PARCEP: A Network Protocol for Parental Controls

Andrew Campling[i]
Director, 419 Consulting Ltd.
Andrew.Campling@419.Consulting

David Wright[ii]
CEO, SWGfL, Director UK Safer Internet Centre
David.Wright@swgfl.org.uk

Submission to IAB/W3C Workshop on Age-Based Restrictions on Content Access

Introduction

The Internet is widely regarded as a powerful force for good. It has become indispensable for communication, education, healthcare access, and economic resilience. For example, during the COVID-19 pandemic, the Internet enabled remote working, online learning, medical information dissemination, and social connection despite physical distancing, proving itself crucial to societal functioning and survival during that period.

Beyond crisis response, the Internet facilitates social connection, supports mental health by enabling contact even when physical interaction is difficult, and provides access to information and opportunities that would otherwise be unavailable. It also empowers charitable actions and community building, embodying the concept of "digital citizenship" as an active use of technology for social good.

However, the Internet is not without challenges. It faces threats from censorship, control by governments and corporations, and misuse by scammers or those spreading hatred, all of which can undermine its positive potential. There are concerns about safety, especially for vulnerable groups, including children, and the need for ongoing efforts to protect users and ensure equitable access. In some instances, the level of harm being caused has led governments to legislate to bar access to devices (eg smartphones) or particular applications (eg social media platforms) until children reach a certain age.

Tools exist that allow parents to set boundaries for their children’s online access and experience, including access to specific categories of content, some of which have age-appropriate settings. However, these tools currently operate independently, some within operating systems and others within individual applications. The functionality can vary widely, and sometimes even common terms can have different meanings. Even knowledgeable and motivated parents struggle with the plethora of options, especially where children have access to multiple devices on different platforms.

The lack of standardisation of parental control software is hindering its ability to protect children. The authors believe that effective parental controls are a better option than banning children from accessing the benefits of the Internet. We propose developing a new protocol to aid interworking between the many options that are currently on the market.

PARCEP: A Cross-Vendor Interoperability Standard for Family Device Management

1. Context

Children face a broad range of online harms, including exposure to harmful or inappropriate content, contact with potential abusers or manipulators, conduct-based risks such as bullying, and commercial threats like scams or misuse of personal information.

Examples of risks of online harm to children include:

- **Exposure to Harmful Content**: Children may encounter violent, sexual, hateful, or extremist material, as well as age-inappropriate or inaccurate information. Content promoting self-harm, suicide, eating disorders, or terrorism is particularly concerning.
- **Contact Risks**: Online predators can use technology for grooming, harassment, or sexual exploitation. Children may be contacted by adults or peers intending to bully, intimidate, manipulate, or exploit them.
- **Conduct Risks**: This covers cyberbullying, peer pressure, trolling, sharing sexual images (sexting), and participating in or being victimised by harmful online communities promoting unsafe behaviours.
- **Commercial Risks**: Children may fall victim to scams, phishing, or inadvertent spending due to in-app purchases, advertising, or sharing personal data with malicious actors.
- **Impact on Wellbeing**: The effects can range from short-term emotional upset (such as fear, confusion, shame), through behaviour change (social withdrawal, aggression), to serious psychological harm (anxiety, depression, self-harm).

Children may experience harm through both direct exposure (viewing or receiving harmful content) and indirect exposure (content about them shared by others or cumulative exposure over time). Some children are more vulnerable depending on age, maturity, and personal circumstances. As a result, they may feel compelled to share inappropriate material or adopt harmful beliefs and behaviours.

2. Proposal

Digital parenting is now a cross-platform challenge. Major technology companies such as Apple (Family Sharing), Google (Family Link), Microsoft (Family Safety), and Amazon (Parental Controls) offer proprietary tools that allow families to manage children’s access to digital devices, screen time, content and purchases; applications and gaming systems also offer their own tools. These systems have become essential in supporting children’s well-being in an increasingly connected world.

However, these tools are not interoperable. Parents whose children use devices across more than one ecosystem cannot manage them coherently. This fragmentation reduces visibility, consistency, and ultimately effectiveness, forcing parents to navigate multiple dashboards, apps, and settings to achieve even basic oversight.

PARCEP (**Par**ental **C**ontrol N**e**tworking **P**rotocol) is a proposed technical standard that will enable these systems to communicate and cooperate. It is inspired by efforts such as the IETF's MIMI working group (a protocol and standards effort for messaging interoperability) and MLS (an IETF protocol that provides end-to-end encryption for group messaging at Internet scale).

MIMI (More Instant Messaging Interoperability) is a useful comparator as it is intended to enable interworking between existing messaging platforms, allowing users to retain their preferred messaging application whilst being able to communicate with users on another platform. Equally MLS (Messaging Layer Security) is the first open, interoperable standard for secure group messaging, filling a gap left by previous protocols that focused mainly on one-to-one communication.

PARCEP is intended to offer an open, decentralised, and secure protocol framework to enable cross-platform coordination of family device management tools. The aim is not to replace or rebrand existing services, but to enable them to work together in a way that reflects the real-world complexity of modern families and the diverse ecosystems they inhabit.

3. Why PARCEP Is Needed

The rise of the **Smartphone-Free Childhood** movement highlights the sense of powerlessness felt by many families. While this movement has gained traction following tragic events and well-founded concerns about children’s exposure to online harms, it also reflects an important truth: the tools parents are offered today are not sufficient.

Children rarely use just one device. A child may do schoolwork on a Windows laptop, message friends on an iPhone, watch videos on a Fire tablet, and play games on a Nintendo Switch or Sony PS5, all in one evening. No single tool today allows families to establish and monitor coherent rules across that range of platforms, or even the software on a specific device.

This creates enforcement gaps, confusion, and often leads to conflict. Moreover, it risks further exacerbating digital inequality given the level of digital literacy required for parents to navigate the current morass of options. **PARCEP** seeks to address these issues by offering a framework through which all compliant vendors can interoperate whilst still retaining control over their own feature sets and user experiences.

4. Objectives of the PARCEP Standard

PARCEP will establish a framework for **interoperability, consistency and coordination** across family management systems. Specifically, it will:

- **Define a shared data model** for screen time limits, application restrictions, age ratings, content category restrictions and purchase permissions.
- **Enable synchronised enforcement** of these controls across participating devices and applications, regardless of vendor.
- **Support unified identity and role delegation**, allowing family managers to assign guardianship roles, set rules, and manage children's access across multiple households or care settings.
- **Respect privacy and security by design**, ensuring that data minimisation, user consent, and protection of children's personal information are embedded within the protocol.
- **Provide auditability and transparency**, offering families consistent insights into usage patterns, alerts, and override requests across platforms, with visible error messages on devices when any restrictions apply to an action so that a child is aware that the proposed action has been impacted by the controls.

The standard will be **vendor-neutral**, extensible, and adaptable to evolving policy and regulatory frameworks.

5. Alignment with Policy and Regulation

The timing of PARCEP aligns with a growing international focus on child online safety and digital rights. Relevant frameworks include:

- **The UK Online Safety Act 2023**, which enshrines a duty of care on platforms to protect children from harmful content.
- **The UN General Comment No. 25 (2021)** on children's rights in the digital environment, which calls for tools that support both autonomy and protection.
- **The EU Digital Services Act**, which mandates risk assessments and mitigations for child users.
- **The US Kids Online Safety Act (KOSA)**, under discussion, which encourages safety tools and transparency mechanisms for families.

There is also growing emphasis on **interoperability as a safeguard in its own right,** preventing platform lock-in, enhancing user control, and enabling consistency across digital services. PARCEP would complement these regulatory directions by offering a voluntary technical foundation that supports the policy intent of protecting children online.

6. Technical Scope and Considerations

PARCEP is envisaged as a modular, extensible framework, with the following technical components:

- **Family Profile Schema**: A shared, vendor-agnostic schema to describe a child's age, permissions, restrictions, and device associations.
- **Policy Synchronisation Protocol**: A standard for issuing, updating, and revoking family control rules across registered devices.
- **Role and Delegation Model**: A mechanism for defining who can access or manage a profile (e.g., parents, carers, shared households, school), and with what permissions.
- **Activity Reporting Interface**: Optional modules to standardise how usage data, screen time metrics, and alerts are surfaced to authorised guardians.
- **Fallback Behaviours**: Guidance for non-compliant devices or platforms, ensuring transparency about what is and is not enforceable.
- **Device Management:** where feasible, making use of device management tools (eg MDM) to "lock down" settings on devices so that they cannot be changed by the user (eg the DNS resolver) and to block or limit the ability to load new applications without permission from the profile manager.
- **Content Filtering:** A mechanism to specify categories of content that should not be accessible, with the ability to appeal access (by a user to the profile manager or a profile manager to the list provider) in the event of incorrect categorisation.

Like MIMI and MLS, PARCEP will prioritise end-to-end trust, platform neutrality, and user autonomy. Importantly, it will not require a single "master app" — instead, existing tools can integrate the standard, allowing families to manage controls from the system(s) they already use.

7. Conclusion and Next Steps

PARCEP represents a new opportunity for the technology sector to collaborate in the service of a shared societal priority: protecting and empowering families in the digital world. Whilst parental controls restrict the ability of children to access content, as well as placing other restrictions on their activities, we believe that this is entirely proportionate to the risk of harm.

Support for measures such as a smartphone-free childhood or a ban on social media for children. When combined with other measures, we believe that PARCEP provides a mechanism that helps demonstrate that children can continue to enjoy the benefits of relatively unrestricted access to the Internet.

We propose either initiating a new IETF working group or aligning this work under an existing group if it fits within the charter. The work should commence with the publication of a formal problem statement and the development of a draft architecture. Collaboration with child rights experts, standards bodies, platform engineers, and regulators will be essential in developing a solution that is effective, inclusive, and sustainable.

We welcome discussion and participation from all sectors in shaping PARCEP into an open standard that meets the needs of families, not just today, but in the years to come.

About the Authors

[i] **Andrew Campling** is Director of 419.Consulting™, a consultancy offering public policy, public affairs and marketing strategy guidance to companies in the tech and telecoms sectors. In addition, he is a trustee of the Internet Watch Foundation, a charity focused on the elimination of child sexual abuse imagery online.

[ii] **David Wright** is CEO of SWGfL, a UK-based charity dedicated to promoting and ensuring the safe and secure use of technology for everyone, especially within educational and youth settings. He is also a Director of the UK Safer Internet Centre, a partnership of three charities with a shared mission to make the internet a safer and better place for children and young people; it is part of the Insafe network of Safer Internet Centres across Europe.