An introduction to the Telecoms (Security) Bill and the Digital Services Regulation

LINX112
February 2021

Malcolm Hutty

18/02/2021

Agenda

1. Telecoms Security Bill
2. Digital Services Regulation (EU)
3. Forthcoming events

To be notified of forthcoming events or when more information is available, please e-mail publicaffairs@linx.net

1

Telecommunications (Security) Bill

Background

- Existing security requirements for network operators are contained in s105A – s105D of the Communications Act 2003
  - These were inserted as a result of changes to the Telecoms Framework Directive in 2007, now the European Electronic Communications Code (EECC)
  - IXPs, DNS providers, cloud services etc, are currently regulated separately, but similarly, under the Network and Information Systems Regulations 2018
- The EU proposes changes to extend the EECC requirements (see later)
- The UK is separately extending/replacing these requirements – a lot

Three elements of the Bill

- A duty to notify "others" of security compromises
- Extensive new requirements to implements
  - Preparatory and preventative security measures;
  - Incident response measures
- Designated vendor directions
  - Limiting or banning the use of particular High Risk Vendors

General: “security compromise”

- A new definition of “security compromise” is created
  - Covers compromise to availability, performance or functionality of the network
  - Any compromise to confidentiality of data (“signals”) transmitted
  - Also covers unauthorised access, exploits and preparatory exploits

- This is potentially more encompassing than the previous “security incident”

Notifying Ofcom of security compromises

- Extends the existing duty to notify Ofcom of security incidents with significant impact
- Applied to the new definition of security compromise
- Emphasises notifying compromises that seek to secure further/later access
- New obligation to inform users who may be affected of the *risk* of a compromise
  - NB: not just an incident that occurred
  - Must recommend mitigation measures
- Powers for Ofcom to inform (a) government bodies (b) users and (c) the public about risks of compromise

Designated vendor notices and directions

- Government is taking a power to name specific High Risk Vendors, so as to apply rules specifically to each HRV individually
  - Called a "designation notice"
- The designated vendor will be informed they've been designated, and may be told what rules have been applied in respect of them
  - But the rules can be kept secret too
- The Secretary of State will issue a designation notice when he considers it necessary in the interests of national security
  - There is a right for the HRV to be consulted, but no right of appeal
  - This power is technically subject to judicial review
  - However, as done "in the interests of national security", in practice highly resistant to judicial review – courts will not second guess necessity

Designated vendor directions

- "Designated vendor directions" will be orders from the Secretary of State to a public network operator about a "designated vendor"
  - i.e. about a vendor named in one of those designation notices
- These grant the Secretary of State broad powers to (for example)
  - Ban installation of new equipment / services from that vendor
  - Remove existing equipment / discontinue use
  - Implement specified mitigations, processes, technical controls around such equipment / services
  - Set deadlines for implementation
- Designated vendor directions are addressed to individual network operators
- Again a (qualified) right to be consulted, but no right of appeal

Designated vendor directions (2)

- Additional powers and duties for Ofcom, including
  - Powers to obtain information from network operators subject to a notice
  - Duty to make reports to the Secretary of State
  - Powers to conduct inspections
- Penalties for non-compliance (up to 10% of turnover and £100,000 per day), imposed by Secretary of State (not Ofcom)
- Urgent enforcement directions
- Designated vendor directions can be published (laid before Parliament)
  - But can be redacted or kept secret in the interests of national security
  - Network operator can be placed under a duty to keep secret parts secret

Telecoms Security Requirements

- The Bill creates
  - A general duty for network operators to take measures to
    - Identify risks of security compromises;
    - Reduce risk of compromises occurring; and
    - Prepare for incidents
  - A power for the government to make regulations requiring network operators to take specified measures
  - A power to issue "Codes of Practice" describing what the regulations require
    - Informally known as the "Telecoms Security Requirements" (TSRs)

- The government has published draft Regulations and a draft Code of Practice

Hierarchy of requirements

The Telecoms Security Bill	Binding on everyone	Only provides legal framework: No explanation of what you actually need to do
Regulations	Binding on everyone	Describe in principle what must be done
Code of Practice	Not binding May not be applied to smaller operators	Specifies in more detail the measures the operator must take

Example of breakdown

Regulations	Code of Practice
A network provider must have in place, and use where appropriate, means and procedures for isolating security critical functions from all signals which the provider does not believe on reasonable grounds to be safe.	Operators implement a 'protocol break/DMZ' to isolate their core network from external signalling networks.
	The management plane used to manage Network Oversight Functions shall be isolated from other networks, including the management plane used by other equipment.

Counting the obligations

- Breaking down the Regulations and Code requirements into separately itemised requirements so as to perform a count is not an exact science

- However, as an indication of the relative levels of detail, LINX counts
  - 10 full Regulations, which we break down into
  - Around 90 separate requirements for operators in the Regulations; and
  - 357 requirements from the TSRs and the associated Cyber Assessment Framework to which it refers

Stated policy on implementation

- Government has said three tiers of operators will be recognised:

Tier One: largest operators	➢ Must follow the Code ➢ Will be subject to extensive oversight from Ofcom
Tier Two: many operators	➢ Must follow the Code ➢ Less oversight from Ofcom
Tier Three: very small operators	➢ Must follow the Regulations in principle ➢ Not Ofcom's focus

- This is not actually written into the Bill, the Regulations, or even (yet) the Code

Deadlines

- Over the course of its development, the government has extensively consulted Tier 1 operators about the TSRs (the Code)
- During that time, the TSRs were set out as a five-year programme
  - Various elements were identified as needing to be achieved by the end of year one, year two, etc.
- The published version of the Code makes no mention yet of varying deadlines
  - If this becomes final, everything would technically be applicable from Day One
  - Although Ofcom would have a discretion in enforcement
  - The omission may be just because the Code is in draft, and government doesn't want to commit to the specific deadlines yet
  - Alternatively, it may want operators to have to rely on Ofcom's discretion

2

Digital Services Regulation

Introduction

- The European Commission has introduced two proposals for two major new pieces of legislation
  - **Digital Services Regulation** – an overhaul of the regulation of Internet intermediaries in respect of Internet content, replacing the provisions of the E-Commerce Directive 2001
  - **Digital Market Regulation** – entirely new legislation to provide sector-specific economic/competition regulation for "gatekeeper platforms"
- This presentation is about the first, and not the second

- Both are intended to become *Regulations*
  - i.e. have direct effect in law across the EU
  - Contrast with the E-Commerce *Directive*, which had to be implemented by Member States

Background: the E-Commerce Directive

- The E-Commerce Directive 2001 is the bedrock of Internet content regulation in the EU
- It contains two main elements
  - It establishes the "Country of Origin" principle, that online services are regulated under the law in the country in which they are based, not under the law in each country in which their users live
  - It creates liability shields for Internet intermediaries
    - **Mere conduits** have absolute immunity from liability for content that merely passes over their network
    - **Hosting providers** have immunity until they have actual knowledge of the content they are hosting
    - **Caching service providers** have immunity so long as the cache is not allowed to contain stale data, acting as an independent source once the originator has removed it.
  - The shield has "horizontal effect" i.e. it applies to all types of content

Historical background

- In 2001 the Internet was seen as a nascent industry that needed protection from premature regulation that could not foresee future development in a rapidly changing sector
  - This was before Facebook, YouTube or Twitter were founded
  - Yahoo! was the world's most popular search engine
  - Amazon was a bookshop
  - Apple launched MacOS X; later that year, it also launched the iPod

Recent political context

- The last 20 years has seen a succession of initiatives intended to make Internet intermediaries take more responsibility for Internet content
  - These have been "vertical" i.e. focussed on a particular type of content

- Each Commission/Parliament has faced pressure from some Member States to "review" the E-Commerce Directive
  - This would challenge the "bedrock" nature of the liability shield, potentially inserting loopholes that would eliminate its practical value
  - Commission and industry both resisted, until now
  - With this proposal, the Commission attempts a new framework that is not about either maintaining the status quo nor simply removing the liability shield

Summary of main provisions

- The liability shield is retained
  - Word for word copy from the E-Commerce Directive
  - Only change is to exclude online marketplaces from "hosting providers"
  - Prohibition on obligation for general monitoring also retained
- Notice-and-action by hosting providers once notified becomes a statutory process
- Substantial new obligations for most hosting providers and more for "very large online platforms"
- Extra-territorial effect
  - Country-of-origin applies *within* EU, but EU expects Country-of-reception to apply between EU and non-EU countries

Types of intermediary

- Mere conduit, hosting and caching providers retained
  - No changes to requirements for mere conduit or caching providers
- New category of "online platform"
  - **Important:** Under the Commission's proposals *most* hosting providers would be re-classified as 'online platforms'
- New category of "very large online platform"

“

‘online platform’ means a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation.

Article 2(h)

”

“

‘online platform’ means a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation.

Article 2(h)

”

Hosting service / online platform?

- A website would not be an online platform if it contains no user-generated content at all
  - But the hosting service provider for the website would be
- A website with an online forum would be an 'online platform' unless the UGC was "a minor and purely ancillary feature"
- Likewise, a mobile app that disseminates UGC will be an 'online platform' unless the UGC was "a minor and purely ancillary feature"
- Cloud storage would not be an 'online platform' if there is no content sharing feature or it is sharing within the enterprise only
  - No 'dissemination to the public'

Cumulative obligations

	VERY LARGE PLATFORMS	ONLINE PLATFORMS	HOSTING SERVICES	ALL INTERMEDIARIES
Points of contact	•	•	•	•
Legal representatives	•	•	•	•
Terms and conditions	•	•	•	•
Reporting obligations	•	•	•	•
N&A	•	•	•	
Statement of reasons	•	•	•	
Complaint handling	•	•		
OOC	•	•		
Trusted flaggers	•	•		
Abusive behaviour	•	•		
KYBC	•	•		
Reporting criminal offences	•	•		
Advertising transparency	•	•		
Reporting obligations	•			
Risk assessment and mitigation	•			
Independent audits	•			
Recommender systems	•			
Enhanced advertising transparency	•			
Crisis protocols	•			
Data access and scrutiny	•			
Compliance officer	•			
Reporting obligations	•			

CUMULATIVE OBLIGATIONS!

New obligations for all intermediaries

- To establish a single point of contact for Member State regulators
- To have a legal representative in the EU
  - NB: These will be responsible for ensuring compliance, not just a PO Box!
- To publish terms and conditions that respect fundamental rights
- Annual transparency reports on content moderation

New obligations for *all* hosting service providers

- Statutory Notice-and-Action mechanism
  - For removal of illegal content
  - Notices meeting the requirements of the mechanism shall be deemed to impart "actual knowledge"

- Duty to give written statement of reasons for removal or non-removal under N&A
  - Detailed list of elements the statement must contain

New obligations for “online platforms”

- Statutory complaint handling process
  - Acts as appeals mechanism for notice-and-action
- Out-of-court dispute resolution mechanism
- Accept reports from ‘Trusted flaggers’
  - Status as ‘trust flagger’ to be granted by national regulators?
- Duty to notify law enforcement of suspected serious crimes
- Know Your Business Customer rules
- Transparency obligations for any advertising content shown

- Remember, this means most hosting providers with UGC
- But small and micro entities are exempt

Very large online platforms

- More than 45 million users per month
- Calculation methodology t.b.d.
- Decision to designate an online platform as a “very large online platform” to be taken by the regulator

New obligations for VLOPs (1)

- Duty to assess risk caused by their platform to society
  - Against a broad range of social and societal harms
- Duty to implement risk mitigation measures for identified risks
  - Could result in open-ended source of new obligations
- Duty to have independent audit of the same, at own expense
- Advertising
  - Archive of advertisements displayed, data on the advertiser, reach and impressions etc.
  - Code of conduct for advertising
- Open access to data for regulators and academic researchers

New obligations for VLOPs (1)

- Transparency reports
  - How ‘recommender systems’ work
  - Report to regulators on risk mitigation
  - Audit report
  - ‘Audit implementation report’ (report on implementation of corrective action demanded by auditor)
- Compliance officer
  - Responsible for ensuring VLOP’s compliance
- ‘Crisis protocols’
  - State co-option of the VLOP to disseminate/promote public information campaigns issued by Member States during “extraordinary circumstances affecting public security or public health”

Additional provisions

- A new set of national regulators, called "Digital Services Coordinators"
- A new 'European Board for Digital Services'
  - Similar to BEREC's relationship with Ofcom etc (the Irish Ofcom, post Brexit!)
- Numerous provisions on enforcement and sanctions
  - Up to 6% of global turnover for one-off fines
  - Up to 5% of daily global turnover for periodic fines (VLOPs only)
  - Powers of inspection, information gathering, to interview staff etc.
  - Own initiative investigations by Commission or Board

To be notified of forthcoming events or when more information is available, please e-mail publicaffairs@linx.net

linx

Thank you