Playing catch up: The Government's White Paper on Online Harms

Gordon Menzies, Six Pump Court

That the law has struggled to meet the challenges posed by the use of the internet has been most poignantly emphasised by the case of Molly Russell, a tragic case which has come to dominate the debate about the need for robust enforcement of harmful online activities. Those familiar with use of the internet in the context of regulatory enforcement and criminal prosecution know that misuse is facilitated by the ease of retaining anonymity and the lack of any effective control by many of those organisations who provide such services. Indeed, examples are often come across of internet service providers who will actively market their services on the explicit promise that they will not disclose users' information to law enforcement agencies.

The two principal steps that the Government have taken so far are, firstly, commissioning a review by the Law Commission of existing criminal sanctions, announced in February 2018, and the recent April 2019 White Paper on Online Harms.

As far as the Law Commission's work is concerned its own terms of reference specifically exclude consideration of the liability of internet platforms that transmit or store offensive or abusive communications. Its work is focused on the perpetrators of such conduct and consideration of the existing criminal sanctions, in particular the Malicious Communications Act 1988 and the Communications Act 2003. The offence in section 1 of the Malicious Communications Act is wide; it prohibits the sending of a communication which is indecent or grossly offensive, a threat, or false information with the purpose of causing distress and anxiety. Two issues however arise which limit its efficacy; firstly the threshold of indecency or offensiveness which, whilst wide, may not be wide enough and set the threshold too high and, secondly, and perhaps, more significantly, this offence does not appear to extend to representations made in public forums being limited to communications directed specifically to another. The offence in s127 of the Communications Act 2003 is one of sending a message which is known to be false for the purpose of causing inconvenience or needless anxiety to another. Again this is limited by the need to show that a message is false and also, as noted by the Law Commission, it does not extend to a communication sent over a private network such as Bluetooth.

So, not only are there issues requiring consideration as far as offences committed by individuals but there is to be no consideration of the position of those who facilitate such offences by the provision of the necessary internet services and platforms. However it can be readily appreciated that reliance on established principles which relate to aiding and abetting (given the need for the necessary mental element which will almost always involve direct knowledge) are unlikely to constitute part of an effective enforcement regime.

That then is the context of the new White Paper. It is specifically directed at companies who provide services or tools that allow, enable or facilitate users to share or discover user generated content or interact with each other online. Thus posts on a public forum or the sharing of a video would be caught as would instant messaging or comments on posts.

The central suggestion is that such companies would be subject to a new duty of care to take reasonable steps to keep users safe and tackle illegal and harmful activity on their services. It will also extend to take reasonable steps to prevent other persons coming to harm as a direct consequence of activity on their services. Thus victims of non-consensual images would be protected.

The breadth of the duty will be tempered by adoption of the principle of proportionality by the regulator. It states that this proportionate approach will also be enshrined in the legislation by making it clear that companies must do what is reasonably practicable. The White Paper makes it clear that the Government has not yet decided whether the regulator will be a new or existing body nor the way it will be funded. What is clear is that the thrust of the new regime will be one which is based on corporate governance rather than result based sanctions. The regulator will establish codes of practice which will outline the systems, procedures, technologies and investment, including staffing, training and support of human moderators, that companies need to adopt to help demonstrate that they have fulfilled the duty of care. It does not envisage that companies will be compelled to undertake general monitoring of all communications on their online services but rather an approach based on specific monitoring. Further what is expected is that companies have sufficient internal procedures so that individuals can raise complaints with the relevant company and have the opportunity for effective redress. However what seems to be missing at this stage is a recognition of the key role that anonymity plays in online harm. The ease with which an individual can set up an account with minimal unverified details allows users to conduct their activities with considerable assurance that they can do so with impunity. There is little in the White Paper which recognises this.

It is proposed that failure to comply with this duty is to be met with civil fines and consultation is being sought as to whether or not the regulator should have powers to force companies to withdraw services or, in the last resort, adopt blocking of non-compliant websites or apps. Further consultation is sought in relation to senior management liability for civil fines consequent upon breach.

What is almost completely absent from the White Paper is any detailed consideration of the role that the criminal law should play. There is a suggestion that liability of senior management could be extended to include criminal liability and that specific illegal harms would be expected to be referred to law enforcement and other relevant government agencies (not the regulator) to aid investigations. It refers to the existing provisions of the EU's e-commerce directive although these are limited because they require direct knowledge of unlawful activity on the part of the provider. It concludes that what is proposed in the White Paper will be in line with the existing law. However that is far as matters go. The position is that given the potential harm that can be caused, as tragically illustrated by the case of Molly Russell, and the potential scope of misuse of the internet, there is a clear case for the intervention of the criminal law. Specific offences will always be subject to particular limitations which will often mean they are inapplicable in a context where harm can be caused in a myriad of ways. A general duty of care as envisaged by the Government is surely the only effective means of giving enforcement agencies the flexibility they need to meet this challenge. There must be a strong case for extending the ambit beyond civil liability as proposed in the White Paper and backing the duty with criminal sanctions for failure to comply.

Such criminal liability could be framed in the language familiar with regulatory lawyers. The duty to 'ensure' individuals are not 'exposed to risk' is the basis of health and safety legislation and if a potential duty of ensuring individuals are not exposed to risk of online harm is viewed as being unduly wide then the lessor duty to 'protect' against risk of harms are familiar in the context of food safety. However given the seriousness of harm that can result there is surely a case for establishing a duty to 'ensure' rather than a less onerous alternative.

Such a duty, of course, needs to be qualified. Again the experience of regulatory lawyers familiar with defences of due diligence can be drawn on in this respect. But, again, the parallel with health and safety provides the most effective starting point qualifying a general duty to the extent that the duty holder is only required to do that which is reasonably practicable. This of course mirrors the formulation proposed by the Government in the white paper to ensure proportionality. The value of this approach is that it means that competing interests and values, in particular the right of freedom of expression, can be properly weighed in the balance, ultimately by a jury.

There appears to be little doubt about the seriousness and extent of the problem. The inadequacies of the present legal provisions are recognised explicitly by the Law Commission and implicitly in the proposals made in the White Paper. Of course, an approach based on civil fines for failures in respect of corporate governance is laudable and important. However there is clearly a debate to be had about whether in these circumstances the Government needs to go further and recognise the need for a review of the existing criminal law as it relates to service providers with a view to imposing a general duty of care upon such companies to ensure, so far as is reasonably practicable, that individuals are not exposed to a risk of online harm, breach of which is a criminal rather than a civil matter.

Gordon Menzies, Six Pump Court Chambers

http://www.6pumpcourt.co.uk/barrister/gordon-menzies/