Submission to Children, Education and Home Affairs Scrutiny Panel

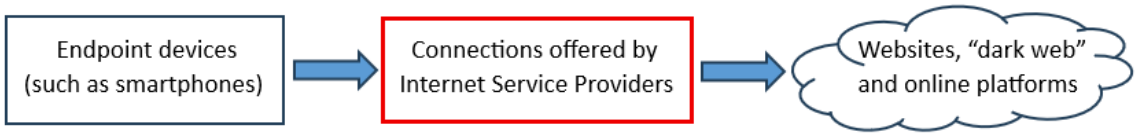
Re: What protection do children in Jersey have from online harms?

I warmly welcome this scrutiny and I have read the departmental submissions with interest. I am concerned that there are many references to discussions and considerations in the Ministerial replies but there is a paucity of evidence regarding newly-developed actions and a future vision linked to specific timescales.

In my submission, I would like to focus on one aspect of protection from online harm; the ability to filter content before it is delivered to children's mobile devices. In particular, I am focusing on network-level filtering by Internet Service Providers (ISPs), which has been in place in the UK since (at least) 2014.

Context

Public debate about online harm tends to focus on hardware devices and is epitomised by the call to ban smartphones from schools. This is, however, a very limited view of the problem as the devices themselves are not synonymous with online harm. Devices are at one end of the digital communications chain that has websites and online platforms at the other end, linked by Internet Service Providers through mobile data and broadband connections.



Point 1: **There can only be a risk of online harm if the device is connected to online services.**

This fact is recognised in various submissions;

- In his submission, the Minister for Children and Families refers to Sophos endpoint device management software, which monitors and filters online content delivered to children's own devices when they are connected to Wi-Fi networks in settings that are part of Residential Services (Question 3) but also notes "there is currently no need to oversee and monitor the use of technology when attending a youth club" because "the Jersey Youth Service does not currently provide any devices for young people to access the Internet" (Question 14).

  Is the act of not providing devices sufficient grounds for obviating Youth Clubs' duty of care?
- In his submission, the Minister for Education and Life-long Learning states that for personally-owned devices taken into school "the web filtering policy will be applied to all devices connected to the Wi-Fi provided" (Question 6) and the "Lightspeed Filter protects mobile devices connected to the Wi-Fi provided in schools from harmful content" (Question 13).

  These responses refer only to Wi-Fi networks and overlook the fact that children are also at risk of online harm in schools when they access the Internet using mobile data connections.

The Minister for Education and Life-Long Learning, in response to Question 7c, states "None" of the Government of Jersey schools are without systems to check ***all*** (my emphasis) online activity. This is untrue because online activities carried out through mobile data connections, regardless of whether their use contravenes schools' policies and acceptable use agreements, cannot be monitored using schools' systems.

Point 2: **There is a significant shortfall in the online protection that is afforded to children in Jersey due to the lack of voluntary measures and formal regulation of Internet Service Providers.**

In the UK, ISPs block 18+ content by default (it can be removed using credit-card age verification) and also offer other filtering profiles to protect young children and teenagers. This filtering was introduced more than a decade ago as a result of work undertaken by the UK's regulator for communications services,

Ofcom, which is empowered to "make online services safer for the people who use them, by making sure companies have effective systems in place to protect users from harm." (https://www.ofcom.org.uk/about-ofcom/what-we-do/what-is-ofcom). Significantly, TalkTalk introduced voluntary (opt-in) web filtering in 2011, two years prior to Ofcom's initiative and more than three years ahead of the UK's legal requirements (https://www.infosecurity-magazine.com/news/talktalk-introduces-first-isp-level-malicious-url/).

Jersey's ISPs do not fall under Ofcom's remit so have not been compelled to act in the same way as UK ISPs and nor have they acted voluntarily by offering opt-in services to users. To compound matters, Government of Jersey has not seen fit to create its own regulator for communication services or, more recently, to oversee the prevention of online harm. *Perhaps now is the time for such a body to be inaugurated?*

Point 3: **Why have Ministers not required Jersey's ISPs to offer network-level protection to users?**

The risks of online harm exist for all children regardless of where or when they happen to be online: Jersey's children are no exception. It is lamentable that the UK introduced these measures more than a decade ago yet there has been no visible progress in this direction in Jersey throughout that period.

> *In the absence of voluntary (opt-in) measures, the Government of Jersey should require all on-Island ISPs to introduce network-level filtering that is active by default and customisable by the contract holder (over 18s). The timescale for the implementation of network-level filtering should be specific and brief, having been achieved in the UK within an 18-month deadline.*

"In a July 2013 speech, the Prime Minister announced a series of agreements the Government had secured with mobile operators, Internet Service Providers (ISPs) and public wi-fi operators that put adult content filters on mobile phones, public wi-fi networks and home networks. The four main ISPs have begun offering these filters to all new customers and existing customers should also be offered the choice of installing a filter by the end of 2014." (https://commonslibrary.parliament.uk/research-briefings/sn07031/).

Point 4: **It is simply not good enough to be "following current activities" elsewhere when there has been more than a decade of inaction on network-level filtering for ISPs in Jersey.**

The Minister for Sustainable Economic Development stated "addressing online harms is a cross-ministerial issue" (Question 8) and "there is a consensus across Government that children should not have access to material that is not age appropriate," adding "we are following current activities in the UK and in the EU who are looking for ways to introduce a more robust age verification process of users".

> *The Minister for Sustainable Economic Development is correct in stating current age-verification processes can be circumvented but this is not a reason for inaction. There will probably never be a foolproof method of age-verification, nor of network-level filtering in general, but if we claim to be waiting for such a solution then we will wait for ever. It is better to do something than to do nothing.*

In his submission, the Minister for Sustainable Economic Development states that imperfect age-verification systems "provide parents with a false sense of security" (Question 9). This will be true for some parents but age-verification and network-level filtering will be effective in blocking some content. In line with best practice, the efficacy of any introduced measures should be monitored and reported to quantify their effectiveness and allow parents to assess their own level of confidence in the steps that have been taken (see Evaluating Online Safety Measures: Economics Discussion Paper Series Issue 10, Ofcom, May 2024, https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/economic-discussion-papers-/evaluating-online-safety-measures.pdf?v=360945).

Jon Tarrant
May 2025