The Communications Offences under the OSB (Part 10)

This briefing note, prepared by Prof. Lorna Woods and Dr. Alexandros Antoniou of the University of Essex, is designed to help those following the progress of the Online Safety Bill to understand the new communications offences and how the amendments will change the existing criminal law.

The Online Safety Bill (HL Bill 87) revises existing communications offences, in part following the recommendations of the Law Commission. The original proposal by the Commission to replace s. 127(1) of the Communications Act 2003 with a "harm-based" communications offence was dropped in November 2022, following some concerns about its potential to "produce unintended consequences on freedom of expression". We are now left with the offences of:

1) false communications (cl. 160);
2) threatening communications (cl. 162); and
3) sending or showing flashing images electronically, known as 'epilepsy trolling' (cl. 164)

The offences of sending images of genitals, known as "cyber-flashing" (cl. 167), encouraging serious self-harm, the promotion of small boat crossings, or any other offences the government has said it will bring forward, are not discussed here. Note that the criminalisation of false or misleading information is not limited to the offences under the Communications Act. There are specific offences in relation to fraud, for example, and a specific offence relating to bomb hoaxes (s. 51 of the Criminal Law Act 1977). The common law offence of criminal libel was abolished in 2010 (when s. 73 of the Coroners and Justice Act 2009 came into effect).

1. The offence of false communications (cl. 160)

Cl. 160 sets out the false communications offence which is intended to protect individuals from any communications where the sender intended to cause harm by sending something knowingly false.

The existing law

Currently, s. 127 of the Communications Act 2003 (CA 2003) covers a number of behaviours, including one related to false information. Specifically, under s. 127(2) of the 2003 Act, a person commits an offence if, for the purpose of causing "annoyance, inconvenience, or needless anxiety to another", sends or causes to be sent via (or persistently make use of) a public communications network a message which the defendant knows to be false. The maximum penalty for this offence is six months' imprisonment or a fine.

False information is also covered by s. 1(1)(a)(iii) of the Malicious Communications Act 1988 (MCA 1988), which provides that any person who sends to another person information which is false and known or believed to be false by the sender is guilty of an offence if their purpose (or one of their purposes) in sending it is that it should cause "distress or anxiety to the recipient or to any other person to whom he intends that it or its contents or nature should be communicated". The maximum penalty for this offence is two years' imprisonment or a fine.

The two offences cover very similar ground but there are differences between them. While s. 127 of the CA 2003 is concerned with the misuse of a public electronic communications network, the MCA 1988 covers offline communications (e.g., letters and any articles sent) too. For the purposes of s. 127, the offence does not depend on the message being addressed to or received by another person. Rather, it is complete when the message is sent. While the case law has focussed on the offence under s. 127(1) (i.e., sending "grossly offensive, indecent, obscene or menacing" communications), the principle established in jurisprudence can also apply to s 127(2). Namely, the latter offence covers the posting of a message, as well as re-posting or other sharing of a post or message. So, in *Chabloz v CPS* (2019), the posting of hyperlinks to YouTube videos were caught. The Law Commission suggests that the MCA 1988 is slightly narrower than the CA 2003 in this regard but there is still no requirement that anyone sees the content.

Under the CA 2003, the person sending the message must know that the content is not true. This protects people who pass on inaccurate information but sincerely believe it to be true. It would also seem to protect the communications of those who may suspect that what they say may not be entirely accurate, but do not know. However, the courts have not grappled with where the boundaries of knowledge and truth lie for these purposes. The MCA 1988, likewise, protects the misguided disseminator of inaccuracies but catches - seemingly by contrast to s 127(2) of the CA 2003 - the person who spreads accurate information knowing or believing it to be false.

The communication must be sent for the purposes of causing "annoyance, inconvenience or needless anxiety" (CA 2003) or "distress or anxiety" (MCA 1988), but there is little reported case law on what these terms might mean. The Law Commission gave the example of the case against Dure (Law Comm No. 381, para. 11.22), a self-styled "paedophile hunter" who made false claims online that another man was a "violent psychopath" who "grooms teenagers". Dure was convicted and sentenced to 15 weeks' imprisonment. The Law Commission questioned whether these phrases were potentially too broad. Conversely, it also noted that the offences would not catch some online behaviours which caused harm (Law Comm No. 399, paras. 1.5-1.6).

Of note, s. 127 of the 2003 Act extends to the whole of the UK and s. 1 of 1988 Act extends to England and Wales only. Where either of the two offences have a foreign dimension, they could constitute an offence in England and Wales if a "substantial measure" of the activities constituting the crime take place here. But as the Law Commission has noted there is some uncertainty in relation to the

application of this approach to online activities (Law Comm No. 381, paras. 4.135-4.139).

The new false communications offence

The offence under cl. 160 raises the current threshold of criminality and would be committed if:

a) a person sends a message conveying information that the person knows to be false; and
b) the person intended the message to cause "non-trivial psychological or physical harm" to a likely audience; and
c) the person had no reasonable excuse for sending the message

The new offence has many similarities to the existing position. Although phrased differently, the notion of "sending" a message (defined in cl. 163(2)) seems similar to the position under existing case law and central to the offence is the requirement of knowledge of falsity, i.e., the sender knows - rather than believes - the information to be false. In essence, cl. 160 covers false communications deliberately sent to inflict harm, rather than misinformation in circumstances where people genuinely believe it to be true or are unaware that what they are sending is false (protecting thus individuals who share contested ideas in good faith).

The purpose of causing "annoyance etc." under s. 127(2) of the 2003 Act, according to the Law Commission, set the bar "too low" (Law Comm CP No. 248, para. 6.45). This has now been changed. The new offence raises the current threshold of criminality. It requires that the sender intends the message or information in it to cause psychological or physical harm that is *more* than trivial.

Moreover, the harm must relate to a "likely audience" (cl. 160(2)), meaning that it is reasonably foreseeable that a person would encounter the message, or a reposting or forwarding of the message. This intention is judged at the time of sending the message. "Encounter" in relation to a message has the same broad meaning it does in the rest of the OSB: i.e., to "read, view, hear or otherwise experience" (cl. 163(5)).

The lack of reasonable excuse for sending the message (i.e., (c) in the list above) is not a defence, but rather an element of the offence, requiring the prosecution to prove, beyond reasonable doubt, that the communication at issue was sent without a good reason. This assessment must include consideration of whether the message was or was intended as a contribution to a matter of public interest (Explanatory Notes, para. 670).

Defined media bodies and cinematographers enjoy a carve out: in particular, recognised news publishers (as defined in cl 50 of the OSB), holders of a broadcast licence and on-demand programme service providers are exempt from the false communications offence (cl. 161(1)-(4)). The offence cannot be committed in

connection to the showing of a film made of public cinema release either (cl. 161(5)).

Finally, if someone is found guilty of the false communication offence, they could go to prison for up 51 weeks (cl. 160(6)(b)).

2. The offence of threatening communications (cl. 162)

The OSB also creates under cl. 162 a new offence of sending threatening communications.

The existing law

Some threatening behaviours are already covered by the criminal law, although there is little coherence in the approach overall. The "menacing" communication aspect of s. 127(1) of the CA 2003 and s. 1(1)(a)(ii) of the MCA 1988 currently specifically criminalise threats. The High Court held in *Chambers v DPP* (2012) that in order to have a menacing quality the message would need to be one which would "create fear or apprehension in those to whom it is communicated, or who may reasonably be expected to see it" (para. 30).

Other examples of offences including a requirement of threat are: threats to kill (contrary to s. 16 of the Offences Against the Person Act 1861), threats to commit criminal damage (contrary to s. 2 of the Criminal Damage Act 1971), threats to disclose private sexual images without consent (contrary to s. 33 of the Criminal Justice and Courts Act 2015, as amended by s. 69 of the Domestic Abuse Act 2021), various Public Order Act 1986 offences (ss. 4, 4A and 5), and some forms of "cyber-stalking" in the context of VAWG offences (e.g., involving threatening emails or text messages).

There are, however, some challenges in translating some of these offences to the online environment. There is a question about the extent to which the online environment equates to public spaces, but this may be a question of fact depending on how the service is configured and how easy it is to transmit information from or to other services, as well as the size of the audience even on the platform itself. Moreover, given there are no offences designed for the purpose, there are questions about the selection and use of existing offences and whether this could lead to inconsistencies and gaps, and perhaps also over-coverage, especially because the online environment gives rise to the possibilities of old behaviours with greater impact (doxing), new behaviours (dogpiling) and new languages of communication (emojis).

The new threatening communications offence

The new threatening communications offence has the same starting point as the false communications offence under cl. 160, i.e., a person "sending a message" (as defined in cl. 163(2)) that "conveys" (presumably the language here was chosen to be open to different ways of intimating a threat) a "threat of death or serious harm", *intending* that those who encounter the message will fear the threat will be carried out or is *reckless* as to whether that person would so think (this is in line with the fault element under the "menacing" communications offence in the CA 2003; the standard under the MCA 1988 is higher in this regard, requiring proof of the sender's "purpose"). The Law Commission observes that requiring that the defendant intend or be reckless as to whether the victim would fear that the defendant would carry out a threat ensures that only threats reflecting a level of seriousness will be within the scope of the offence (Law Comm No. 399, para. 3.97). "Serious harm" in the context of the threatening communications offence is specifically defined (cl. 162(2)) as:

a) serious injury amounting to grievous bodily harm (within the meaning of the OAPA 1861);
b) rape;
c) assault by penetration (s. 2 of the SOA 2003); or
d) serious financial loss.

It is noteworthy that although there is a statutory definition of rape (see s. 1 of the SOA 2003), this is not used in cl. 162(2)(b) and that financial loss is included in a list that otherwise deals with threats of personal violation and infliction of physical violence.

In addition to footballers, celebrities and public figures who become targets of messages threatening their safety, the new offence can help tackle coercive and controlling online behaviour especially in domestic violence contexts, including threats related to a partner's finances. For instance, an individual posting a public comment falsely suggesting his ex-partner was dishonest in their relationship and threatening to withdraw all remaining money from their shared account would likely be found guilty under the threatening communications offence by threatening to cause serious financial harm (provided the necessary fault element is met too).

It is worth noting that those fearing the threat will be carried out need not be the intended victims of the threatened conduct. The framing of the new offence would seemingly cover circumstances in which a person who encounters the message will fear the threat will be carried out against a third party with whom the recipient is in a close tie of affection, e.g., in familial relationship or close friendship. So, an individual who posts a video on Facebook in which they suggest that they are going to set fire to their local NHS hospital and all inside it "to cleanse his town of diseased people" would likely be found guilty under cl. 162 offence. Their statement conveys a threat of at least serious physical harm to those in the hospital and also causing serious financial loss to the relevant NHS trust. Those fearing the

threat will be carried out could include NHS staff at the hospital or family members.

It seems that cl. 162 is mostly concerned with physical impacts, as threats of digital only forms of violation are not included. Although, as mentioned earlier, threats to disclose private sexual images without consent are already criminalised, threats relating to other forms of digital humiliation, like threats to publish sexual information or threats to upload manufactured intimate images ("DeepFakes") to get a victim to obey commands, would not seem to be covered (though note that the government announced in November 2022 it intended to bring forward legislation to tackle such emerging forms of image-based sexual abuse).

Of note, threats of serious financial loss could be acceptable (and so it is a defence for a person to show they issued the threat) to "reinforce a reasonable demand" when the person reasonably believed this was a "proper means" to reinforce the demand (cl. 162(3)). This provision mirrors the defence under s. 1(2) of the MCA 1988. In the example given above, the former partner would lack a defence as the threat to cause serious financial loss was not used to reinforce a reasonable demand, and neither did they believe that the use of the threat was a proper means of reinforcing the demand.

Finally, if someone is found guilty of the threatening communications offence, they could go to prison for up five years (cl. 162(5)(b).

3. The offence of sending or showing flashing images electronically (cl. 164)

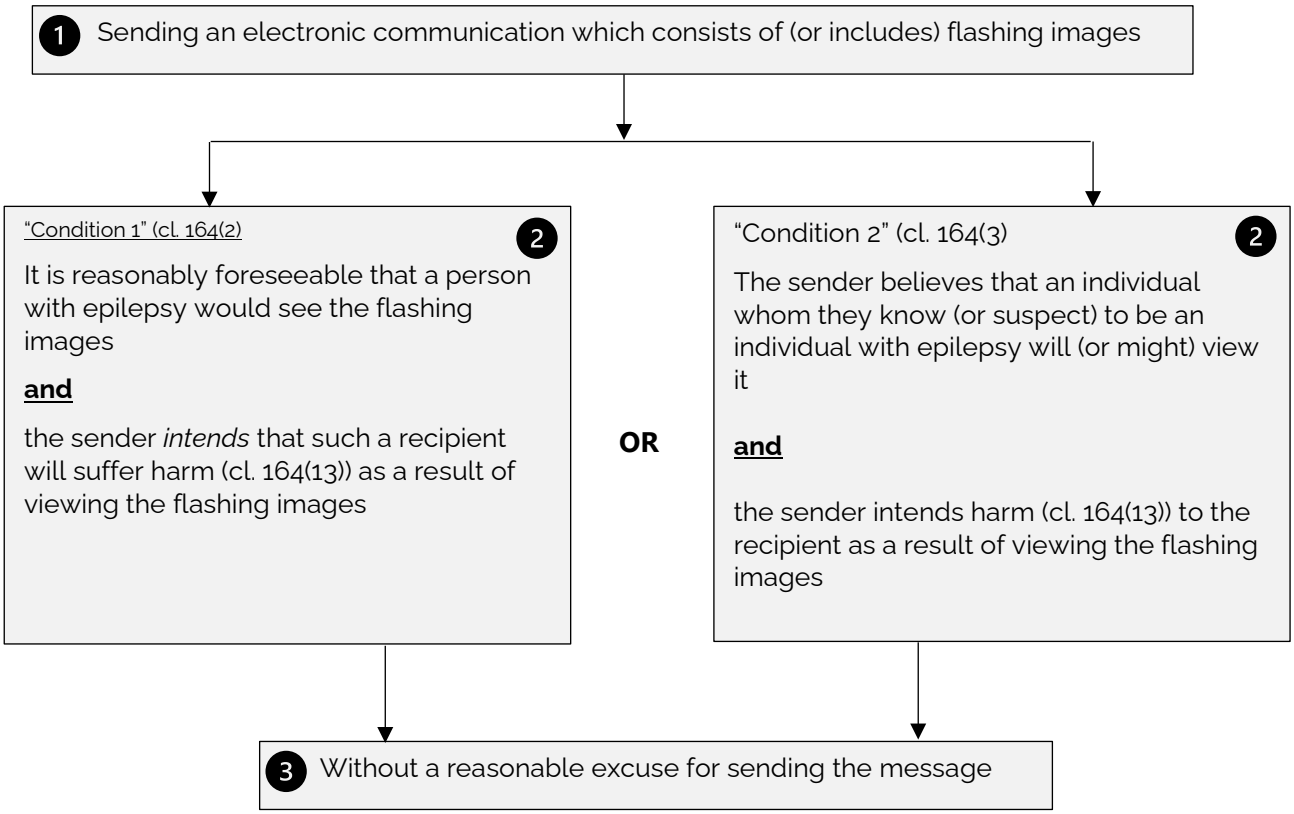
This is the so-called "Zach's law" and is intended to address the phenomenon of sending flashing images to people with epilepsy with the intention of triggering seizures. The Law Commission noted that it was distinct in the online and communications offences because it directly caused physical harm. There was no specific offence in statute dealing with this issue and relying on the Offences Against the Person Act 1861 was not a good fit for the behaviour.

The Law Commission recommended that the potential seriousness of the offending conduct warranted a separate response other than a general communications offence but did not make any recommendations as to the precise form of such an offence. The commitment to introduce the "epilepsy trolling" offence was made in July 2022 by the then DCMS Secretary Nadine Dorries (HCWS193, vol. 717, col. 69WS) and was later incorporated as cl. 164 when the OSB came to the House of Lords.

Cl. 164 creates two offences, i.e., an offence of sending (see 3a below) and an offence of showing (see 3b) electronically flashing images to people with epilepsy with the intention to cause them "harm", meaning a seizure or alarm or distress (cl. 164(13)).

3a. The cl. 164(1) offence of "sending"

Cl. 164(1) creates an offence of sending by electronic means a communication with flashing images where one of two conditions are met and without reasonable excuse. So, the "sending" offence can be committed in two ways:



Condition 1 envisages capturing speculative messages sent to multiple people (e.g., on social media), whereas **condition 2** envisages capturing the more targeted sending of flashing images to an individual who the sender knows (or suspects) has epilepsy (Explanatory Notes, paras. 687 and 688).

3b. The cl. 164(8) offence of "showing"

The second offence targets showing another person flashing images by means of an electronic communications device. This is committed if a person, with no reasonable excuse, shows an individual flashing images (e.g., on a device's screen), while knowing (or suspecting) that the individual concerned is an individual with epilepsy, and *intends* harm to come to that person as a result.

Notably, both offences (3a and 3b) require proof that the defendant sent a communication intending to cause harm. This may appear inconsistent with the threatening communications offence under cl. 162 (the fault element of which captures both intention and recklessness), especially because both cls. 162 and 164 address particularly harmful subsets of communications. There is also a question as to whether cl. 164 addresses an adequate range of culpable behaviour.

The current drafting suggests that the fault element is directed exclusively to the offender's state of mind and if they may have intended the harmful message as entertainment/ amusement ("for a laugh") or some high jinks or because of misjudged humour, it is unlikely that the mental element required before conviction for the offence will be established.

The cl. 164 offences carry a potential prison sentence of up to five years. Cl. 164(9) creates a carve out for healthcare professionals acting in that capacity. Of note, cl. 164 extends to England and Wales and Northern Ireland only. "Epilepsy trolling" is already a criminal offence in Scotland (Baroness Fraser of Craigmaddie, HL Deb, 16 May 2023, vol. 830, col 166).