Publicising Terrorism in Private:
Criminal Law, Online Safety and the Meaning of 'Public Communications'

Professor Stuart Macdonald (Swansea University)
s.macdonald@swansea.ac.uk

Jonathan Hall KC (Independent Reviewer of Terrorism Legislation)
Jonathan.Hall@6kbw.com

Abstract

The Online Safety Act creates the power to impose a Terrorism Content Notice on providers of user-to-user services, requiring them to identify and swiftly remove terrorism content that has been communicated publicly, not privately. A distinction between public and private communications has also been drawn in the practical application of the encouragement of terrorism offence, to which Terrorism Content Notices are inextricably linked via the definition of terrorism content. This article argues that this dichotomous public/private approach is flawed. Through an examination of how Islamic State disseminates its propaganda online, the article demonstrates empirically that such content may be communicated publicly in (what some might regard as) private settings. It discusses various factors that might be considered when answering what should be the key question – whether the content was communicated publicly or not – including the number of users that are able to access the statement and any restrictions on access.

Publicising Terrorism in Private:
Criminal Law, Online Safety and the Meaning of 'Public Communications'

A. Introduction

Domestic law strikes an uneasy balance between penalising harmful speech and intruding excessively into private discourse. The prohibition on public encouragement of terrorism derives from legislation enacted after the London Transport bombings in 2005. Almost two decades later, the UK's Online Safety Act 2023 targets terrorism content and other harmful speech in the online domain, whose complex ecosystem requires fresh attention to the distinction between the 'public' and the 'private'.

Many years in the making, the Online Safety Act received Royal Assent in October 2023.[1] Expected to apply to more than 25,000 companies, including the likes of Facebook, Twitter and Google,[2] the Act seeks to tackle a wide range of online harms – from terrorism, human trafficking and child sexual exploitation and abuse to fraud, foreign interference and drugs and firearms offences – by imposing numerous duties on service providers and vesting enforcement powers in Ofcom, the new online safety regulator.

The duties placed on service providers include to mitigate and manage the risk of harm to individuals, with specific duties to safeguard children and conduct risk assessments of services likely to be accessed by them.[3] For its part, OFCOM has the power to require the use of proactive and accredited technology in case of identified failures, including by issuing a Terrorism Content Notice. With the sole exception of using accredited technology to detect child sexual exploitation and abuse content, Ofcom's power to stipulate the use of proactive

---

Unless otherwise stated, all URLs were last accessed 14 September 2023.

[1] The initial *Online Harms White Paper* was published in April 2019: HM Government, *Online Harms White Paper* CP 57 (2019).

[2] Department for Digital, Culture, Media and Sport, 'Impact Assessment: The Online Safety Bill' 31 January 2022 at https://publications.parliament.uk/pa/bills/cbill/58-02/0285/onlineimpact.pdf. Though note that providers of email, short messaging service (SMS), multimedia messaging service (MMS) and live one-to-one aural communications are outside the regulatory framework (Online Safety Act 2023, Sched 1).

[3] Online Safety Act 2023, ss 9-13, 26-30.

or accredited technology applies to public, and not to private, communications.[4] Other national and transnational regulatory regimes employ a similar restriction, as do the terms of service of some tech companies.[5]

Underlying this distinction between the public and the private is the concern to ensure the efficacy of the enforcement powers while simultaneously respecting individuals' human rights.[6] On the one hand, a broad understanding of what constitutes a public communication would ensure that the vast majority of illegal and harmful content is encompassed but risks resulting countermeasures intruding inappropriately into essentially private interactions online. On the other hand, a broad understanding of what constitutes a private communication would safeguard the privacy of individuals but risks allowing malevolent actors to exploit these ostensibly private online spaces.

Yet distinguishing between public and private communications can be difficult. For a start, the terms public and private are themselves not straightforward. There are contrasting theories of privacy, spanning the deontological (the 'right to be let alone'[7]), the instrumental (focusing on control over private information[8]), limitations on access (comprising secrecy, anonymity and solitude[9]) and the pluralistic (which is also capable of encompassing intrusion[10]). This can result in dissensus in individual cases.[11] Abstracting a general definition of public is similarly difficult. The Law Commission has commented:

> Assessing whether a person's use of new media constitutes a communication to the public or a section of it will vary significantly both between the various media available and

[4] *ibid*, ss 121(2)(a), 232(1).

[5] For example, Germany's Network Enforcement Act applies to platforms that make content available to the public (s 1), while the EU's Terrorist Content Online Regulation is targeted at the dissemination of terrorist content to the public (Article 1(1)).

[6] S. Macdonald, 'Why we should abandon the balance metaphor: a new approach to counterterrorism policy' (2009) 15 *ILSA Journal of International and Comparative Law* 95.

[7] S. Warren and L. Brandeis, 'The Right to Privacy' (1890) 4 Harvard LR 193, 195.

[8] A. F. Westin, Privacy and Freedom (New York: Atheneum, 1967).

[9] R. Gavison, 'Privacy and the Limits of Law' (1980) 89 Yale LJ 421.

[10] D. J. Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2009).

[11] T. Bennett, 'Triangulating intrusion in privacy law' (2019) 39 OJLS 751.

> depending on how the particular service is used … In such cases, it appears that whether a communication was to the public or a section of it would need to be decided on a case-by-case basis.[12]

These definitional challenges are compounded by the fact that the public and private spheres overlap. It is widely accepted that privacy is not an all or nothing concept and that 'a degree of privacy may be retained in a semi-public environment'.[13] As the European Court of Human Rights has stated, there is 'a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"'.[14] This article explains that the converse is also true: it is possible to publicise in (what might be regarded by some as) private spaces. From this starting point, the article argues that the distinction drawn by the Online Safety Act between public communications and private communications is an infeasible dichotomy. The key question should be whether content was communicated publicly or not.

To substantiate this argument, the article uses as a case study the process by which Islamic State (IS) disseminates its propaganda online with specific reference to a particular platform (Telegram). After describing this process in Part B, the article turns in Part C to the encouragement of terrorism offence in the Terrorism Act 2006. This offence is inextricably linked to the Online Safety Act via the latter's definition of 'terrorism content'.[15] The first

[12] Law Commission, *Contempt of Court (1): Juror Misconduct and Internet Publications* (Report No 340) HC 860 (2013), 15.

[13] H. Fenwick and G. Phillipson, 'The Doctrine of Confidence as a Privacy Remedy in the Human Rights Act Era' (2000) 63 MLR 660, 675. See also: J. R. Reidenberg, 'Privacy in Public' (2014) 69 *University of Miami Law Review* 141; L. Edwards and L. Urquhart, 'Privacy in public spaces: what expectations of privacy do we have in social media intelligence?' (2016) 24 *International Journal of Law and Information Technology* 279; K. Bajpai and K. Weber, 'Privacy in Public: Translating the Category of Privacy to the Digital Age' (2017) 51 *Research in the Sociology of Organizations* 223; B. Zhao, 'Exposure and Concealment in Digitalized Public Spaces. in T. Timan, B. C. Newell and B. J. Koops (eds) *Privacy in Public Space: Conceptual and Regulatory Challenges* (Cheltenham: Edward Elgar, 2018). An example of the contrasting, all-or-nothing approach is the public observation doctrine in the US.

[14] *PG v UK* (App No 44787/98) (2008) 46 EHRR 51, [56].

[15] This definition states that terrorism content is content that amounts to an offence specified in Schedule 5 (Online Safety Act 2023, s 59(8)). This involves consideration of all elements of the offence, including mental

requirement for the encouragement of terrorism offence is that the defendant published a statement. This requirement may raise questions of accessibility that are also relevant to the distinction between public and private communications drawn by the Online Safety Act – meaning that Ofcom may sometimes have to consider restrictions on accessibility both when deciding whether there is terrorism content present on a service, and when determining whether this content was communicated publicly. It will be argued that the fact that content is deliberately difficult to access should not be taken to mean that it has not been published, nor that the online spaces in which it is published are private. Such obstacles are designed to safeguard the initial stages of a process we call chain accessibility, and so in practice operate to maximise public dissemination at the later stages of the process.

In part D, attention turns to the Online Safety Act, the power it vests in Ofcom to require the use of accredited technology by issuing a Terrorism Content Notice and the Act's approach to distinguishing between public communications (to which Terrorism Content Notices apply) and private communications (to which they do not). It analyses the three factors that the Act states Ofcom must, in particular, consider when determining whether content is communicated publicly or privately and argues that our proposed approach – to focus on whether or not content was communicated publicly – is consistent with the factors identified in the Act (as well as with what is not). The article then concludes by considering the implications of our argument for privacy-related concerns about the scope of online safety legislation, in particular the impact on encrypted services.

B. IS's propaganda dissemination process

Terrorist groups and their supporters use the internet for a variety of purposes: from recruitment, community-building and attack-planning to training, fund-raising and psychological warfare.[16] Of particular concern to policymakers has been the use of online

elements and any possible substantive defences (s 192(6)). One of the 22 substantive offence listed in Schedule 5 is the encouragement of terrorism offence.

[16] S. Macdonald and D. Mair, 'Terrorism Online: A New Strategic Environment' in L. Jarvis, S. Macdonald and T. M. Chen (eds), *Terrorism Online: Politics, Law and Technology* (Abingdon: Routledge, 2015).

platforms, including the largest social media sites, to disseminate propaganda.[17] Since the time, less than a decade ago, when Islamic State (IS) was able to maintain a stable presence on Twitter,[18] the largest tech companies have made significant progress in identifying and removing terrorist content.[19] Today, user and law enforcement referrals account for only a small proportion of content takedowns, with Facebook, YouTube and Twitter each reporting proactive detection rates of more than 90%.[20] Such efforts rely heavily on the use of automated tools, including: image matching (checking whether a photo or video that is being uploaded to the platform matches a photo or video that has previously been removed for promoting terrorism); language understanding (analysing text that has been removed for promoting terrorism in order to train algorithms to detect similar posts in the future); and, identifying recidivists (detecting new, fake accounts created by repeat offenders).[21] Collaborative initiatives have also been developed, most notably the hash-sharing database created by the Global Internet Forum to Counter Terrorism (GIFCT) and Tech Against Terrorism, which provides support for small platforms whose services have been exploited by terrorist groups.[22]

---

[17] For example, it was described by the Home Affairs Committee as 'one of the greatest threats that countries including the UK face' (*Radicalisation: the counter narrative and identifying the tipping point* (Eighth Report of 2016-17), HC 135 (2016), 11).

[18] One study found that in late 2014 there were between 46,000 and 90,000 overt IS supporter accounts on Twitter, posting an average of 7.3 tweets per day (J.M. Berger and J. Morgan, *The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter* (Washington, DC: Brookings Institution, 2015)).

[19] In 2021, Facebook removed more than 34 million items of terrorist propaganda ('Community Standards Enforcement Report – Dangerous Organizations: Terrorism and Organized Hate' at https://transparency.fb.com/data/community-standards-enforcement/dangerous-organizations/facebook/#content-actioned), YouTube removed 513,908 videos for the promotion of violence and violent extremism ('YouTube Community Guidelines Enforcement' at https://transparencyreport.google.com/youtube-policy/removals), and Twitter suspended 78,668 accounts for the promotion of terrorism ('Rules Enforcement' at https://transparency.twitter.com/en/reports/rules-enforcement.html).

[20] *ibid*.

[21] M. Bickert and B. Fishman, 'Hard Questions: How We Counter Terrorism' at https://about.fb.com/news/2017/06/how-we-counter-terrorism/.

[22] See https://gifct.org/hsdb/ and https://www.techagainstterrorism.org/.

One effect of increased enforcement activity on the biggest platforms has been to displace propaganda dissemination activities to other parts of the online ecosystem.[23] After IS enjoyed its so-called 'Golden Age' on Twitter in 2013 and 2014,[24] its community-building activities were driven to other platforms, particularly Telegram.[25] Telegram has been found to be used for a variety of purposes by pro-IS users, including instruction, interaction and communication, but by far the most common purpose for which it is used is the distribution of core IS media and other pro-IS materials.[26] Other jihadist and far-right groups have used Telegram in a similar way.[27] It can be anticipated that other platforms, offering similar or better affordances, will come become prominent over time.

Telegram is a cross-platform messaging app on which users can share an unlimited number of photos, videos and files, of up to 2 gigabytes each.[28] It has over 500 million active users[29] and is popular for its enhanced privacy and encryption.[30] Its features include: secret chats, with end-to-end encryption; a self-destruct timer that permanently deletes secret messages after a set period of time; groups, which are multi-person chats and can have up to 200,000

[23] S. Macdonald, S. Correia and A. Watkin, 'Regulating Terrorist Content on Social Media: Automation and the Rule of Law' (2019) 15 *International Journal of Law in Context* 183.

[24] M. Conway, M. Khawaja, S. Lakhani, J. Reffin, A. Robertson and D. Weir, 'Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts' (2019) 42 *Studies in Conflict & Terrorism* 141, 150.

[25] N. Prucha, 'IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram' (2016) 10(6) *Perspectives on Terrorism* 48; A. Alexander, *Digital Decay? Tracing Change Over Time Among English-Language Islamic State Sympathizers on Twitter* (Washington, DC: George Washington University Program on Extremism, 2017) at https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/DigitalDecayFinal_0.pdf.

[26] B. Clifford and H. Powell, *Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram* (Washington DC: George Washington University Program on Extremism, 2019) at https://scholarspace.library.gwu.edu/work/9s161692z.

[27] M. Conway, M. Khawaja, S. Lakhani and J. Reffin, 'A Snapshot of the Syrian Jihadi Online Ecology: Differential Disruption, Community Strength, and Preferred Other Platforms' (2020) *Studies in Conflict and Terrorism* at https://doi.org/10.1080/1057610X.2020.1866736; S. J. Baele, L. Brace and T. G. Coan, 'Uncovering the Far-Right Online Ecosystem: An Analytical Framework and Research Agenda' (2020) *Studies in Conflict & Terrorism* at https://doi.org/10.1080/1057610X.2020.1862895.

[28] 'Telegram FAQ' at https://telegram.org/faq.

[29] *ibid*.

[30] D. Johnson, 'What is Telegram? A quick guide to the fast and secure messaging platform' *Business Insider*, 24 March 2021 at https://www.businessinsider.com/what-is-telegram?r=US&IR=T.

members; and, of particular relevance, channels, which are a tool for broadcasting messages to large audiences and can have an unlimited number of subscribers.[31] Channels can be public or private. Public channels have a username, so anyone can find them in Telegram's search function and join, whereas to join a private channel a user must be added by the owner or receive an invite link (known as a joinlink).[32]

Given the disruption that pro-IS users now face on the biggest online platforms, a variety of different platforms are used in the propaganda dissemination process, in order to achieve the widest possible reach while ensuring resiliency.[33] When a new item of official IS propaganda is produced, it is posted in private channels on Telegram.[34] It is then acquired by pro-IS users, following which the dissemination process 'becomes rapidly decentralized'.[35] These users store each piece of propaganda on multiple file-sharing sites – often hosted by small or micro companies that lack the capacity to regulate their platform effectively – generating multiple URLs for each item on each site.[36] These banks of URLs are then made openly available on public Telegram channels and, increasingly, decentralised messaging services and chat apps as well.[37] From here, IS sympathisers can gather the URLs and post them on 'beacon'

[31] Channels FAQ' at https://telegram.org/faq_channels.

[32] *ibid*.

[33] S. Macdonald, C. Rees and J. S, *Remove, Impede, Disrupt, Redirect: Understanding & Combating Pro-Islamic State Use of File-Sharing Platforms* (Washington DC: RESOLVE Network, 2022) at https://doi.org/10.37805/ogrr2022.1; A. Fisher, N. Prucha, and E. Winterbotham, *Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability* (London: Royal United Services Institute, 2019) at https://static.rusi.org/20190716_grntt_paper_06.pdf.

[34] A. Almohammad and C. Winter, *From Battlefront to Cyberspace: Demystifying the Islamic State's Propaganda Machine* (West Point, NY: Combating Terrorism Center, 2019) at https://ctc.usma.edu/wp-content/uploads/2019/05/Battlefront-to-Cyberspace.pdf ; L. Bindner and R. Gluck, 'Assessing Europol's Operation Against ISIS' Propaganda: Approach and Impact' 18 June 2018 at https://icct.nl/publication/assessing-europols-operation-against-isis-propaganda-approach-and-impact/.

[35] D. Milton, *Pulling Back the Curtain: An Inside Look at the Islamic State's Media Organization* (West Point, NY: Combating Terrorism Center, 2018), 10 at https://ctc.usma.edu/wp-content/uploads/2018/08/Pulling-Back-the-Curtain.pdf.

[36] A. Shehabat and T. Mitew, 'Black-boxing the black flag: anonymous sharing platforms and ISIS content distribution tactics' (2018) 12(1) *Perspectives on Terrorism* 81.

[37] S. Macdonald, C. Rees and J. S, n 33 above; S. Macdonald and S. McCafferty, *Online Jihadist Propaganda Dissemination Strategies* (VOX-Pol, 2024) at https://voxpol.eu/wp-content/uploads/2024/03/DCU-PN0752-Online-Jihadist-WEB-240305.pdf (accessed 13 April 2024).

platforms, such as Twitter, to signpost as wide an audience as possible to the propaganda.[38] Tactics such as hashtag hijacking and use of the @reply and @mention functions are employed to try and maximise exposure.[39]

In terms of content moderation, Telegram draws a sharp distinction between public and private channels. Its Terms of Service state that, by signing up to Telegram, users agree not to 'Promote violence on *publicly* viewable Telegram channels, bots, etc'.[40] Telegram has in the past taken part in Referral Action Days organised by Europol's EU Internet Referral Unit[41] and, in the first four months of 2022, it claimed to have removed 90,349 terrorist bots and channels.[42] Whilst some have nonetheless doubted Telegram's commitment to moderating publicly available content,[43] its stated approach to public channels stands in marked contrast to its refusal to moderate the contents of private channels, undertaking to 'ensure that no single government or block of like-minded countries can intrude on people's privacy and freedom of expression'.[44] At the same time, Telegram recognises that some users may seek to exploit its public/private dichotomy, stating that 'private channels with publicly available invite links will be treated in the same way as public channels, should it come to content disputes'.[45]

The question that this raises – and which goes unanswered in Telegram's Terms of Service – is when will a joinlink be regarded as publicly available? As noted above, new pieces of official IS propaganda are released in private Telegram channels. While these channels are

[38] A. Fisher, N. Prucha, and E. Winterbotham, n 33 above.

[39] M. Al Darwish, 'From Telegram to Twitter: The Lifecycle of Daesh Propaganda Material', VOX-Pol Blog, 11 September 2019 at https://www.voxpol.eu/from-telegram-to-twitter-the-lifecycle-of-daesh-propaganda-material/; S. Macdonald, C. Rees and J. S, n 33 above.

[40] 'Terms of Service' at https://telegram.org/tos (emphasis added).

[41] 'Europol and Telegram take on terrorist propaganda online', Europol at https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online.

[42] 'ISIS Watch' at https://t.me/s/ISISwatch.

[43] H. Gais and M. Squire, 'How an Encrypted Messaging Platform is Changing Extremist Movements', Southern Poverty Law Center, 16 February 2021, https://www.splcenter.org/news/2021/02/16/how-encrypted-messaging-platform-changing-extremist-movements.

[44] 'Telegram FAQ' at https://telegram.org/faq.

[45] 'Channels FAQ' at https://telegram.org/faq_channels.

highly secretive, by scouring the contents of public IS channels it is possible for those with the necessary expertise and patience to locate openly available joinlinks to these private channels. Indeed, it is through this painstaking process that some researchers and investigators manage to gain access to these private channels to monitor the release of IS propaganda. So while, on the one hand, these private channels possess privacy-enabling technical features, on the other hand joinlinks are made openly available (albeit secretively, so that locating them is a laborious task) and, importantly, these channels are being used as part of the propaganda dissemination process, which is in essence a public-facing form of communication.

C. Encouragement of terrorism: the publication of a statement

This part examines the encouragement of terrorism offence created by section 1 of the Terrorism Act 2006. There are of course significant differences between prosecution for a criminal offence and the imposition by Ofcom of a Terrorism Content Notice. The former involves the censure of an individual for a statement that has been published. By contrast, the latter poses a far wider potential risk to individuals' privacy, since it involves the proactive inspection of the content posted by all users of a particular service. Nonetheless, the two are connected by the Online Safety Act's definition of terrorism content and they share some important similarities, not least the fact that in practice a distinction is drawn between public and private communications when deciding whether to prosecute for the encouragement of terrorism offence.

Punishable by up to 15 years' imprisonment,[46] the *actus reus* of the section 1 offence requires, first, that the defendant published a statement or caused another to publish a statement.[47] A 'statement' is defined as a 'communication of any description', and includes communications 'without words consisting of sounds or images or both'.[48] This recognises the important role that images play in terrorist propaganda.[49] 'Publishing' is defined as encompassing publication 'in any manner', and expressly includes providing an electronic

[46] Terrorism Act 2006, s 1(7).

[47] *ibid*, s 1(2)(a).

[48] *ibid*, s 20(6).

[49] N. Lorenzo-Dus and S. Macdonald, 'Visual Jihad: Constructing the "Good Muslim" in Online Jihadist Magazines' (2021) 44 *Studies in Conflict & Terrorism* 363.

service ‘by means of which the public have access to the statement’ and ‘using such a service … to enable or to facilitate access by the public to [it]’.[50] The legislation’s accompanying explanatory notes explain that Internet Service Providers and website administrators may therefore be regarded as publishing statements on their platforms/websites.[51] As with other publication offences, it is not necessary that the statement is in fact seen by any member of the public.[52]

A superficial reading of section 1 – specifically the expression ‘to some or all of the members of the public to whom it is published’ – might suggest that the statement in question must additionally have been published *to the public*.[53] In fact, the existence of such a requirement is doubtful. The expression ‘to some or all of the members of the public to whom it is published’ is used in the context of the impact of the statement, as the next paragraph explains. At the same time, it is implicit that there is some element of *the public* in the act of publication. This is clear in the online context because of the extended definition of publishing by means of an electronic service. In such cases, the legislation stipulates that the public must have access to the statement. A separate requirement of publication to the public would not, therefore, add anything, if the statement has in fact been published. Indeed, this was the Government’s view at the time of enactment.[54]

The second *actus reus* requirement of the offence is that the statement was ‘likely to be understood by a reasonable person as a direct or indirect encouragement or other inducement, to some or all of the members of the public to whom it is published, to the commission, preparation or instigation of acts of terrorism or Convention offences’.[55] Although the term

[50] Terrorism Act 2006, s 20(4).

[51] At paragraph 95.

[52] As in *R v Sheppard* (n 74 below). The Law Commission considered that this approach also applied to contempt of court: see Law Commission, ‘Contempt of Court (1): Juror Misconduct and Internet Publications’, HC 860 (2013) at 2.30 to 245.

[53] According to section 20(3), the ‘public’ is defined as the public (or any section thereof) of any part of the UK or of another country, and expressly includes public meetings or gatherings (regardless of whether payment is required to attend).

[54] Baroness Scotland, HL Deb vol 676 col 435 5 Dec 2005.

[55] Terrorism Act 2006, s 1(1). The term ‘acts of terrorism’ ‘includes anything constituting an action taken for the purposes of terrorism’, with ‘purposes of terrorism’ in turn defined as including ‘action taken for the benefit of a proscribed organisation’ (Terrorism Act 2000, s 1(5)). ‘Convention offence’ means ‘an offence listed in

indirect encouragement is not defined, section 1(3) does offer an illustrative example: a statement that glorifies the commission or preparation of terrorist acts or offences and is one from which 'members of the public could reasonably be expected to infer that what is being glorified is being glorified as conduct that should be emulated by them in existing circumstances'.[56] When assessing how a statement is likely to be understood, its contents and the circumstances and manner of its publication must be taken into account.[57] It is irrelevant whether the statement encouraged one or more acts of terrorism specifically or acts of terrorism in general,[58] and whether anyone was in fact encouraged by the statement to engage in terrorism-related activity.[59]

The *mens rea* of the offence is either an intention to encourage (directly or indirectly) members of the public to commit, prepare or instigate acts of terrorism, or (subjective) recklessness as to whether the statement will have this effect.[60] The offence may therefore be established absent proof of a terrorist purpose,[61] though it should be noted that in cases of alleged reckless encouragement there is a defence of non-endorsement.[62] This defence applies where: (a) the statement neither expressed the defendant's views nor had his endorsement; and, (b) in the circumstances it was clear that the statement neither expressed his views nor had his endorsement.[63]

The section 1 offence needs to be distinguished, on the grounds of its scope and impact on individual rights, from the offence of disseminating terrorist publications under section 2 of

---

Schedule 1 or an equivalent offence under the law of a country or territory outside the United Kingdom' (Terrorism Act 2006, s 20(2)). The offences listed in Schedule 1 include offences involving explosives, hostage-taking, hijacking of aircraft and ships, and biological, chemical and nuclear weapons.

[56] Terrorism Act 2006, s 1(3).

[57] *ibid*, s 1(4).

[58] *ibid*, s 1(5)(a).

[59] *ibid*, s 1(5)(b).

[60] *ibid*, s 1(2)(b).

[61] *R v Brown* [2011] EWCA Crim 2751. In this case the defendant was guilty of the offence contained in section 2 of the Terrorism Act 2006 (dissemination of terrorist publications). He sold various terrorist materials via his website, earning over $100,000. It made no difference that his motivation was financial gain, not ideology.

[62] Terrorism Act 2006, s 1(6).

[63] *ibid*. It should also be noted that, in the case of an electronically published statement, the non-endorsement defence is unavailable if, in the opinion of a police constable, the statement is unlawfully terrorism-related and the defendant fails to comply with a take-down notice from the constable within two days (*ibid*, s 3).

the Terrorism Act 2006. The latter offence can be committed through private dissemination but it only concerns 'terrorist publications', defined as an article or record containing matter which is likely to be understood as an encouragement to terrorism or which is useful to terrorists.[64] Although the boundaries between words amounting to encouragement under the section 1 offence and words amounting to a publication within section 2 may not be watertight, in general section 2 is used to prosecute pre-existing documents, such as IS's *Dabiq* magazine. By contrast, section 1 is used to prosecute the words generated by the speaker or user himself. It therefore reaches further into the world of discussion and spontaneous expression.

Understandably, then, the section 1 offence has received significant academic attention. This has concentrated largely on the notion of indirect encouragement, the expressions 'likely to be understood' and 'some or all of the members of the public to whom it is published', and the deployment of a recklessness *mens rea* standard. This academic critique has expressed concern that the offence is unjustifiably broad and vague, potentially chilling individuals' exercise of their right to freedom of expression, especially those from ethnic minorities.[65] The focus of this article is instead the requirement that the statement was 'published', including through being made accessible to 'the public'. Closer examination of this requirement yields important insights for efforts to distinguish between public and private communications in the context of the Online Safety Act.

During the Parliamentary passage of the 2006 Act, a probing amendment was tabled by Liberal Democrat peer Lord Goodhart to clarify the meaning of the term 'members of the public'. On behalf of the Government, Baroness Scotland reiterated that – like Article 5 of the Council of Europe Convention on the Prevention of Terrorism (CECPT), which requires member states to criminalise 'public provocation to commit a terrorist offence' – the

[64] *ibid*, s 2(3).

[65] T. Choudhury, 'The Terrorism Act 2006: Discouraging Terrorism' in I. Hare and J. Weinstein (eds), Extreme Speech and Democracy (Oxford: Oxford University Press, 2009); A. Hunt, 'Criminal Prohibitions on Direct and Indirect Encouragement of Terrorism' [2007] Crim LR 441; S. Macdonald and N. Lorenzo-Dus, 'Intentional and Performative Persuasion: The Linguistic Basis for Criminalizing the (Direct and Indirect) Encouragement of Terrorism' (2020) 31 *Criminal Law Forum* 473; S. A. Marchand, 'An Ambiguous Response to a Real Threat: Criminalizing the Glorification of Terrorism in Britain' (2010) 42 *George Washington International Law Review* 123.

encouragement of terrorism offence 'is concerned with making messages available to the public'.[66] She continued by adding that

> It is not appropriate for this offence to target private communications … [W]e see no reason why the clause should not make it explicit that we are describing public communications by referring to members of the public as well … [T]he offence is not directed at private conversations …'.

The distinction drawn in this passage is between public communications, or messages that are available to the public, on the one hand, and private communications or conversations, on the other.

At first, this distinction appears to be a useful touchstone. However, Baroness Scotland's formulation is problematic. First, it adds a gloss to the legislation that is not found in the statutory text. The word 'private' does not appear in the definition of the offence in section 1, nor the accompanying definitions in section 20. The distinction that is drawn by the statute is between statements that were published (in the sense described above) and statements that were not.[67]

Second, whilst Baroness Scotland was presumably intending to paraphrase the statutory language, the distinction that she drew is not synonymous with the one contained in the 2006 Act. Specifically, her distinction rests on the assumption that private statements are not to be regarded as having been published for the purposes of the encouragement of terrorism offence. As the description of IS's propaganda dissemination strategy illustrated, this assumption has proven to be unjustified. As explained further below, when new items of official IS propaganda are posted in private Telegram channels, these posts constitute statements that are published to a section of the public (pro-IS users). Yet, they might also be regarded as private communications. The channels in which the content is posted are secretive and normally anonymous, so as to limit access to the user posting the content. For some, qualities such as secrecy, anonymity and limited access are the hallmark of privacy.[68] Admittedly, some would challenge this conceptualisation of privacy, pointing instead to such

[66] HL Deb vol 676 col 435 5 December 2005.

[67] Terrorism Act 2006, s 20(4).

[68] R. Gavison, n 9 above.

things as the principle of inviolate personality[69] or control over information.[70] The point is that Baroness Scotland's paraphrasing of the statutory test raises these difficult conceptual questions about privacy, when in fact the sole question should be whether the statement was published or not. Key to answering this question in the online context is whether the public have access to the statement.

a. Accessibility of the statement

In practice, prosecutors have struggled with the question whether communications within a closed group amount to the publication of a statement, and this has led to a certain reluctance to prosecute in this type of case.[71] This might be explained by reference to Baroness Scotland's distinction between public and private communications, and uncertainty regarding the degree of accessibility that must apply to the statement in question. As explained above, the accessibility-based understanding of publication derives from section 20(4), which stipulates that publishing a statement includes providing an electronic service 'by means of which the public have *access* to the statement',[72] and using an electronic service 'so as to enable or to facilitate *access* by the public to the statement'.[73] This interpretation of publication is also consistent with earlier case law in other contexts. For example, in *R v Sheppard* the appellants had published racially inflammatory material and been convicted of offences under the Public Order Act 1986.[74] Dismissing their appeals against conviction, the Court of Appeal held that publication is established where 'the material was generally accessible to all or available to or was placed before or offered to the public'.[75] Moreover, accessibility does 'not require proof that anybody actually read or heard the material',[76] nor

[69] See, for example, S. Warren and L. Brandeis, n 7 above.

[70] See, for example, n 8 above.

[71] J. Hall, *The Terrorism Acts in 2021: Report of the Independent Reviewer of Terrorism Legislation on the Operation of the Terrorism Acts 2000 and 2006, and the Terrorism Prevention and Investigation Measures Act 2011* (London: His Majesty's Stationery Office, 2023).

[72] Terrorism Act 2006, s 20(4)(b), emphasis added.

[73] *ibid*, s 20(4)(c), emphasis added.

[74] [2010] EWCA Crim 65.

[75] *ibid* at [34]. See also *R v Perrin* [2002] EWCA Crim 747, on the offence of publishing an obscene article (Obscene Publications Act 1959, s 2).

[76] *ibid* at [35].

that anyone 'would have seen it in the future'.[77] The point was that the material was available to anyone that might choose to access it.

A question that arises here concerns the extent to which ease of access is relevant (if at all). Locating the joinlinks needed to access a private IS Telegram channel is a time-consuming task that requires knowhow and expertise. It might be argued that these practical challenges mean that, for the purposes of the encouragement of terrorism offence, the content posted in these channels is relatively inaccessible to the public and therefore not published.[78] We do not agree, for five reasons.

First, the words of the statute should be given their ordinary meaning. This is the approach that has been taken to the term 'public place' in the Road Traffic Act.[79] In terms of the Terrorism Act 2006, section 20(4)(c) describes the use of an electronic service to 'enable or facilitate access' to the statement in question. The focus here is on whether the statement has been placed before the public so as to make it available. There is no reference in the statutory wording to the level of difficulty involved in accessing the statement.

Second, the Terrorism Act 2006 gives an extended meaning to 'public' so that it includes references to 'a meeting or other group of persons which is open to the public (whether unconditionally or on the making of a payment or the satisfaction of other conditions)'.[80] The legislation accepts that those to whom a statement is published may already have jumped through certain hoops. There is no limitation to the types of condition that may have to be satisfied, or requirement that it is easy to do so.

Third, assessing the ease or difficulty involved in accessing a statement brings with it various practical challenges, and questions of degree. There is the obvious challenge of articulating clearly the tipping point, that is, the point at which the difficulty in accessing a statement that

[77] *R v Perrin* [2002] EWCA Crim 747 at [22].

[78] For example, in its 1981 report *Breach of Confidence*, the Law Commission discussed when information should be regarded as being in the public domain. It drew a distinction between material that 'is generally available to the public' and material that would not be so regarded because 'it was only accessible to the public after a significant contribution of labour, skill or money' (Law Commission, *Breach of Confidence* Report Cmnd 8388 (1981) at para 6.74).

[79] *DPP v Vivier* [1991] 4 All ER 18; *Brown v Fisk* [2021] EWHC 2769 (QB).

[80] Terrorism Act 2006, s 20(3).

has been made available to (a section of) the public means that it can no longer be regarded as having been published. If a boundary had been intended, failure to delineate this boundary clearly could result in the offence being applied inconsistently in practice.[81] There is also reason to doubt whether such a limitation on the notion of publication would have much practical value. It is unlikely that defendants will seek to challenge whether a statement was published based on the difficulties in accessing it. Doing so would open the defendant up to embarrassing cross-examination about why the statement was inaccessible to ordinary members of the public ('Who is WhiteKnight123? Is he a friend of yours? What does he do when he's not hanging around on Fascist Forge?').

Fourth, whilst private IS Telegram channels are secretive and difficult to access, there are also important respects in which they are not analogous to, for example, a private group in which family members exchange messages and photos. In particular, private IS channels are characterised by anonymity, with pseudonyms or random strings of letters and numbers used for user IDs. Channel administrators will often not know the identities of the users in the channel. (It is this anonymity that enables some researchers and investigators to gain access). In reality, the difficulties in accessing these groups are designed not to limit the members of the group to trusted family and friends. Rather, it is to limit access to just one section of the public (pro-IS users). But, as section 20(3)(a) of the 2006 Act spells out, 'publishing' includes publishing to 'any section of the public'.

Fifth, it is important to view the posting of official IS propaganda in private Telegram channels in the context of the broader propaganda dissemination process. The remainder of this process involves posting links to these items of propaganda in searchable public Telegram channels and attempting to use platforms such as Facebook and Twitter to signpost the wider public to the propaganda. This process may be understood as a series of actions,[82] in which IS members and sympathisers act together for a shared purpose.[83] Taken as a whole,

[81] If so, a possible example of a borderline case would be *R v Shehroz Iqbar*, which concerned a closed WhatsApp group with 22 people in it: 'Royal Festival Hall: Shehroz Iqbal jailed for inciting attack', *BBC News*, 20 November 2020 at https://www.bbc.co.uk/news/uk-england-london-55016621. In this case the CPS (and the Court) must have taken the view that the group was constituted by members of the public despite its limited membership.

[82] *Thabo Meli v R* [1954] 1 WLR 228; *R v Le Brun* [1992] QB 61.

[83] *R v Jogee* [2016] UKSC 8.

this process – which we term chain accessibility – results in the propaganda being published to the public, notwithstanding the challenges involved in accessing the content at the initial stage of the process.

b. The purpose of the user

A further setting in which a distinction is drawn between public and private content is data protection. According to the EU's General Data Protection Regulation,[84] one of the permitted grounds for the processing of special categories of personal data (which include data that reveal political opinions or religious or philosophical beliefs) is that the data have been 'manifestly made public by the data subject'.[85] In her discussion of the ethics of online terrorism research, Conway comments, 'the only type of extremist and terrorist content that is uncontestably public is that which, like branded extremist and terrorist group propaganda, is produced and circulated online with the express purpose that it be widely disseminated, copied, downloaded, and similar'.[86]

Like the notion of chain accessibility that we introduced previously, Conway's observation emphasises the importance of the purpose for which content is posted when assessing whether or not it is public. Such an emphasis is also found in the Terrorism Act 2006's definition of publication. Section 20(4)(c) specifies that a statement is published when an electronic service is used '*so as to* enable or facilitate access by the public to the statement' (emphasis added). More generally, consideration of a user's purpose is important in a criminal justice context. Indeed, Article 5 of the CECPT – one of the catalysts for the creation of the encouragement of terrorism offence – requires states to criminalise the 'distribution, or otherwise making available, of a message to the public, with the *intent* to incite the commission of a terrorist offence' (emphasis added). It is also consistent with speech act theory, according to which the meaning of a speech act is determined by reference to the locution (the act of saying something), the illocution (the reason for which the speaker is using the locution) and the perlocution (the effect of what was said).[87] Of these, it is the

[84] Regulation (EU) 2016/679.

[85] *ibid,* Article 9(2)(e).

[86] M. Conway, 'Online Extremism and Terrorism Research Ethics: Researcher Safety, Informed Consent, and the Need for Tailored Guidelines' (2021) 33 *Terrorism and Political Violence* 367 at 372.

[87] S. Macdonald and N. Lorenzo-Dus, n 65 above.

illocution – the intention behind the locutionary act – that is the key aspect to consider in determining the intrinsic meaning of a speech act.[88] So, whilst it might be argued that propagandising is by its very nature a public activity, a speech act can only be so regarded if the intention of the speaker was to propagandise.

This part has examined the encouragement of terrorism offence in order to shed some light on the question when online content might properly be regarded as public. Three key points emerged. First, asking whether a statement was private is not the same as asking whether a statement was published to (a section of) the public. A statement might be published to a section of the public in conditions of secrecy and anonymity which, to some at least, would constitute a private setting. Second, difficulty in accessing content is not, in itself, sufficient to say that the content was not published to the public – particularly where these difficulties relate to just part of a broader process that is designed to make content available to a wide audience. And, third, determining the intention of the individual user is essential in order to determine whether they were engaged in this process of chain accessibility, or propagandising more generally. With these three points in mind, we turn next to consider the relevant provisions of the Online Safety Act.

D. Online Safety Act

When Ofcom considers it necessary and proportionate to do so, it is empowered to issue a Terrorism Content Notice requiring a service provider to use accredited technology to identify and swiftly remove publicly communicated terrorism content from its platform. This part describes the process for imposing a Terrorism Content Notice, before examining the Act's approach to distinguishing public from private communications and discussing its relationship to the encouragement of terrorism offence.

A. Terrorism Content Notices

A Terrorism Content Notice can require a user-to-user service[89] to use 'accredited technology' to, first, identify and 'swiftly take down' terrorism content that has been communicated *publicly* by means of the service and, second, prevent individuals from

[88] *ibid*.

[89] A user-to-user service is one on which a user can generate, upload or share content that may be encountered by other users of that service: Online Safety Act 2023, s 3(1).

encountering such content by means of the service.[90] For search services,[91] a Terrorism Content Notice may require the provider to use 'accredited technology' to identify search content that is terrorist content and to 'swiftly take measures designed to secure, so far as possible, that search content of the service no longer includes terrorism content identified by the technology'.[92] Accredited technology must have been accredited by Ofcom (or its appointee) as meeting 'minimum standards of accuracy' in the detection of terrorism content.[93] Its use may be supplemented by human moderators.[94] The notice may also require the provider to operate an effective complaints procedure to enable users to challenge decisions taken in respect of their content.[95] Terrorism Content Notices may impose requirements for up to 36 months.[96] The exact period must be specified in the notice, as well as other information including Ofcom's reasons for its decision, details of the accredited technology and the manner in which it should be implemented, a 'reasonable' time period for compliance and the consequences of non-compliance.[97] The maximum financial penalty that Ofcom is empowered to impose is £18 million or 10 per cent of the company's worldwide revenue (whichever is greater).[98]

[90] *ibid*, s 121(2)(a). Where the provider is already using accredited technology, the notice may require it to use it more effectively (s 125(2)). Section 231(11) states that accredited technology is an example of content identification technology. The latter term means 'technology, such as algorithms, keyword matching, image matching or image classification, which analyses content to assess whether it is content of a particular kind (for example, illegal content)' (s 231(2)).

[91] A search service means an internet service that is, or includes, a search engine: *ibid*, s 3(4). Search engines encompass services or functionalities that enable a person to search some websites or databases, but do not include services that enable a person to search just one website or database: *ibid*, s 229(1).

[92] *ibid*, s 121(3)(a)(i).

[93] *ibid*, s 125(12). The standards are approved and published by the Secretary of State, following advice from Ofcom (s 125(13)).

[94] *ibid*, s 121(5).

[95] *ibid*, s 125(3), (4).

[96] *ibid*, s 125(7).

[97] *ibid*, s 125(6). Directions on how the technology should be implemented could cover such things as technical set up, human moderation requirements or the image database to be used ('Online Safety Bill: Explanatory Notes' (HL Bill 87) 18 January 2023 at https://bills.parliament.uk/publications/49377/documents/2735).

[98] Online Safety Act 2023, s 140; Sched 13, s 4(1).

Before issuing a Terrorism Content Notice, Ofcom must first obtain a skilled person's report and give the service provider a warning notice.[99] The warning notice must contain a summary of the skilled person's report, the details of any accredited technology that the provider may be required to use, any other requirements that are being considered and the time period for which the requirements will apply.[100] The warning notice must also state that the provider may make representations to Ofcom and the time period within which such representations must be made.[101] The Terrorism Content Notice cannot be imposed until the period for representations has expired.[102]

A Terrorism Content Notice may only be issued if Ofcom considers it necessary and proportionate to do so.[103] In determining this, Ofcom must 'particularly consider' the twelve 'matters' listed in section 124(2). These include: the kind of service and its functionalities; the user base; the prevalence of relevant content on the service and the extent of its dissemination by means of the service (or, in the case of search services, its prevalence within search content);[104] the systems and processes already used by the service to identify and remove terrorist content; the level of risk of harm to individuals in the UK and its severity; the extent of any interference with the right to freedom of expression; and, the level of risk of a 'breach of any statutory provision or rule of law concerning privacy'. The tests of necessity and proportionality also apply if, following a review of a provider's compliance with a Terrorism Content Notice, Ofcom decides to issue a further notice.[105] A further notice (which may contain different requirements) may also be imposed if there are reasonable grounds for

[99] *ibid*, ss 122-123. The role of the skilled person's report is to assist Ofcom in deciding whether to impose a Terrorism Content Notice and advise about the requirements that the Notice might impose: *ibid*, s 122(2).

[100] *ibid*, s 123(2).

[101] *ibid*, s 123(2).

[102] *ibid*, s 123(5).

[103] *ibid*, s 121(1).

[104] Opposition amendments were moved at Commons Committee stage to change the word 'prevalence' to 'presence'. This was resisted by the Government: 'we think the significant power to compel companies to adopt certain technology … should be engaged only where there is a reasonable level of risk … The use of "prevalence" ensures that the powers are used where necessary' (HC Public Bill Committee col 473 16 June 2022).

[105] Online Safety Act 2023, s 126(4)-(6).

believing that a provider is failing to comply with a Terrorism Content Notice.[106] Where a further notice is issued, no skilled person's report or warning notice is required beforehand.[107]

During the legislation's Parliamentary passage, a number of concerns were raised about Terrorism Content Notices, with some leading human rights lawyers opining that – since the legislation 'ostensibly permits the state to compel [communication service providers] to carry out surveillance of the content of communications on a generalised and widespread basis' with insufficient safeguards – it likely violates the right to freedom of expression.[108] Others have argued that the process for issuing a notice should be subject to independent judicial oversight, with a full merits-based appeal process, as well as a general overarching duty to protect the privacy of users.[109] The process for accrediting technology has been described as unclear, with concerns about the effect on innovation and efficiency as well as the potential intrusiveness of the technologies that service providers might be required to adopt.[110] The potential scope of the power has also caused disquiet. The distinction between public communications and private communications has been described as vague and unclear,[111] with particular concern expressed that end-to-end encryption could be compromised by the application of the power to encrypted messages.[112]

---

[106] *ibid*, s 126(2)-(3).

[107] *ibid*, s 126(9).

[108] As argued by Matthew Ryder KC and Aidan Wills in a legal opinion commissioned by Index on Censorship: Index on Censorship, *Surveilled & Exposed: How the Online Safety Bill Creates Insecurity*, November 2022, 13 at https://www.indexoncensorship.org/wp-content/uploads/2022/11/Surveilled-Exposed-Index-on-Censorship-report-Nov-2022.pdf. See also the legal opinion prepared by Gavin Millar KC: Index on Censorship, *A Legal Analysis of the Impact of the Online Safety Bill on Freedom of Expression*, May 2022 at https://www.indexoncensorship.org/wp-content/uploads/2022/05/Legal-analysis-of-the-impact-of-the-Online-Safety-Bill.pdf.

[109] R. Earley, 'Online Safety Bill: Written evidence submitted by Meta (OSB79)', 16 June 2022 at https://bills.parliament.uk/publications/46955/documents/2012.

[110] C. Voge and R. Wilton, 'Internet Impact Brief: End-to-end Encryption under the UK's draft Online Safety Bill', 5 January 2022 at https://www.internetsociety.org/resources/doc/2022/iib-encryption-uk-online-safety-bill/; R. Earley, 'Online Safety Bill: Written evidence submitted by Meta (OSB117)' 14 December 2022 at https://bills.parliament.uk/publications/49172/documents/2668.

[111] Index on Censorship, *Surveilled & Exposed: How the Online Safety Bill Creates Insecurity*, n 108 above.

[112] See, eg, Open Rights Group, 'Online Safety Bill: Written Evidence Submitted by the Open Rights Group (OSB88)' 24 June 2022 at https://bills.parliament.uk/publications/47022/documents/2030.

b. The distinction between public and private communications

Understandably, the Online Safety Act does not attempt an abstract definition of what constitutes a public or private communication. Instead, section 232 specifies three factors that Ofcom must 'in particular' consider when deciding whether content is communicated publicly or privately by means of a user-to-user service,[113] for the purpose of both Terrorism Content Notices and proactive technology requirements (which may be imposed where a service provider is failing to fulfil its duties in respect of any illegal content, children's online safety or fraudulent advertising).[114] As originally laid before Parliament, these factors were:

- The number of individuals in the United Kingdom who are able to access the content by means of the service;
- Any restrictions on who may access the content by means of the service; and,
- The ease with which the content may be forwarded to or shared with users of the service other than those who originally encounter it.

The Government subsequently laid an amendment to the Bill in response to concerns raised by commentators, who warned that the original wording failed to reflect the cross-platform nature of terrorist propaganda dissemination strategies.[115] The effect of the amendment was to modify the final factor, in order to also take account of the ease with which content might be forwarded to or shared 'with users of another internet service'.[116]

---

[113] It is left to Ofcom to determine whether content is communicated publicly or not. On appeal against a notice or decision, the Upper Tribunal must apply judicial review principles (ss 167, 168). It would therefore seem possible that the Upper Tribunal might disagree with Ofcom's assessment as to the public/private divide, but nonetheless uphold it on the basis that the assessment was reasonable.

[114] Section 136(5) of the Online Safety Act states that Ofcom may impose a proactive technology requirement in a confirmation decision in order to ensure a provider complies with its duties in respect of illegal content, children's online safety or fraudulent advertising. Ofcom may make a confirmation decision if it is satisfied that a provider has failed (or is failing) to comply with a notified requirement (s 132(3)). Ofcom may make a notification requirement if it considers that there are reasonable grounds for believing that the provider has failed, or is failing, to comply with one of the duties listed in section 131 (s 130(1)).

[115] J. Hall and S. Macdonald, 'Online Safety Bill: Distinguishing between public and private communication' (website of the Independent Reviewer of Terrorism Legislation, 1 March 2023) at https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2023/03/Online-Safety-Bill-public-private.pdf.

[116] Amendment 290H; Lord Parkinson of Whitley Bay, HL Deb Vol 829 Col 1323 27 April 2023.

A question that immediately arises is section 232's dichotomous wording: content must have been communicated *either* publicly *or* privately. For the reasons given previously, this dichotomy is problematic. It is out of sync with the statutory wording of the encouragement of terrorism offence, it raises contentious questions about the meaning of privacy and it ignores the fact that the public and private sometimes overlap. A communication might properly be regarded as public notwithstanding the fact that it is disseminated in an online space that possesses (what for some are) the hallmarks of privacy. So, instead of presenting what may be an infeasible binary, when applying section 232 emphasis should be placed on whether a communication was public or not.

This approach is consistent with the list of factors found in section 232, which are geared towards determining whether a communication was published to the public. It is true that the statute stipulates that Ofcom must 'in particular' consider the three listed factors; in other words, that it is a non-exhaustive list of potentially relevant considerations. Nonetheless, the identification of these factors within the body of the statute accords them especial weight. It is also telling that the list in section 232 does not include the nature of the content nor a reasonable expectation of privacy – both of which are key criteria in determining whether the Article 8 right to respect for private life is engaged.[117] The non-inclusion of the nature of the content itself is unsurprising, given that Terrorism Content Notices require the proactive use of technology to identify and take down terrorism content and so cannot depend upon such content having already been identified. The reason for the non-inclusion of a reasonable expectation of privacy – the touchstone for whether an individual's private life is affected[118] – is less clear. It may be because the function of the public/private divide in the Act is less the protection of individual rights than delineation of tech companies' liability to Ofcom enforcement powers. Or it may simply reflect the fact that the existence of a reasonable expectation of privacy is itself contingent upon the factors that are listed in the statute. Either way, its absence suggests that when applying section 232 the focus should be whether the communication was published to the public.

[117] *Sutherland v Her Majesty's Advocate* [2020] UKSC 32.

[118] *Murray v Express Newspapers plc* [2008] EWCA Civ 446 at para 24, per Sir Anthony Clarke MR, summarising the principles stated by Lord Nicholls in *Campbell v MGN Ltd* [2004] UKHL 22; [2004] 2 AC 457.

Closer examination of each of the three factors that are listed in section 232 yields further insights of relevance to the practical application of the question whether or not content has been communicated publicly.

i. The number of individuals in the United Kingdom who are able to access the content by means of the service

The first of the factors is the number of individuals in the United Kingdom who are able to access the content by means of the service. By referring to the potential rather than an intended or actual number of receivers of the content, the implication appears to be that completely open communications on a platform such as Twitter are bound to be considered public. Indeed, content that is available *to the public generally* could be said to meet the very definition of content communicated publicly. Less obvious is content posted to a service which has a limited capacity to accommodate concurrent users, and which is removed after a period: any member of the public could in principle encounter the content but owing to the technical design or deficiencies of the service only a limited number of individuals will in practice be able to access it. Also less obvious is content posted to a public channel with an obscure name, or a private channel whose joinlinks are made publicly available. In these cases, any determined user may access the content, but the number of actual views may be minimal. Questions are also raised by the Act's reference to the number of individuals 'in the United Kingdom' that are able to access the content. For example, if a particular channel is geo-blocked in the UK, but not elsewhere, should UK users be regarded as unable to access the channel's content notwithstanding the possibility that it might be accessed using a VPN?

In a trusted (online) environment, a person might share personal information in the expectation that others will not violate that trust and share the information with others. A small number of users may indicate that the environment is one in which this relationship of trust exists. But this is not necessarily the case. In private IS channels, usernames are anonymised and identities are unknown. Moreover, those posting the propaganda in these channels do so in the expectation that the materials will be disseminated more widely, and the content is expressly designed for wide dissemination. In circumstances like these, the small number of users that are in practice able to access the content should carry little weight.

A further difficulty arises from the qualifying words 'by means of *the* service' (emphasis added). Presumably, these words are included to limit the responsibility of services. However, they suggest that considerations of numbers or scale are only relevant to the service's own user-base rather than to the number of individuals who might eventually access the same content on the internet generally, even though the service plays a vital role in its wider dissemination. This could arise where content designed for wide consumption, such as IS propaganda, is placed on one service as part of a wider dissemination strategy using multiple services. The strategy might use different services (Telegram, Instagram, JustPaste.it) simultaneously or deploy one service (e.g., Telegram or a decentralised messaging service or chat app) to advertise the presence of material in the hope that it will be picked up and taken viral using other services. In such instances, the number of individuals on one service ought not to be the primary factor. Shorn of the wider dissemination context, the harm risked and the need for greater Ofcom intervention may be overlooked.

ii. Any restrictions on who may access the content by means of the service (for example, a requirement for approval or permission from a user, or the provider, of the service)

Restrictions on access are a factor, but not determinative, and taken together with the previous factor squarely raise the case of terrorism content on a private channel with hundreds or perhaps thousands of members. The Act specifies that restrictions on access do not include a requirement to log in or register, to make a payment or take out a subscription, or to access the service using a particular technology (such as the TOR browser) or device, so long as generally available.[119] But all other restrictions on access are in scope including permission from a human administrator who could be a member of a proscribed terrorist organisation and conditional entry based on acceptable answers to bot-administered questionnaires ('Do you hate Jews?') so long as they amount to more than simple registration. The implication of this factor is that restrictions on access are a feature tending towards private communication even though the numbers of those accessing the content may be significant.

[119] Online Safety Act, s 232(3).

In the application of this factor, regard should be had not just to the technical features of the platform, but also their practical operation. At the platform level, private channels are designed to restrict users to those approved by the channel administrator. But in practice, making joinlinks openly available (albeit difficult to locate) undercuts the raison d'etre of the privacy-enabling feature. Section 232 should be interpreted as requiring Ofcom to have regard to the practical operation of the restriction on access, as well as the nature of the restriction itself.

The purpose of the restriction in question is also fundamental. In most instances, restrictions on access will be designed to limit the availability of the content (eg, members of a research institute sharing materials for a security-sensitive research project). But there are some circumstances in which the purpose of restrictions on access will be to facilitate increased dissemination of materials. A clear example would be restrictions designed to prevent law enforcement from accessing the content and taking steps to have it removed. The restrictions on access to private IS channels are designed to safeguard the initial stages of the propaganda dissemination process, in order to enable wider subsequent circulation of the materials. Here Ofcom should take into account the fact that the restriction serves the purpose of wider dissemination and making the content more, not less, publicly available.

iii. The ease with which the content may be forwarded to or shared with users of the service other than those who originally encounter it or users of another internet service

This factor addresses the platform's affordances (specifically, whether users can promote or highlight terrorist content to other users on the same or another platform) rather than the circumstances of the initial communication. It recognises that the numerical reach of content depends not only on the intention of the source or the nature of the message, but also the reaction of recipients. Consistency with the first factor suggests that some assessment should be made of the *number* of other users who may subsequently encounter it.

It would therefore seem that whether a message is itself public or private at the point of communication may be subordinated to the capacity to allow amplification within the same

or across another service.[120] A careful intention by the content-generator to limit the number of original recipients may be overridden by the technical ease of onward forwarding or sharing, whether or not the recipients have any intention of ever doing so. The power of this factor to nullify original intentions appears to depend on how 'service' is defined. If 'service' refers to a channel of communication which is limited by its administrators, such as a closed Telegram group, then its impact is limited. If it refers to the Telegram platform as a whole then its impact is extensive, because in principle it would be open to a member of a closed Telegram channel to share it with Telegram users more generally. The latter interpretation appears more in keeping with how the word 'service' is used in the Act more generally (eg, in the terms user-to-user service and search service), though ultimately it will be for Ofcom to determine which understanding is correct.

Determining the relative ease with which different content may be shared is also not obvious. Most content, even lengthy pdf documents, can now be shared with comparative ease. Additionally, as explained earlier, joinlinks occupy a particular function in the online jihadi universe that means that joinlinks themselves call for added attention, and may more readily qualify as content that is communicated publicly.

c. The relationship between section 232 and the encouragement of terrorism offence

As we have seen, while the nature of the content and the intention of the individual user may be influential in determining whether the user was engaged in the process of chain accessibility for the purposes of the encouragement of terrorism offence, these factors do not appear in the list of items to be considered in section 232. This may be explained by the fact that Terrorism Content Notices require the proactive use of technology and so cannot depend upon knowledge of what materials are being communicated and for what purpose. However, these differences in approach raise the possibility of an item of content being deemed to have been published for the purposes of the encouragement of terrorism offence yet communicated privately for the purposes of Terrorism Content Notices. This could be avoided by stipulating

[120] As originally drafted, this factor referred only to users of '*the* service' (emphasis added). The difficulty with this wording was that it focused on the specific service on which the content was originally shared. This risked reducing the likelihood of capturing wider dissemination strategies. For this reason, the Bill was amended during the Lords Committee stage to expand section 232 to include consideration of the ease with which content may be shared with users of *another* internet service (HL Deb vol 829 col 1323 27 April 2023).

that content will necessarily be deemed to have been communicated publicly for the purposes of section 232 if it has already been adjudged to constitute terrorism content by virtue of Schedule 5 and the encouragement of terrorism offence.

The opposite problem would arise if (contrary to the argument presented above) it was decided that, for the purposes of the encouragement of terrorism offence, the relative inaccessibility of content to the public meant that it was not published. The non-commission of the offence would mean that, according to Schedule 5, it was not terrorism content and therefore the power to issue a Terrorism Content Notice would not apply. Such an interpretation of publication would therefore place the early stages of the chain dissemination process beyond the scope of Ofcom's enforcement powers. Interpreting publication in the manner suggested is necessary to ensure that ostensibly private online spaces are not exploited to disseminate terrorist propaganda.

E. Conclusion

The sheer volume of content posted online every minute means that automated content moderation tools are essential.[121] Unsurprisingly, therefore, the Online Safety Act not only vests in Ofcom the power to require service providers to use accredited technology to identify and remove terrorist content, but also confers the power to require the use of proactive technology to mitigate and manage the risk posed to users by a wide variety of different online harms. This article has shown that the Act's distinction between public and private communications is key to the efficacy of these powers. This distinction will need to be applied to communications across many different online fora, including purportedly private channels on platforms such as Telegram, decentralised messaging services, chat apps and even virtual spaces on Metaverse platforms. Moreover, as Ofcom has pointed out, it will fall 'in the first instance [to the thousands of companies to which the Online Safety Act applies] to assess for themselves … the content that is communicated 'publicly''.[122]

[121] S. Macdonald, A. Mattheis and D. Wells, *Using Artificial Intelligence and Machine Learning to Identify Terrorist Content Online* (Tech Against Terrorism Europe, 2024) at https://static1.squarespace.com/static/63e0c75f41ff767f07530a6f/t/65a5349648ce18428d686126/1705325720146/TATE+-+AI+REPORT+FINAL+%281%29.pdf (accessed 13 April 2024).

[122] *Protecting people from illegal harms online Annex 9: Guidance on content communicated 'publicly' and 'privately' under the Online Safety Act* (London: Ofcom, 2023), 2.

Using the IS propaganda dissemination process as a practical example to open up analysis, the article has identified several points that it is suggested should inform the interpretation and application of the section 232 distinction between public and private communications. First, it may not be possible to formulate an overarching public/private distinction, given the difficult conceptual questions about the meaning of privacy. For this reason, when applying section 232 the key question should be whether the communication was public or not. Second, the fact that only a small number of users are able to access content does not necessarily indicate the absence of an intention that the content be shared widely. Third, when considering any restrictions on access, regard must be had to the practical operation of these restrictions and to the purpose for which they are imposed. Some restrictions on access are designed to enable wider public dissemination at the later stages of the chain accessibility process.

This brings us back to the challenge identified at the outset: to simultaneously resolve concerns about both security and individual rights. While the approach we have advocated may ensure the efficacy of Terrorism Content Notices, and proactive technology requirements more generally, could it result in inappropriate intrusions into essentially private interactions online? In particular, what are the implications of our approach for end-to-end encryption? The answer to this has two parts.

While private channels on Telegram are not encrypted,[123] it is not hard to imagine a situation in which the administrator of a private IS channel on Telegram invites those who join the channel to also join a group on an encrypted service such as WhatsApp. Suppose that the administrator sends messages encouraging terrorism to the rest of the WhatsApp group, and that one of the group members chooses to hand these messages to the authorities. Two conclusions follow from the argument advanced in this article. First, by sending these messages to the other members of the WhatsApp group the administrator published them for the purposes of the encouragement of terrorism offence. Second, in terms of the Online Safety Act, the messages would be regarded as terrorism content and they should be regarded as having been communicated publicly. The fact that the messages were sent using an encrypted service would not negate this, since anyone that had invested the time in locating

[123] https://telegram.org/faq.

the joinlink to the private Telegram channel would then have been able to access the WhatsApp group also. To hold otherwise would mean either saying that the administrator did not commit the encouragement of terrorism offence, or that the messages were simultaneously published to the public (for the encouragement of terrorism offence) yet not communicated publicly (for Terrorism Content Notices).

However, this is not to say that the wider public interest in the security of encrypted communications is irrelevant. Under the Online Safety Act, the question whether a communication was public or private is distinct from the question whether a Terrorism Content Notice or proactive technology requirement should be issued. Even if terrorism content is being communicated publicly, a Terrorism Content Notice should only be issued if it is considered necessary and proportionate to do so – and, even then, Ofcom still retains a discretion whether to issue a Notice or not.[124] There is a significant public interest in the security of encrypted communications, and it is essential that this is given due weight by Ofcom when assessing necessity and proportionality and exercising its residual discretion. There are various reasons why the grounds for imposing a Terrorism Content Notice on an encrypted service may not be sufficient to meet the demands of necessity or proportionality. For example, there may be alternative methods of disrupting the dissemination of terrorism content on the platform, or there may be a risk of displacing the activity to other online spaces that are more difficult to monitor.[125] Similar reasoning applies to the decision whether to impose a proactive technology requirement in respect of other types of illegal content, children's online safety or fraudulent advertising.[126] The key point for present purposes is that these are important issues that should be discussed in their own right, and this discussion is likely to be obscured if it is forced into the language of public versus private communications. As this article has shown, the public and private frequently overlap – so privacy interests may be at stake even when content is communicated publicly.

[124] Section 121(1) states that 'If Ofcom consider that it is necessary and proportionate to do so, they *may* give a notice …' (emphasis added).

[125] J. Whittaker and A. Craanen, 'The Unintended Consequences of Content Removal, Marginalisation and the Case of BitChute' (forthcoming).

[126] Before imposing such a requirement, Ofcom must consider the matters listed in section 136(8). While there is no explicit reference to necessity or proportionality, the matters listed do include the impact on users' freedom of expression, any potential violations of privacy and whether compliance could be induced using less intrusive measures.