“Parental Control”
‘on device controls’ primer

qoria.com

Qoria

Background

Parental controls are generally seen through the prism of the (limited) capability of ‘old school’ home web filters and more recently through the ‘hackable’ apps on smart devices or ‘avoidable’ parent settings in games and social media accounts.

This perspective does parental controls a disservice. We prefer to call the area “**safety technology”**.

Other misnomers

Safety technology is not just for parents

- Safety technology is deeply ingrained in educational environments
- Filtering is mandated by regulations (UK:KCSIE, US:CIPA) and duty of care
- In school/enterprise markets OS provider APIs have driven a dynamic and competitive market with comprehensive safety options *
- Research shows that **adults and children** also want safety technology **for themselves**

* The OSs do not YET provide similar capabilities for consumer markets

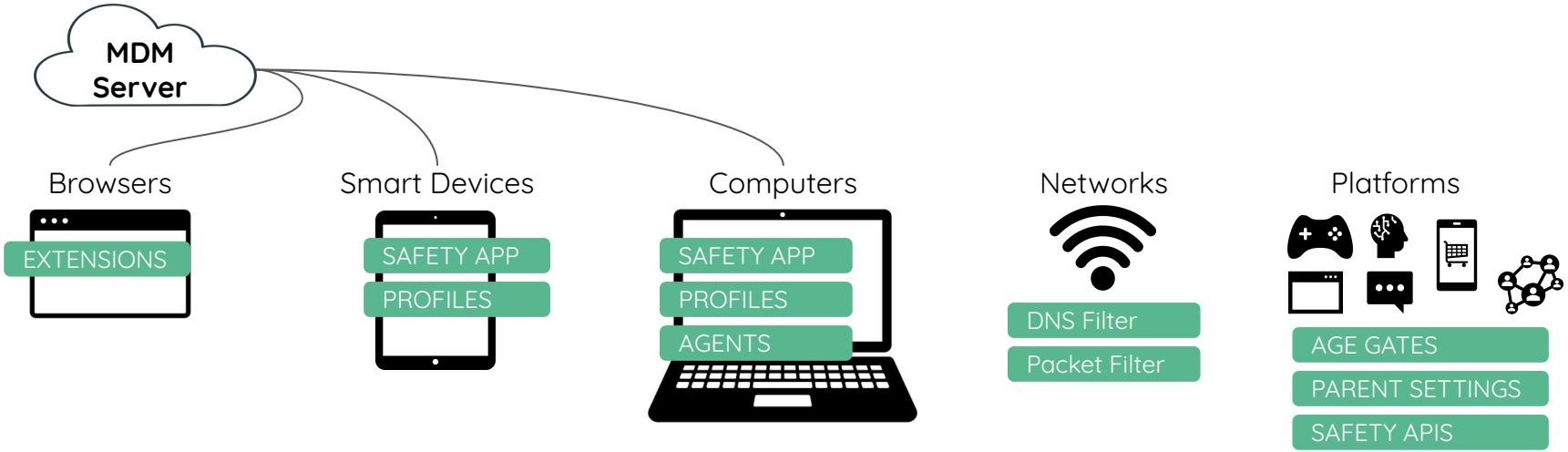
Qoria

Other misnomers

Safety technology is not only about control

- The world has moved on from “blocking stuff”; that does not work
- Repeated blocks will often lead to circumvention attempts
- Safety technology works best when parents, schools and students are empowered and engaged - this is proven by data
- It requires supporting access, respecting privacy & agency
- Legislation (eg GDPR) supports this

Typical capabilities and implementations



BROWSER SAFETY

Chrome, Edge & Safari permit

> install of extensions

Offer full unencrypted access to content.

SMART DEVICE SAFETY

Apple & Google MDM/EMM permit:

> install of profiles

> install of network filters

> use of OS safety features

COMPUTER SAFETY

Apple & MSFT MDM/EMM permit:

> install of profiles / agents

> install of network filters

> use of OS safety features

NETWORK SAFETY

Firewalls and networks can intercept DNS and internet requests for monitoring and control.

Impacted by evolving privacy protocols.

PLATFORM SAFETY

Platforms can enable:

> AA / AV gates

> Parent, privacy settings

> APIs for device signals

> APIs for account scanning

Clearing some things up

Safety v rights, privacy, censorship, easy of use and hacking

Is safety tech an invasion of **child rights**?	**No** - parents & schools have established rights/duties Parents and schools (loco parentis) have a right and duty to act in support of a child's welfare.
Is safety **incompatible** with **GDPR and similar**?	**No** - the child's best interests is a lawful basis If implemented with clear purpose limits, data minimisation, transparency, proportionality, and strong security the safety technology is compliant.
Does safety tech equal **censorship**?	**No** - this is the point of safety technology Access & moderation imposed by the state is a concern. Delegated parental & school responsibility guards against accusations of censorship.

Clearing some things up

cont.

Is safety tech **incompatible with privacy**?	**No** - it does not need to be Privacy preserving techniques are readily available (eg device level policy tokens / signals, children's accounts and parent consent).
Is safety tech **too hard for parents** to use?	**No** - competition in safety technology solves for this Unequivocally capabilities and experiences are getting better and easier, particularly in interoperable fueled & competitive enterprise environments.
Is safety tech **too easy to** bypass by kids?	**No** - however a lack of interoperability creates the gaps It depends on the deployment. For example enterprise deployment of on-device safety tech is extremely robust.

Trust is Key

A trusted 3rd party is essential in on device control.

- The OS vendors leave too many blind spots
- Many people have low trust in “big tech”
- There are too many competing priorities
  - Would advertiser revenue trump safety?
  - “Big tech” have largely had to be legislated into good behaviour
- Categorising content can be subjective - we may want parents and schools to exercise choice here
  - “Big tech X says this LGBTQ site is porn, therefore it is everywhere, for everyone”

Tech challenges: Onboarding

- There are issues getting software on personal devices
  - OSs do not promote or streamline onboarding 3rd party options (but they could)
  - OSs limit anti-tampering features to 1st party and enterprise apps
- Schools have it easier with MDM
- Recently there's growing regulatory pressure (e.g. EU DMA) and acceptance of the need for interoperability

Ultimately the OSs and platforms need to embrace interoperability for safety to be a reality.

Tech Challenges: The stuff that’s not web

- “Being online” is not “the web” as it has been for a few years
- We need to moderate more than just content
- These platforms are often closed
  - IM/Voice/video chat - wether with a human or AI
  - Games platforms
  - Etc..

Tech challenges: Web content

- Many on-device filters still use the same techniques as network filters
  - Proxying (inc MiTM) - works, but increasingly poorly, esp. nn mobile
  - DNS - a blunt instrument, that's increasingly hard to enforce
- Web-in-disguise apps like instagram pin certs and are quite opaque
- There are some vendor APIs, but these are generally quite limited (eg Apple's web filter framework)
- True content filtering is essential
  - The modern web is converging on a small number of platforms
  - URLs are increasingly ephemeral and non-semantic

State Control & Circumvention: Open Issues

- How can we ensure children can't easily acquire unsafe devices?
  - Devices should be safe by default with 1st & 3rd party options
  - **Critically** this empowers parents to protect their children
  - Burner and jailbreaks unavoidable - but mainstream protection is possible
- How could child safety orgs sign up to implement local regulations?
  - Do legislators provide ways to identify content?
  - Perhaps labelling would help here
- Everything is circumventable, ultimately
  - Moves the difficult into tech, rather than chasing a long tail of recalcitrant publishers (the fox guarding the henhouse)