Network Working Group
Internet-Draft
Intended status: Informational
Expires: 11 December 2025

D. Smullen
B. Scriber
CableLabs

9 June 2025

Privacy Preference Declaration for Home Networks
draft-dsmullen-ppd-architecture-03

Abstract

This document proposes a framework that empowers users to define and enforce privacy policies within their home networks through a Privacy Preference Declaration (PPD) protocol. As connected devices proliferate, this approach enhances user control by enabling user-defined privacy settings for different data types, automatic policy discovery by new devices, and accountability measures such as notifications, network restrictions, or perhaps reporting non-compliance with users' defined preferences to designated authorities. The framework aims to cultivate a privacy-conscious home network environment through clear, enforceable privacy governance.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://drspangle.github.io/draft-dsmullen-ppd-architecture/draft-dsmullen-ppd-architecture.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-dsmullen-ppd-architecture/.

Source for this draft and an issue tracker can be found at https://github.com/drspangle/draft-dsmullen-ppd-architecture.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction

The rapid growth of Internet-connected devices in the home has introduced new and often overwhelming challenges to personal privacy. While many of these devices collect sensitive data by design, the tools offered to users to understand or control that collection are fragmented, confusing, or entirely absent. When privacy settings do exist, they are often buried in obscure menus, expressed in legal or technical jargon, and lack the contextual clarity needed to support meaningful decision-making.

This results in a deeply flawed model: users are expected to defend their own privacy across a chaotic landscape of inconsistent, ad hoc controls—many of which are ineffective or misleading. At the same time, device vendors face growing pressure to meet user expectations and comply with evolving privacy regulations. In response, they often develop bespoke privacy mechanisms that are complex to implement, difficult to maintain, and ultimately fail to provide users with clarity or confidence. These mechanisms are typically built in isolation, without shared patterns or cross-device consistency, leading to privacy interfaces that are overengineered, underused, and poorly aligned with real user needs.

[RFC7258] frames mass data collection as a technical threat, urging protocol designers to limit exposure through encryption and data minimization. While this principle is crucial in adversarial, internet-scale contexts, the model proposed in this document takes a different approach: rather than hiding data flows, it seeks to govern them. Privacy here is not achieved by making devices blind, but by ensuring they are accountable to user-defined preferences.

This shift benefits both users and developers. End users gain the ability to make contextual, informed privacy decisions without being overwhelmed by constant prompts or opaque controls. Developers, in turn, are provided with a clearer, more predictable way to meet privacy expectations—reducing the need to reinvent complex and often inadequate consent and configuration systems. What is needed is not more prompts or disclaimers, but a coherent mechanism for devices to retrieve, interpret, and respect user-directed privacy choices.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Privacy, as framed in this document, is not centered on anonymity or data minimization in the abstract, but rather on empowering users to understand and shape how their data is collected, used, and shared within their home networks. This framework introduces a definition of privacy grounded in two core pillars: transparency and user control. Transparency requires individuals to be provided with a clear and comprehensive understanding of what data is being collected by devices in their environment, how that data is processed and shared, and under what conditions. This understanding must be accessible and meaningful to non-expert users, ensuring that privacy decisions are made with full awareness of their implications. User control refers to the ability of individuals to define and enforce privacy preferences across the entire device ecosystem within their home. Control must be both actionable and enforceable, enabling users to express nuanced policies—such as permitting temperature data collection while prohibiting third-party sharing—and ensuring that devices are held accountable to these expectations.

The perspective of this document stands in contrast to the approach taken in [RFC6973], which emphasizes privacy as the reduction of observability, linkability, and identifiability within protocol design. [RFC6973] recommends minimizing data collection and anonymizing information wherever possible, framing privacy primarily

as a technical safeguard against unwanted inference. In this framework, by contrast, privacy is not defined solely by what is withheld, but by what is understood and governed by the user. In emphasizing user agency and data governance, this work finds conceptual alignment with [RFC8280], which frames privacy as a fundamental human right that protocol designers should consider. [RFC8280] underscores the importance of enabling user autonomy and informed decision-making, values that resonate strongly with this document's goals. However, the perspective of this document is more operationally focused: rather than advocating for abstract rights-respecting design principles, it proposes a concrete architectural approach to operationalize those rights within the home environment. Where [RFC8280] calls for privacy-supportive capabilities in protocol design, this document seeks to instantiate those capabilities through specific, enforceable mechanisms that allow users to express, distribute, and apply their privacy preferences in practice. Ultimately, this framework reconceives privacy not as a static property to be preserved by systems, but as a dynamic relationship between users and their devices—one that must be actively mediated through transparency and meaningful control.

2.1. Privacy

Privacy is not about anonymity, but about providing end users with the ability to be aware of how their data is being collected, used, and shared. It aims to empower users with the knowledge and tools necessary to manage their personal information effectively.

2.2. Transparency

Transparency holds that users possess a clear and comprehensive understanding of what data is collected, how it is utilized, and how it is shared by devices within their network. It involves making the data practices of devices visible and comprehensible to ensure users are fully informed.

2.3. User Control

User control empowers users to exert meaningful influence over the data collection and dissemination practices of these devices. It ensures that users have the capability to define their privacy preferences and enforce policies that align with their comfort levels and expectations.

3. Limitations of Existing Mechanisms

Current mechanisms for managing data privacy within the home environment exhibit limitations.

3.1. Device-specific Configurations

Individual devices often employ unique privacy settings, thereby complicating user management of privacy across the entire network. This complexity can inadvertently lead to unintended data sharing

3.2. Ineffective and Unusable User Interfaces

Navigating and configuring privacy settings on individual devices can be a time-consuming and frustrating experience for users. These ineffective interfaces often lead users to habitually agree to relax their privacy preferences without fully understanding the implications of their decisions. This fosters a general resignation towards privacy management, making it difficult for users to exert meaningful control over their personal data and ultimately compromising their privacy expectations.

3.3. DNT and P3P

Protocols like Do Not Track (DNT) and Platform for Privacy Preferences Project (P3P) have not achieved widespread adoption and have proven inadequate for addressing nuanced privacy needs. These protocols lack the granularity required to express fine-grained user preferences and may not effectively prevent unintended data collection or sharing. For instance, consider a smart security camera within a home network. While DNT or P3P can signal a user’s general preference not to be tracked or share data, they do not enable users to specify detailed privacy settings, such as allowing the camera to record video but not audio, or restricting data sharing to only within the home network. Users need more precise control options to manage their privacy effectively and ensure their preferences are respected across different devices and contexts. These limitations, coupled with the increasing complexity of the IoT ecosystem, hinder the effective exercise of user control over their data within the home environment and pose a significant threat to user privacy.

4. Vision

This document proposes a framework aimed at changing how users express their privacy preferences within their home network. The new paradigm aspires to achieve a seamless and user-friendly experience, where privacy settings do not hinder the use of devices, reduce the burden of configuration management, and eliminate the need to navigate through long, unintelligible legal-language privacy policies. By simplifying the process for defining privacy preferences, this approach aims to alleviate privacy fatigue and combat the pervasive feelings of resignation that users often

experience regarding their privacy choices. This will empower users to make informed decisions without duress, fostering greater trust and confidence in integrating internet-of-things devices into their homes. In essence, the vision is to provide users with intuitive mechanisms for expressing privacy preferences, thus ensuring their concerns are addressed effectively and promoting a more private home environment.

4.1. Use Case: Smart Thermostat with Location Tracking

Scenario: A user purchases a smart thermostat that offers location-based temperature adjustments.

User Preference: The user desires temperature adjustments based on their presence at home but wishes to prevent the thermostat from collecting and transmitting precise location data.

Expected Outcome: The PPD protocol allows the user to define a policy where the thermostat can only determine presence/absence within the home without collecting precise GPS coordinates. The thermostat must clearly inform the user of this limitation and any potential impact on functionality (e.g., less precise temperature adjustments). Regulatory frameworks such as the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA) in the U.S. already require companies to obtain explicit consent before collecting and processing sensitive personal data, including precise location information. The PPD protocol ensures that consent is gathered in a manner that is transparent and comprehensible to the user, preventing scenarios where users might feel pressured or overwhelmed by the decision-making process.

This protocol empowers individuals to make educated choices regarding their privacy settings by offering clear and concise information about data collection practices, potential risks, and benefits. It places the user in control, fostering an environment where privacy decisions are made without duress, thus promoting confidence and trust in integrating internet-of-things devices into their daily lives.

4.2. Use Case: Smart Speaker with Selective Voice Recording Retention

Scenario: A user gets a smart speaker that can record and store voice data.

User Preference: The user wants to keep general conversations for service improvement but prefers sensitive information to be selectively deleted and not retained.

Expected Outcome: The PPD protocol enables the user to configure the speaker to identify and delete recordings containing sensitive information while retaining other voice data as long as necessary. The speaker must inform the user about its data collection and storage practices, providing an option to manage selective deletion.

This outcome significantly enhances the user experience by ensuring privacy preferences are respected seamlessly within the context of their own network. Users can manage their sensitive information without needing to reveal details to the smart speaker service, which means the user's privacy is upheld. The smart speaker service only sees the retention preferences, avoiding the risks associated with handling sensitive data, including the preferences themselves which may be considered sensitive.

Moreover, this streamlined approach means that device manufacturers do not need to expend resources on developing special user interfaces for managing these preferences. Instead, the preferences are integrated within the home network, allowing for a cohesive and user-friendly experience. This integration prevents the need for users to navigate separate interfaces or endure educational prompts to manage their privacy settings, fostering a smoother and more intuitive interaction with the device.

4.3. Use Case: Home Security Camera with Facial Recognition

Scenario: A user installs a home security camera with facial recognition capabilities.

User Preference: The user desires facial recognition for security purposes but wishes to restrict the storage of captured images and the use of facial recognition data for any purpose other than security within the home.

Expected Outcome: The PPD protocol allows the user to configure the camera to only store and process facial recognition data for security purposes within the home network and prohibits the sharing of this data with third parties.

This approach provides numerous benefits for both the camera manufacturer and the user. For the user, it ensures that their privacy preferences are respected and that their personal data is used solely for the intended security purposes. By having control over the storage and usage of their facial recognition data, users can feel more secure and confident in their privacy being upheld. This can lead to a higher level of trust in the device and its manufacturer.

For the camera manufacturer, implementing such a protocol reduces the risk of data breaches and the misuse of sensitive facial recognition data, which can lead to legal complications and damage to their reputation. It streamlines the development process, as they do not need to create complex user interfaces for managing these preferences. Instead, integrating the PPD protocol within the home network allows for seamless and user-friendly privacy management. This approach can also make the product more attractive to privacy-conscious consumers, increasing its marketability and potentially leading to higher sales. This outcome showcases a mutually beneficial relationship where user privacy is prioritized, and manufacturers can offer a more privacy-preserving and appealing product.

5. Goals

5.1. Enhance User Control

* Empower users with the ability to define and enforce clear, concise, and easily understandable privacy policies for their home networks.

* Provide users with the means to effectively exercise control over the collection, use, and dissemination of their personal data by devices within their home network.

5.2. Promote Interoperability

* Establish a standardized mechanism for devices from diverse manufacturers to discover and adhere to user-defined privacy policies, thereby facilitating consistent privacy management across the home network.

5.3. Enable Flexibility

* Provide a framework that allows for the customization of privacy policies to accommodate the unique privacy requirements and preferences of individual users and households.

5.4. Facilitate Transparency

* Ensure that devices within the home network are obligated to provide clear and concise information regarding their data collection and usage practices to users.

* Establish a mechanism for users to easily understand the implications of their privacy policy settings on the functionality of devices within their home network.

6. Scope

This document focuses on defining a high-level architectural framework for a Privacy Preference Declaration (PPD) protocol specifically designed for home network environments. This document concentrates on the conceptual framework, key architectural components, and fundamental principles for enabling users to express and enforce their privacy preferences on devices within their home networks.

This document does not delve into specific implementation details, such as message formats, data structures, security algorithms, or user interface design. Furthermore, this document does not address enforcement mechanisms, legal and regulatory considerations, or specific security protocols.

Specific implementation details and message formats will be addressed in subsequent RFCs. This document aims to be complementary to existing and future standards related to home networking, IoT security, and data privacy.

This document provides the foundation for subsequent work, including:

* Privacy Preference Declaration Taxonomy: This document will define a taxonomy of privacy preference categories and attributes, including a mechanism for registration and management of these categories.

* Privacy Preference Declaration Protocol Specification: This document will specify the message formats, data structures, and communication procedures for the PPD protocol, including mechanisms for device discovery, policy retrieval, and compliance reporting.

7. Architecture Overview

7.1. Assumptions

This document makes the following assumptions:

* User Control: It is assumed that users have a reasonable level of control over their home network infrastructure. This includes the ability to configure routers, install software updates, and manage device access to the network. This control is essential for users to effectively manage their privacy preferences and enforce them on devices within their home network.

* Resource Constraints: It is assumed that the home network environment and devices operating therein have resource limitations, such as limited processing power and bandwidth. We limit this assumption by considering that the PPD protocol and its associated mechanisms should be designed with these constraints in mind, minimizing overhead and ensuring efficient operation even on resource-constrained devices.

* Security Considerations: It is assumed that home networks in scope of this document are susceptible to typical security threats, including insider threats (or non-malicious misconfiguration) and vulnerability to local attacks. We limit this assumption by considering specific security threats to protect user privacy and the integrity of the privacy policy. This includes considerations for secure policy dissemination, device authentication, and protection against unauthorized access and modification of privacy preferences.

* Single User Policy: This document assumes that each device implementing the protocol is governed by a single, unified privacy policy defined by its primary user. While other individuals within the same physical environment (e.g., household) may have different privacy preferences, the protocol is designed with the expectation that a device conforms to the policy established by its primary user. Future extensions could explore mechanisms for managing and reconciling multiple user-defined policies on a single device, particularly in shared or multi-user environments.

* Policy Agreement: It is assumed that devices joining the network are expected not only to retrieve the household privacy policy but also to explicitly agree to abide by its terms. This agreement forms a crucial part of the association process and is essential for ensuring device compliance with user privacy preferences. Failing to agree to the policy is a failure to adhere to the protocol.

* Policy Enforcement: At a minimum, devices must acknowledge that they have received and reviewed the user’s privacy policy. This acknowledgment provides a basic mechanism for users to ensure device accountability and decide whether to onboard it onto the network. Future extensions could introduce more robust enforcement mechanisms to address non-compliance, such as network access restrictions or reporting to a designated authority. These measures would enhance the integrity of the privacy framework and reinforce user trust.

7.2. Key Components

User Interface: A user-friendly interface (e.g., mobile app, web portal) for creating and managing privacy preferences.

Preference Repository: A secure and reliable mechanism for storing user preferences (e.g., local device, cloud service).

Declaration Protocol: A standardized protocol for devices to:

* Discover and retrieve user-defined privacy policies.

* Report their data collection and sharing practices.

* Request user consent for specific data uses.

Enforcement Mechanisms: Mechanisms for devices to enforce user-defined privacy restrictions.

7.3. Data Flows

This section outlines the high-level data interactions between users, devices, and the Preference Repository in the Privacy Preference Declaration (PPD) framework. It describes how privacy preferences are defined by users, retrieved by devices, and used to guide behavior in a home network environment.

The process begins when a user defines a set of privacy preferences that apply to their household. These preferences may express rules such as which types of data may be collected, under what conditions data may be processed or shared, or which retention practices are acceptable. The design of the user interface used to author these preferences, including its presentation, usability, or input modalities, is out of scope for this document, and will be addressed separately. Likewise, the underlying vocabulary and structure of the privacy preferences, including data categories and associated constraints, is specified in (Privacy Preference Declaration Taxonomy).

Once created, the user's preferences are stored in a secure Preference Repository, which may reside locally on a networked controller or be accessible through other trusted infrastructure. When a new device joins the home network, it initiates an onboarding process during which it discovers the repository and establishes a secure channel. Following onboarding, the device performs association, which involves retrieving the household privacy policy and issuing a formal acknowledgment of its terms. Devices may optionally report their data handling declarations to the repository at this stage.

If a device seeks to perform actions not permitted under the baseline policy, for example, collecting or sharing data beyond what the user has authorized may initiate a consent request workflow. However, the design and behavior of this consent mechanism is explicitly out of scope for this document. Inappropriate or poorly designed consent flows, such as those that involve excessive prompting, ambiguous language, or misleading options, can inadvertently pressure users into accepting data practices that conflict with their preferences. Even without malicious intent, these experiences may degrade trust and lead to outcomes inconsistent with user expectations. Future specifications should ensure that consent interactions are clear, proportionate, and respectful, helping users make informed decisions without friction or fatigue.

When the household policy is updated, or when a device's previous association has expired, the device is required to re-associate by re-retrieving and accepting the latest version of the policy. Reassociation ensures that devices remain accountable to current user expectations over time. Devices are not expected to re-collect consent for data uses already covered by existing, valid consent.

To support efficient transmission of privacy policies, consent records, and compliance data (particularly in constrained environments typical of home IoT systems) a compact, machine-readable encoding is recommended. [RFC8949], offers an efficient format for structured data that is well-suited for this context. CBOR balances low-overhead serialization with the ability to represent extensible and semantically rich policy structures. While this document does not mandate any specific encoding, CBOR should be considered as a candidate for future protocol-level message formats.

It is important to note that the minimum requirement under this architecture is limited to the discovery, retrieval, and formal acknowledgment of the user's privacy policy. This acknowledgment provides a foundational mechanism for establishing device accountability. However, this document does not define how policy enforcement must be carried out by the device, nor does it specify

how to handle cases where a device cannot fully comply with a given policy. These aspects, including runtime enforcement, conflict resolution, or auditing, may be addressed in future work.

Finally, while this document defines the overall data flow and interaction sequence, it does not define message formats, communication protocol details, or consent interface specifications. These elements will be specified in a companion document, (Privacy Preference Declaration Protocol Specification).

8. Security Considerations

For a privacy framework to be effective, it must not only support the expression of user preferences but also ensure that those preferences are protected during transmission, retrieval, and enforcement. This section outlines the necessary safeguards for ensuring the confidentiality, authenticity, and integrity of the privacy policy, as well as the anonymity of the household during key protocol operations.

8.1. Secure Policy Dissemination

Communication between devices and the Preference Repository must be protected against unauthorized access and tampering. Cryptographic mechanisms such as encryption and mutual authentication should be employed to ensure that only legitimate devices can retrieve privacy policies and that those policies are delivered without modification.

8.2. Anonymity and Metadata Protection

Even when privacy policies themselves do not contain sensitive personal information, the act of retrieving or acknowledging a policy may reveal characteristics about the household— such as the types of devices in use, specific user preferences, or behavioral patterns over time. [RFC7258] cautions against protocol designs that expose unnecessary metadata, treating the accumulation of such information as a legitimate technical threat. This framework takes that warning seriously: metadata exposure during policy retrieval and device onboarding must be minimized to avoid turning privacy infrastructure into a new source of privacy leakage. Concepts from [RFC9577] may help inform this effort. [RFC9577] introduces techniques for authorization without identification, enabling a client to prove it is authorized without revealing who it is. While [RFC9577] is optimized for pseudonymous web authentication over the public internet, and assumes a centralized token issuer model, its core ideas— particularly around unlinkable token presentation— could be adapted to the PPD protocol to reduce metadata correlation and minimize household identifiability during policy exchanges. However,

this must be done carefully, as the assumptions of [RFC9577] do not fully align with the goals or context of a local, user-governed home network.

8.3. Policy Integrity

Devices must be guaranteed that the policy retrieved is authentic and unaltered. Integrity protections, such as digital signatures, are necessary to ensure that users' preferences cannot be tampered with—either in transit or at rest—by other devices, malicious actors, or misconfigurations.

8.4. Device Authentication

Devices participating in the privacy framework must authenticate themselves before accessing the Preference Repository. This ensures that policy dissemination is limited to known, authorized devices, and that users can maintain trust in the integrity of their home network's privacy relationships. By aligning with the concerns raised in [RFC7258] and incorporating ideas from [RFC9577] where appropriate, this framework seeks to protect users not only from overt data collection, but also from silent inference and passive metadata surveillance. At the same time, it avoids treating anonymity as an end in itself. The goal is to support privacy with accountability—where user-defined preferences are respected, devices are identifiable only as much as necessary, and no more, and the user retains ultimate visibility and influence over what occurs within their domain.

8.5. Policy Agreement and Enforcement

Devices must not only acknowledge receipt of the privacy policy but also explicitly agree to abide by its terms. This agreement should be recorded and verifiable. Enforcement mechanisms should be in place to address non-compliance, including network access restrictions or reporting to a designated authority.

9. Policy Language

The specific details of the Privacy Policy Language, including its syntax, structure, and extensibility mechanisms, are considered out of scope for this document, which focuses on the overall framework. The Privacy Policy Language, along with a taxonomy of privacy concepts and attributes, will be fully defined in a separate RFC, the "Privacy Preference Declaration Taxonomy," allowing for more detailed exploration and development of this crucial component of the PPD framework.

9.1. Language Requirements

* Human-readable: Policies should be easily understandable by users.

* Machine-readable: Policies should be machine-processable for automated enforcement.

* Extensible: The language should be flexible enough to accommodate evolving privacy needs and technologies.

* Internationalization-compatible: Policies and identifiers used within them may need to support multilingual environments and non-ASCII characters.

To ensure consistent interpretation and comparison of string-based policy elements, such as device names, labels, or category identifier string handling practices should align with the guidelines defined in [RFC7564]. This is particularly important when identifiers or user-facing labels are created, stored, or matched across vendors or systems that operate in different locales or character encodings.

9.2. Proposed Approach

Consider leveraging existing privacy policy languages (e.g., P3P) or drawing lessons from privacy labeling systems used in modern application ecosystems—such as Apple's App Privacy Labels and Google's Data Safety section for Android apps. While these approaches are not protocols per se, they demonstrate how structured, declarative privacy metadata can be communicated to users and systems in a consistent way.

Alternatively, a new, concise, and user-friendly privacy policy language may be developed specifically for the PPD framework. One possibility is to define an intermediate representation—similar in spirit to the intermediate representation used in compilers such as LLVM—that captures the fundamental privacy constraints and regulatory considerations (e.g., from GDPR, CCPA) in a machine-readable form. This representation would support automated enforcement while being straightforward to translate into human-readable language.

Future specifications should also define guidance for how string identifiers—such as device roles, policy tags, or consent status labels—are formatted, compared, and stored, to avoid ambiguities across systems. In contexts where internationalized strings are involved, alignment with [RFC7564] should be considered to ensure interoperability and consistency.

10. Future Work

This document defines an architectural framework for enabling users to express and enforce privacy preferences within home network environments. Several aspects critical to a fully operational implementation are intentionally left out of scope here and are expected to be addressed in future specifications or companion documents.

10.1. Policy Taxonomy and Semantics

A separate document, tentatively titled "Privacy Preference Declaration Taxonomy", will define:

* A common vocabulary and set of categories for expressing privacy preferences.

* Attributes and semantics for data types, sharing constraints, and processing conditions.

* An extensibility model for incorporating future data types and policy dimensions.

This taxonomy is foundational for consistent policy interpretation across heterogeneous devices and vendors.

10.2. Protocol Specification and Message Formats

A companion document, "Privacy Preference Declaration Protocol Specification", is expected to define:

* Message formats for device onboarding, policy retrieval, acknowledgment, and compliance reporting.

* Optional mechanisms for consent request flows.

* Transport-layer considerations and discovery mechanisms.

* Recommended encoding formats, such as [RFC8949], for efficient representation of structured data.

10.3. Consent Request Workflow Design Specifications

The mechanism by which devices request additional user consent for data uses not covered by the baseline policy is out of scope. However, future specifications should:

* Define clear constraints to prevent manipulative or fatiguing consent flows (e.g., dark patterns).

* Ensure that consent interactions are transparent, infrequent, proportionate, and user-respecting.

* Explore user interface standards or API affordances to preserve meaningful choice.

This is a particularly sensitive area and must balance user experience, privacy expectations, and implementation feasibility.

10.4. Enforcement and Policy Compliance

This architecture does not define how privacy policies are to be enforced by devices or how non-compliance is to be detected or remediated. Future work may include:

* Runtime enforcement models and device-side implementation expectations.

* Auditing mechanisms for verifying compliance.

* Deconfliction strategies for devices unable to meet all user-defined constraints.

* Options for escalation (e.g., network access restrictions, notifications, or isolation).

10.5. User Interface Design Specifications

The user-facing interface used to author, modify, and review privacy preferences is out of scope. Future design guidance may address:

* User experience design principles for presenting privacy concepts clearly and accessibly.

* Models for progressive disclosure of policy impact.

* Multi-user and household-role-specific control models (e.g., parental vs. administrative roles).

10.6. Internationalization and Identifier Comparison

In contexts where privacy preferences or taxonomy elements involve user-facing or vendor-defined string identifiers, additional work may be required to:

* Define string normalization and comparison rules, particularly for internationalized text.

* Ensure identifier consistency across diverse vendors and locales.

* Consider alignment with the [RFC7564] for handling Unicode-aware identifiers in a secure and interoperable way.

10.7. Interoperability Testing and Reference Implementations

Future work may also include:

* Development of reference implementations of the PPD protocol and repository components.

* Interoperability testing across devices and vendors.

* Conformance guidelines and self-certification procedures.

11. IANA Considerations

This document has no IANA actions.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/rfc/rfc8949>.

12.2. Informative References

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/rfc/rfc6973>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/rfc/rfc7258>.

[RFC7564] Saint-Andre, P. and M. Blanchet, "PRECIS Framework: Preparation, Enforcement, and Comparison of Internationalized Strings in Application Protocols", RFC 7564, DOI 10.17487/RFC7564, May 2015, <https://www.rfc-editor.org/rfc/rfc7564>.

[RFC8280] ten Oever, N. and C. Cath, "Research into Human Rights Protocol Considerations", RFC 8280, DOI 10.17487/RFC8280, October 2017, <https://www.rfc-editor.org/rfc/rfc8280>.

[RFC9577] Pauly, T., Valdez, S., and C. A. Wood, "The Privacy Pass HTTP Authentication Scheme", RFC 9577, DOI 10.17487/RFC9577, June 2024, <https://www.rfc-editor.org/rfc/rfc9577>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Daniel Smullen
CableLabs
Email: d.smullen@cablelabs.com

Brian Scriber
CableLabs
Email: brian.scriber@computer.org