeneous devices and delivery environments.

REFERENCES

[1] Associação Brasileira de Normas Técnicas. (2025). ABNT NBR 25608: TV 3.0 – Application Coding [Standard]. ABNT, Brazil.

[2] Brasil, 2018. Law No. 13,709 of August 14, 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Compiled version. Official Gazette of the Union.

[3] Wang, S.Q, Gao, L., Chetty, M., Feamster, N. (2025). Understanding User Privacy Concerns of Shared Smart TVs. Proc. ACM Hum.-Comput. Interact. Association for Computing Machinery, USA

[4] European Telecommunications Standards Institute. (2023). Hybrid Broadcast Broadband TV (ETSI TS 102 796 V1.7.1). ETSI.

[5] Advanced Television Systems Committee. (2025). ATSC A/344:2025-10 ATSC 3.0 Interactive Content [Standard]. Washington, DC.

[6] Varmarken, J., et al. 2020. The TV is smart and full of trackers: Measuring smart TV advertising and tracking. Proceedings on Privacy Enhancing Technologies.

[7] Tagliaro, C., Hahn, F., Sepe, R., Aceti, A. and Lindorfer, M., 2023. I still know what you watched last Sunday: Privacy of the HbbTV protocol in the European smart TV landscape. In 30th Annual Network and Distributed System Security, NDSS 2023.

[8] Santos, Cristiana and Bielova, Nataliia and Matte, Celestin. (2020). Are Cookie Banners Indeed Compliant With the Law? Technology and Regulation, 2020, 91-135.

[9] Tang, B., Bui, D., & Shin, K. G. (2025). Navigating cookie consent violations across the globe. arXiv. Available: https://arxiv.org/abs/ 2506.08996. Porvisional reference: paper to appear in Proceedings of 34th USENIX Security Symposium, 2025.

[10] Moreno, M. F. et al (2023). R&D Progress on TV 3.0 Application Coding Layer. SET International Journal of Broadcast Engineering (IJBE), 9(1).

[11] Fórum SBTVD. (n.d.). TV 3.0 Project. Retrieved September 21, 2025, from https://forumsbtvd.org.br/tv3_0/

[12] International Organization for Standardization & International Electrotechnical Commission. (2023). ISO/IEC 27560:2023 – Privacy technologies – Consent record information structure [Technical Specification]. ISO/IEC.

[13] W3C Data Privacy Vocabularies and Controls Community Group. (2024). Data Privacy Vocabulary (DPV) – Version 2.0 [Community Group Final Report]. W3C.

[14] W3C Data Privacy Vocabularies and Controls Community Group. (2024). Personal Data Cetagories (PD) – Version 2.0 [Community Group Final Report]. W3C.

[15] Advanced Television Systems Committee. (2024). ATSC A/331:2024-04 Signaling, Delivery, Synchronization, and Error Protection [Standard]. ATSC.

[16] Associação Brasileira de Normas Técnicas. (2025). ABNT NBR 25602: TV 3.0 – Transport Layer [Standard]. ABNT, Brazil.

Marcelo F. Moreno is an Associate Professor at the Federal University of Juiz de Fora (UFJF), Brazil. He holds a Ph.D. in Computer Science from PUC-Rio and works in the areas of multimedia systems and computer networks. From 2022 to 2023, he was a Visiting Professor at the International Audio Laboratories Erlangen (FAU/Fraunhofer IIS), Germany. He co-edited the ITU-T Recommendation H.761 (“NCL and Ginga-NCL”) and has contributed to several international standards, coordinating ITU-T working groups for over a decade. Since 2015, he has led the Application Coding Working Group of the Brazilian Digital TV System Forum (SBTVD) and serves as editor of the ABNT standards for TV 2.5 and TV 3.0. His research focuses on application-oriented broadcasting, second-screen integration, audience measurement, and privacy-aware media platforms for next-generation digital television. He has published widely in the field and is a member of the IEEE and the Brazilian Computer Society (SBC).

Eduardo Barrére has been a full professor in the Department of Computer Science at the Federal University of Juiz de Fora (UFJF) since 2009. He holds a master's degree (1997) in Computer Science form the Federal University of São Carlos (UFSCar) and a doctorate (2008) in Systems and Computing Engineering from the Federal University of Rio de Janeiro (UFRJ). He is the coordinator of the Computer Application and Innovation Laboratory (LApIC) at UFJF. Develops research in the areas of computer networks, Digital TV and multimedia.

Débora Christina Muchaluat-Saade is a full Professor at the Department of Computer Science of Fluminense Federal University (UFF). She holds a Computer Engineering bachelor's degree, MsC and PhD in Computer Science from PUC-Rio. She is currently the vice-coordinator of the Special Committee on Multimedia and the Web (CE-WebMedia) of the SBC (Brazilian Computing Society) and she was the coordinator of the Special Committee on Computing Applied to Healthcare (CE-CAS) from 2017 to 2019. She is the founder of the MídiaCom Research Lab (www.midiacom.uff.br) and one of the lab deans. She is a member of the council and technical committee of the Brazilian Digital TV Forum. She has been contributing to the development of NCL (Nested Context Language) and Ginga-NCL, used in the Brazilian Digital TV Standard (ABNT NBR 15606-2) and IPTV services (ITU-T H.761). Her research interests are multimedia, mulsemedia, computer networks, wireless networks, smart grids, IoT, interactive digital TV and digital healthcare.

Received in 2025-06-25 | Approved in 2025-08-09

https://set.org.br/ijbe/ doi:10.18580/setijbe.2025.6 Web Link: https://dx.doi.org/10.18580/setijbe.2025.6