



Public Affairs Update

A Regulator for Online Harms

Malcolm Hutton

LINX105 -
May 2019

Regulating Internet Harms

- 1 (Not) a duty of care
- 2 Harm
- 3 What will you need to do?
- 4 Companies/services in scope
- 5 Out of scope
- 6 Sanctions
- 7 Costs and levies
- 8 Criticism

1

A duty of care



“

A new statutory duty of care to make companies take more responsibility for the safety of their users and tackle harm caused by content or activity on their services.

”

2

Harm



What is harm?

What is harm?

Harms with a clear definition

Child sexual exploitation & abuse

Terrorist content

Organised immigration crime

Modern slavery

Hate crime

Sexting of indecent images by minors

Encouraging or assisting suicide.

What is harm?

Harms with a clear definition

Child sexual exploitation & abuse

Terrorist content

Organised immigration crime

Modern slavery

Hate crime

Sexting of indecent images by minors

Encouraging or assisting suicide.

Underage exposure to legal content

Children accessing pornography

Children accessing inappropriate material

- (under 13s on social media)

- (under 18s on dating apps)

- Excessive screen time

What is harm?

| Harms with a clear definition | Harms with a less clear definition | Underage exposure to legal content |
|--------------------------------------|------------------------------------|---|
| Child sexual exploitation & abuse | Cyber-bullying and trolling | Children accessing pornography |
| Terrorist content | Extremist content & activity | Children accessing inappropriate material |
| Organised immigration crime | Coercive behaviour | - (under 13s on social media) |
| Modern slavery | Intimidation | - (under 18s on dating apps) |
| Hate crime | Disinformation | - Excessive screen time |
| Sexting of indecent images by minors | Violent content | |
| Encouraging or assisting suicide. | Online abuse of public figures | |

What is harm?

| Harms with a clear definition | Harms with a less clear definition | Underage exposure to legal content |
|--------------------------------------|------------------------------------|---|
| Child sexual exploitation & abuse | Cyber-bullying and trolling | Children accessing pornography |
| Terrorist content | Extremist content & activity | Children accessing inappropriate material |
| Organised immigration crime | Coercive behaviour | - (under 13s on social media) |
| Modern slavery | Intimidation | - (under 18s on dating apps) |
| Hate crime | Disinformation | - Excessive screen time |
| Sexting of indecent images by minors | Violent content | |
| | Online abuse of public figures | |

Not really a duty of care

- Not owed to anyone in particular, but to society
- No actual harm to a person need be shown
- No clarity as to what may be regarded as harmful
- Or as to what may cause harm
- Or as to what is an acceptable or unacceptable risk of harm resulting

Actually this is a delegation of legislative authority

3

What will you need to do?

Delegating to a regulator

- White Paper says little about what a company must do to satisfy a duty of care
- Instead, government proposes to create a new regulator for Internet harms
- This regulator will have the power to
 - Define harm
 - Issue Codes of Practice
 - Impose sanctions on companies
- Unclear whether regulator will also have executive power to establish systems and tools

Delegating to a regulator

- White Paper says little about what a company must do to satisfy a duty of care
- Instead, government proposes to create a new regulator for Internet harms
- This regulator will have the power to
 - Define harm
 - Issue Codes of Practice
 - Impose sanctions on companies
- Unclear whether regulator will also have executive power to establish systems and tools

Duties for business

- Ensure their relevant terms and conditions meet standards set by the regulator and reflect the codes of practice as appropriate.
- Enforce their own relevant terms and conditions effectively and consistently.
- Prevent known terrorist or CSEA content being made available to users.
- Take prompt, transparent and effective action following user reporting.
- Support law enforcement investigations to bring criminals who break the law online to justice.
- Direct users who have suffered harm to support.
- Regularly review their efforts in tackling harm and adapt their internal processes to drive continuous improvement.

Some ideas for Codes of Practice

- Steps to ensure products and services are safe by design.
- Guidance about how to ensure terms of use are adequate and are understood by users when they sign up to use the service.
- Measures to ensure that reporting processes and processes for moderating content and activity are transparent and effective.
- Steps to ensure harmful content or activity is dealt with rapidly.
- Processes that allow users to appeal the removal of content or other responses, in order to protect users' rights online.
- Steps to ensure that users who have experienced harm are directed to, and receive, adequate support.
- Steps to monitor, evaluate and improve the effectiveness of their processes.



“

Developing a culture of transparency, trust and accountability will be a critical element of the new regulatory framework.

”



“

The regulator will have the power to require annual transparency reports from companies in scope, outlining the prevalence of harmful content on their platforms

”

Transparency reports: content

- Evidence of effective enforcement of T&Cs “which should reflect guidance by the regulator issued in Codes of Practice”
- Processes for reporting illegal content and behavior
 - Number of reports received and how many led to action
- Proactive use of technology to identify, flag, block and remove content
- Evidence of cooperation with UK law enforcement
- Safeguards for fundamental rights
- Details of investment in user education and awareness raising, including in collaboration with civil society



“

We are consulting on allowing designated bodies to make ‘super complaints’ to defend the needs of users.

”

Transparency reports: process

- When transparency reports required, they will be mandatory
- Regulator will publish transparency reports received from companies
- Regulator may demand algorithm disclosure

4

Companies in scope



“

We propose that the regulatory framework should apply to companies that allow users to share or discover user-generated content, or interact with each other online.

”

Services with user-generated content

- Hosting, sharing and discovery of user-generated content (e.g. a post on a public forum or the sharing of a video).
- Facilitation of public and private online interaction between service users (e.g. instant messaging or comments on posts).

Secondary enforcement

Other companies potentially in-scope for applying sanctions against non-compliant services (under consultation)

- Internet access providers
- Banks and payment services
- Advertising platforms
- Other businesses on which non-compliant services depend



“

The scope will include companies from a range of sectors, including social media companies, public discussion forums, retailers that allow users to review products online, along with non-profit organisations, file sharing sites and cloud hosting providers.

”

Public vs private communications

- For example, there is an obvious difference between one-to-one messaging, and a WhatsApp group of several hundred users.
- However, users should be protected from harmful content or behaviour wherever it occurs online, and criminals should not be able to exploit the online space to conduct illegal activity.

Internet Access Blocking

- Blocking is not the main focus of the White Paper
 - Mainly focused on services that host content
- But blocking access to non-compliant services is proposed as a “backstop” measure
 - E.g. should a foreign service decline to submit to UK regulatory requirements
- Follows the model of porn site blocking recently introduced

5

Out of scope

Out of scope

- All harms to organisations
- Breaches of data protection
- Cyber-security and hacking
- Harms suffered on the “dark web” instead of the open Internet

6

Sanctions & enforcement



“

... when companies do not cooperate
there will be serious consequences.

”



Civil fines

- Civil fines can be tied into metrics such as
 - annual turnover,
 - volume of illegal material,
 - volume of views of illegal material, and
 - time taken to respond to the regulator.

Procedural remedies

- Serving a notice to a company that is alleged to have breached standards, and setting a timeframe to respond with an action plan to rectify the issue.
- Requiring additional information from the company regarding the alleged breach.
- Publishing public notices about the proven failure of the company to comply with standards.



“

However, because of the particularly serious nature of some of the harms in scope, the global nature of many online services and the weak economic incentives for companies to change their behaviour, we think it is likely the regulator will need additional powers at its disposal.

”

Options for further sanctions

- Disruption of business activities
 - E.g. forcing other companies to stop doing business with the company in question (banks, advertising, peering & connectivity?)
- ISP blocking.
- Senior management liability.
 - Personal liability for civil fines
 - Criminal liability

7

Costs and levies



“

The government intends the new regulator to quickly become cost neutral to the public sector.

”



To recoup the set-up costs and ongoing running costs, the government is considering fees, charges or a levy on companies whose services are in scope.



8

Criticism

Major criticisms

1. The “duty of care” isn’t, it’s a delegation of legislative authority.
2. As such, this is technically quite easy to legislate – but the legislation will give little clue as to the requirements or consequences.
3. A quango is being given the authority to determine what speech must be suppressed.
4. That same quango is being given almost unlimited authority to issue almost-binding directions to businesses – any business that carries user-generated content.
5. The purpose of suppressing online harms – by third parties – is a public purpose, but the government proposes to fund it entirely through imposition and levies on private business, not general taxation.



Thank you



malcolm@linx.net