Public Affairs Update

Malcolm Hutty
Executive Director, Legal & Policy

24th November 2022
LINX 117

Telecoms Security Act

Changes to implementation timeframes

Previous				Final		
Phase	Tier 1	Tier 2		Phase	Tier 1	Tier 2
				Initial	March 2024	
1	March 2023	March 2025		1	March 2025	March 2025
2	March 2025	March 2027		2	March 2027	March 2027
3	March 2026	March 2028		3	March 2028	March 2028

Code to be made final: December 2022

Moving between tiers

For the purposes of applying guidance set out in the code of practice, an existing tier designation will apply to a provider until ~~either of the following criteria are met~~:

- The provider has been outside of their existing tier's range for at least two years~~; or,~~
- ~~The provider is above or below their existing tier's range by more than £10 million~~.

National isolation (1)

- Remove the requirements that operator be able to
  - Identify the risks of security compromises occurring; and
  - To operate the network for one month at normal capability

  without reliance on people, systems or data outside the UK

- Remove the requirement to identify risks that would make the above necessary

National isolation (2)

- Retain requirement in regulations for some degree of resilience within the UK
- Updated draft code of practice to explain four types of risk scenarios that could necessitate a reduced reliance on certain non-UK capabilities
- Amended the draft code measures -
  - network providers shall have the ability to maintain within the UK fixed and mobile data connectivity to UK peering points, mobile voice services, and text-based mobile messaging.

Scenarios

1. Loss of access to assets in a specific country or region
   - due to (e.g.) natural disaster or geopolitics;

2. Compromise of non-UK group functions, where parent company located outside the UK;

3. Disruption to transport or telecoms links between UK and RoW
   - due to (e.g.) natural disaster or geopolitics

4. failure of internet routing, where the failure of multiple major global providers, transit routes, or widespread hostile routing updates, or geopolitics cause failure of internet routing, or internet routing protocols, such as eBGP

Privileged Access Workstations

Industry request:

- virtual PAW to accept inbound connection over an insecure network from an approved (VDI) application with compensating controls
- browse up to a virtual PAW from a VDI application with compensating controls
- browsing from third party physical PAW to a virtual PAW within a provider environment

Government Response

- Rejected
- Ask NCSC to work with industry "to provide further clarity on intent"

Patching

Industry request

- Reduce the administrative burden from recording all patches that take longer than 14 days to apply
- Take a risk-based approach to patching rather than the 14-day requirement

Government Response

- Accepted: changes made to include a risk-based approach in this scenario
- More detailed guidance on when patches taking more than 14 days is considered reasonable

“Legacy networks”

- No definition of a “legacy network”
- Some guidance added to the Code on ‘proportionality’ of requirements “where there is a demonstrable plan for removal”

Online Harms Bill

Brief Recap

Summary

- Long-awaited Bill for regulating user-generated content online
  - "User to user services" and "search services"
- Regulates illegal content, "harmful to children" and "harmful to adults"
  - Bill designates "priority illegal content"
  - Future Regulation extend, and designate "priority content harmful to" children and adults
- Extensive duties for risk assessment and "mitigating the risk of harm"
  - Including systems to prevent individuals encountering "priority illegal content"
  - Must assess each type of content separately
  - Must assess differentially for harm to children "with a certain characteristic" or "of a certain group"

Political uncertainty

- When first introduced the Online Harms Bill received little political opposition
  - Mostly, in Committee, from the perspective that major online platforms should be treated even more strictly
- Late in legislative process, some media comment criticising impact on freedom of expression, "heckler's veto"
- During Conservative leadership election campaign, Kemi Badenoch raised profile of concerns about freedom of expression significantly, and Bill was placed on hold
- As Prime Minister Liz Truss said Bill would be brought back "as a priority" but aspects on freedom of expression would be "tweaked"

Latest pronouncements

- Michelle Donelan, the latest Secretary of State at DCMS said of "legal but harmful" content on BBC Radio 4 Today programme

  "that's the bit we will be changing. That element in relation to adults".

  "The bits in relation to children and online safety will not be changing"

Content harmful to children

Summary of children's risk assessment duties (s.10)

- Duties to
  - Carry out "suitable and sufficient risk assessment" of content likely to be accessed by children
  - Keep it up to date, including when Ofcom makes a change to "risk profile" that relates to services of the kind in question
    - At least every year
  - Make a further risk assessment before making "any significant change to any aspect of a service's design or operation"
  - Notify Ofcom of
    - the kinds of content identified by a risk assessment; and
    - the incidence of those kinds of content.

What is a children's risk assessment (1)

- An assessment of
  - The user base
  - The level of risk of children who are users of the service encountering
    - Each kind of content of each classification that is harmful to children (out of "primary priority content", "priority content" and "non-designated content harmful to children");
    - With each kind of content separately assessed;
    - Giving separate consideration to children in different age groups; and
    - Taking into account how easily, quickly and widely content may be disseminated by means of the service

What is a children's risk assessment (2)

- An assessment of
  - the level of risk of harm presented by different kinds of content that is harmful to children, again giving separate consideration to children in different age groups
  - The level of risk of harm [...] which particularly affects individuals with a certain characteristic or members of a certain group
  - The level of risk of functionalities of the service facilitating the presence of disseminate content harmful to children, including
    - Ability for anyone (including adults) to search for users;
    - Ability for anyone (including adults) to contact users
  - The different ways in which the service can be used, and the impact of that on the level of risk of harm to children
  - The nature and severity of the harm in all the above
  - How the design and operation ("including the business model, governance and use of proactive technology" etc) may reduce or increase the risks identified

Safety duties protecting children

- Duty to
  - Mitigate and mange *risk of harm* presented by content identified in risk assessment
  - Mitigate the impact of harm
  - Prevent children of any age from encountering primary priority content
  - Prevent children in age groups likely to be harmed by other content from encountering it
  - Include protective provisions in the terms of service
  - Apply those terms of service provisions consistently
  - Give information about any proactive technology used in terms of service

All the above to be "proportionate", and when considering proportionality must take into account *each* risk assessment, as well as size and capacity of service provider.

So what is “likely to be accessed by children”?

- Content is deemed “likely to be accessed by children
  - If it is possible to be accessed by children; and
  - Either
    - There are “a significant number of children who are users of the service”; or
    - The service is “of a kind likely to attract a significant number” of children

- “A provider is only entitled to conclude that it is not possible for children to access a service if there are systems or processes in place […] that achieve” that result.
  - E.g. age verification systems

- Content is also deemed “likely to be accessed by children” if
  - An assessment of whether it is likely is not performed (or recorded) properly; or
  - Ofcom investigates the adequacy of the assessment and decides that it is likely to be so accessed

Personal musings (with which the government would vigorously disagree)

Would deleting "harmful to adults" even matter?

Go forth and multiply

Parameters for number of individual assessments to be made:

- "Find the level of harm for":
  - Number of categories of harmful content to be considered
  - Number of age groups
  - Number categories of "particular characteristics" or "membership of particular groups"

- For each of those level of harm assessments
  - For each of the number of different ways the service can be used,

  find the impact on the level of harm of the way in which it is used

- For each of those "use impacts"
  - For each type "aspect" to be considered (governance, business model, etc)

  Find the ways in which that aspect can increase or reduce the impact

What are the practical options for a service provider?

- They could restrict access to the service with an (approved?) age-verification scheme
  - Likely this makes the service completely non-viable (whether commercial or otherwise)

- They could attempt to comply fully with the child risk assessment duties
  - Tantamount to an impossible task

- (In reality, many smaller providers)
  - Make some more or less superficial attempt at compliance with the child protection duties
  - Hope that their service is deemed sufficiently low risk it isn't targeted for enforcement action
  - *Desperately avoid being the subject of controversy that might lead to full impact of the child protection duties being unleashed on them via enforcement.*

linx

Questions

linx

Malcolm Hutty

malcolm@linx.net

linkedin.com/company/linx/

facebook.com/LondonInternetExchange/

twitter.com/linx_network

youtube.com/user/LINXnetwork