Age Assurance and the Role of Network Operators

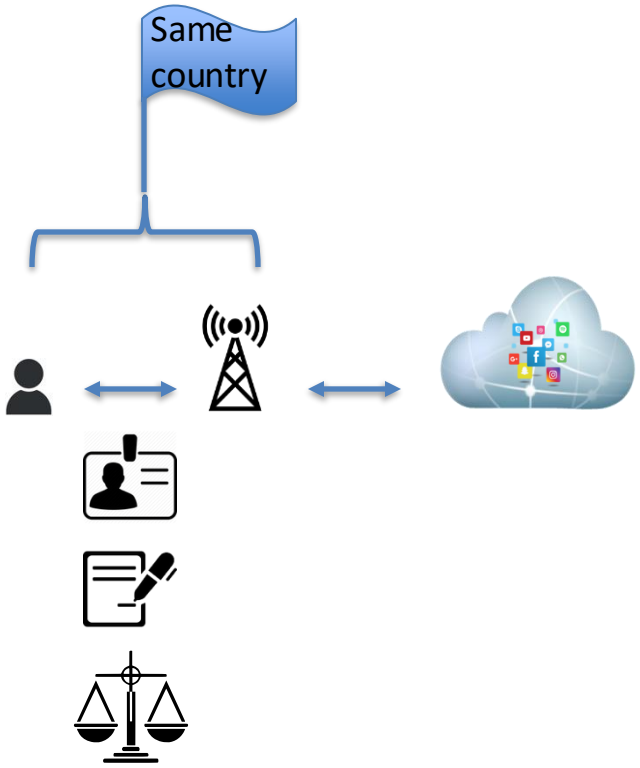
Workshop on Age-Based Restrictions on Content Access

Gianpaolo Angelo Scalone & Kevin Smith – Vodafone Group

Global Context

- **Europe**
  - Digital Services Act (DSA) - framework for age assurance
  - UK Online Safety Act – age checks for harmful content, default all users to “child” status until they undergo age verification
  - Italy AGCOM mandate – ISPs must block adult sites
  - France ARCOM – similar blocking mandate
  - Germany JMStV – covers pornography and violent games
- **Asia-Pacific**
  - Australia’s eSafety Commissioner,: Roadmap for Age Assurance
  - South Korea & India: SIM registration tied to ID documents
  - Japan & Singapore: youth online safety codes
- **LATAM & Africa**
  - Nigeria & Kenya: SIM biometric registration
  - Brazil & Chile: ANATEL & child protection initiatives
- **Middle East**
  - Mandatory ISP blocking of gambling, political or social media sites
- **United States**
  - Fragmented: Utah S.B.152, Louisiana H.B.142, California Age-Appropriate Design Code

Why Operators are Unique



- **Operators are distinct because**:
  - Contractual relationship with subscribers → billing, service terms, customer support
  - License to operate → obligations (security, lawful intercept, consumer protection, sometimes child protection)
  - Jurisdictional alignment → same laws/regulator as user
  - Identity-linked accounts → in many countries, ID required at sign-up (SIM/broadband)
  - Operators = *legally accountable enforcers*
- **Examples**:
  - South Korea & India – mandatory ID for SIM registration
  - Kenya & Nigeria – SIM re-registration programs with biometrics
  - EU – some ISPs offer voluntary "child filter" options tied to contracts
  - U.S. – ISPs licensed by FCC/FTC rules, but less tied to ID verification

Definitions of “Adult Content” Local vs Global

- **Not uniform across countries:**
  - Sexual/explicit → almost always adult
  - Weapons → restricted in some (e.g., Germany), not in others (e.g., U.S.)
  - Gambling → regulated in EU/Asia; variable in U.S. (state-level)
  - Social networks (market place) → restricted in some regions (China, Middle East)
- **Global providers:**
  - can classify content technically, but not always match local legislation
- **Operators:**
  - licensed locally → know and apply the local definition of adult content

Operators Know the Law, Not Always the Content

- **Obligation: comply with local legislation (blocking/age assurance rules)**
- **Challenge:**
  - Encryption (HTTPS, DoH, QUIC, ECH) → traffic opaque
  - Operators cannot always see or classify flows
- **Implication**:
  - legal accountability without full technical visibility
- **Mitigations**:
  - Metadata-based enforcement (DNS filters, tokens, categories)
  - Content-provider labeling/self classification
  - Federated assurance with independent providers
  - Policy alignment to recognize encryption limitations

Categorization in Practice

- **Vendors** (e.g., Forcepoint, Netsweeper, Palo Alto, Cisco Umbrella)
  - provide micro-categories (hundreds: pornography, gambling, violence, alcohol, etc.)
- **Operators** aggregate them into macro-categories aligned with:
  - Local legislation (e.g., gambling = 18+ in EU; weapons vary)
  - Parental profiles (“child safe,” “teen safe,” “adult”)
- **Strengths**:
  - scalable, legally aligned, non-intrusive
- **Limitations**:
  - Mostly domain-level, not per-content
  - Multi-purpose platforms hard to classify
  - Dependent on Vendor accuracy & updates required

Operator Leverage Points

- **Traffic Classification & Filtering**
  - DNS/IP blocklists, DPI (obsolete)
  - Australia, India, UK “Family Friendly Filters”
  - Italy AGCOM mandates, some U.S. ISPs with “family filters”
  - Challenges: encryption, over-blocking, privacy risks
- **Subscriber Age Attributes**
  - Linking age claim to subscriber record (South Korea, LATAM pilots)
  - U.S.: less common, but ISPs could, in theory, assert account-holder age
- **Parental Control Models**
  - DNS filters
  - operator apps
  - Home router controls
- **Federated / Hybrid Systems**
  - Operator enforces after third-party age verification (euCONSENT pilot, Asia)

Cross-Cutting Technical Considerations

- **Privacy vs compliance:**
  - GDPR (EU), Convention 108+, state/federal laws (U.S.)
- **Encryption & Internet Architecture:**
  - DoH, QUIC, ECH reduce visibility
- **Scalability & interoperability:**
  - roaming, multi-device households, global platforms
- **User experience**
  - risk of friction vs parental empowerment
- **Architectural alignment:**
  - consistency with end-to-end principle

Emerging Questions

- Should operators be **primary enforcers** or **enablers** (via APIs, e.g. Camara knowYourCustomerAgeVerification)?
- How can national obligations (e.g., SIM ID in Asia, state laws in U.S.) coexist with global Internet services?
- How to design privacy-preserving operator roles?
- How sustainable are operator roles under increasing encryption?
- Can vendor categorization + parental empowerment + operator enforcement be integrated?

Closing

- Operators are **licensed, regulated, and contracted** with users → unique legal position
- They have technical leverage points, but face encryption & architectural limits
- Practices vary widely:
  - Asia, Africa, LATAM → strong ID-tied operator role
  - EU → privacy constraints, some country mandating
  - U.S. → fragmented, platform-centric regulation with some ISP tools
- No universal model → need for discussion on proportional, privacy-preserving operator roles

Thank you

Gianpaolo Scalone / gianpaolo-angelo.scalone@vodafone.com
Kevin Smith / kevin.smith@vodafone.com

Wrap-up

- Network operators have unique advantages in age verification due to proximity to the customer.
- Content providers excel in content classification due to control over content.

- Split-trust models offer a promising path: operators verify age, providers classify content.
- Collaboration is essential for detailed classification (e.g., social media).