Online terrorism and online laws

*Clive Walker*<sup>a</sup> *and Maura Conway*<sup>b</sup>

<sup>a</sup> School of Law, University of Leeds, Leeds, UK

<sup>b</sup> School of Law and Government, Dublin City University, Glasnevin, Dublin, Ireland

Terrorist and extremist movements have long exploited mass communications technology in pursuit of their political ends. The advent of the internet offers new opportunities. In response, state counter-measures seek to stem the impact of extreme ideologies by a number of tactics. “Positive” measures refer to those online initiatives that seek to make an impact through digital engagement and education and the provision of counter-narratives. “Negative” measures describe those approaches that advocate for, or result in, the deletion or restriction of violent extremist online content and/or the legal sanctioning of its online purveyors or users. More sanctions-based outcomes arise through discretionary state activity such as warnings and counselling of vulnerable individuals, or through disruptive counter-measures such as bans on the giving of lectures or prohibitions on the entry into the country of speakers or the taking down of extremist internet sites. Other measures step over into criminal justice, as when individuals are prosecuted for collecting materials or information (including typically information downloaded from the internet) or for issuing messages which can be construed as direct or indirect incitements to terrorism. This paper will analyse the responses to extremist uses of the internet, with an emphasis upon legal responses – “online laws”.

**Keywords:** prevent; pursue; criminal justice; online laws

**Background**

Terrorism can be broadly defined as a combination of “violence and propaganda”, whereby “[v]iolence aims at behaviour modification by coercion [and] [p]ropaganda aims at the same through persuasion” (Schmid & De Graaf, 1982, p. 14). Therefore, its protagonists and the counter-terrorism laws must produce not only “violence” but also “armed propaganda” (Stohl, 1990, p. 93). This twin-track approach, which is also reflected in the legal definition contained in the Terrorism Act 2000, section 1, was famously illustrated by the pronouncement of the then director of publicity for Sinn Féin, Danny Morrison, in 1981, when he questioned: “Who here really believes we can win the war through the ballot box? But will anyone here object if, with a ballot paper in this hand and an Armalite in the other, we take power in Ireland?” (McAllister, 2004, p. 124). Even 30 years ago, Morrison felt that he was engaged in a perilous exercise – akin to “walking on eggshells” (*R v Martin and others*, 1992, p. 14) - and, while Director of Publicity for Sinn Féin, he paid the price with a conviction (later overturned) and several years of imprisonment for his proximity to the IRA’s “punishment” machinery (*R v Morrison*, 2009).

Terrorist and extremist political movements have long exploited the “performativity” (de Graaf, 2011) of every available mass communications technology. Morrison’s forefathers in the Irish Republican press in the nineteenth century were repeatedly charged with offences against the state (*Martin v R*, 1848; *R v Charles Gavan Duffy*, 1848; *R v Grey*, 1865; *R v John Mitchel*, 1848; *R v Sullivan and Pigott*, 1868). Contemporary attention has turned to electronic news media, including terrestrial and satellite
television, such as Hizbollah’s establishment of its Al Manar television station in the early 1990s (Saul & Joyce, 2010), through to internet media, as latterly represented by the “slickly” produced contemporary digital content of the Islamic State (IS) (Ingram, 2014; Klausen, 2015).

In response, the state’s counter-measures seek to stem the impact of extreme ideologies by a number of tactics. Some measures positively engage and provide counternarratives, responses which are especially attractive since they endorse and promote the value of free speech. This stance is an aspect of the “Prevent” strand of the UK’s counterterrorism strategy by which action is taken to stop people becoming terrorists or supporting violent extremism, including by “Engaging in the battle of ideas – challenging the ideologies that extremists believe can justify the use of violence, primarily by helping Muslims who wish to dispute these ideas to do so” (Home Office, 2006, p. 2). In this way, there is an emphasis on anticipatory risk by attacking upstream the ideologies and behaviours which might foster violence, counselling the vulnerable, and engaging with relevant sectors such as higher education which can be sites for “radicalization”. Problematic aspects of “Prevent” include uncertain boundaries with community integration, weak causal links between radicalization and terrorism, the perception of spying on minority communities, and vague performance indicators (Bartlett & Miller, 2011; Bouhana & Wilkstro´m, 2011; Home Office, 2011; Huq, 2013; Lakhani, 2012; Lord Carlile, 2011; Munton, 2011; Thomas, 2012).

Some aspects of “Prevent” have a sharper focus and more sanctions-based outcomes, and so the battle of ideas may lead into another aspect of CONTEST, namely “Pursue”, by which measures are taken to deal with terrorist threats. Some of these measures remain within “Prevent”, and trigger discretionary state activity such as warnings and counselling of vulnerable individuals; some arise through disruptive counter-measures which can be backed by law such as bans on the giving of lectures or prohibitions on the entry into the country of speakers or the taking down of extremist internet sites. Others step over into “Pursue”, as when individuals are prosecuted for collecting materials or information (including typically information downloaded from the internet) or for issuing messages which can be construed as direct or indirect incitements to terrorism. In this way, repressive action is taken to starve terrorists of what Prime Minister Thatcher called in 1985 the “oxygen of publicity” (http://www.margaretthatcher.org/speeches/display document.asp?docid¼106096).

The state use of counter-measures to shape or close down communications is of venerable lineage and governments have long responded with robust legal restraints. Amongst the most prominent restrictions were those introduced in the Republic of Ireland (1976 – 1994) and the UK (1988 – 1994) arising from the Northern Ireland conflict and banning the broadcasts of Loyalist and Republican paramilitaries (Banwell, 1995; Horgan, 2002; Kingston, 1995).

The advent of the internet means new communications opportunities and facilities for terrorists, just as it has proven a boon for everyone else with access to the technology. For terrorists, there are three potential advantages, all with profound legal implications. The first and most alluring new opportunity is that the internet becomes itself a new societal vulnerability which the terrorists may target. However, while there have been some attacks through hacking and denial of service, the more lurid catastrophes, such as aircraft falling from the sky through sabotaged air traffic control systems, that have often been elaborated upon in the media, have not materialized (Conway, 2014; Gordon & Ford, 2002; Sundaram & Jaishankar, 2008; Weimann, 2005), though governments have become highly conscious of the need for cybersecurity and have issued policies accordingly (Cabinet Office, 2009, 2011; Department of Homeland Security, 2003, 2013; Home Office, 2009a; Legrand, 2014).
At the opposite end of the spectrum, the internet is secondly an increasingly invaluable “back-office” tool of terrorism. In this sense, a variety of other functions can be served by terrorist use of the internet, including information-gathering on potential targets, planning, logistics (including the gathering of financing and the movement of resources), recruitment, and, most basic but most vital of all, intragroup communications (UN Office on Drugs and Crime, 2012; Walker, 2006).

The third aspect of usage concerns the use of the internet as a mass media outlet for publicizing and explaining activities and for engagement with supporters and potential supporters. This aspect of internet activity affords particular advantages to terrorists because it is harder to control and close down than traditional media outlets, being cross-jurisdictional in operation and adaptable to enforcement constraints. Furthermore, internet access means that terrorists are no longer wholly reliant on the mass media to act as carriers and even intermediaries, because it affords otherwise unattainable prominence and meaning to their violence, giving rise to the possibility of “apology” for terrorism (Carruthers, 2000, p. 170; Walker, 2011, chap. 8). The internet now presents actors, whether mass movements or lone actors, with increased opportunities to propagate globally their own interpretations and messages (Weimann, 2014). Thus, even as early as 1998, approximately half of the (then) 30 groups designated as foreign terrorist organizations under the US Antiterrorism and Effective Death Penalty Act of 1996 operated websites, including the Lebanese Hizbollah (Conway, 2005a), the Sri Lankan Tamil Tigers (Tekwani, 2003), and others (Conway, 2005b). These early websites fulfilled a largely unidirectional “broadcast” function. Their content was tightly controlled by the terrorist organizations, and opportunities for interaction were negligible. By the next decade, online interactive forums had become popular (Damphouse, 2008; Zelin, 2013); many forums remain active today, but nationalist and other long-established extremists (Frennett & Smith, 2012; German Federal Office for the Protection of the Constitution, 2013) and now jihadis (Brachman, 2009, p. 19; Zelin, 2013) increasingly have greater recourse to mainstream social media platforms. Moving to the present era, IS and its online supporters have proven themselves to be perhaps the most adept and prolific producers and disseminators of digital content. IS does not have a single official website; instead “official” IS online content emanates from several IS-affiliated content production entities or so-called “media departments” (such as al-Furqan Media, al-Hayat Media Center) and is distributed via jihadi forums, but increasingly also via the major social media platforms and other content-hosting sites. In July 2014, the group released the first issue of its Dabiq magazine, similar in style to Al-Qaeda in the Arabian Peninsula’s Inspire (Lemieux, 2014). However, the relationship between consumption of extremist online content, such as that produced by IS, and the adoption of extremist ideology or of recruitment to terrorism remains unproven (Benson, 2014; House of Commons Home Affairs Committee, 2012, para. 38; Rieger, Frischlich, & Bente, 2013; von Behr et al., 2013). Nevertheless, the growth of online content from terrorist groups and its potential attractiveness to, and resonance with, discontented “digital natives” (young people who have grown up with the internet) has become a source of official apprehension throughout Europe (EU Counter Terrorism Coordinator, 2014, pp. 2–3). A particular alleged danger that has received utmost attention is the role of online jihadi content influencing young people to travel to Syria as “foreign fighters” and “jihadi brides” (Fisher & Prucha, 2014), which gives rise to trepidation about their role in the conflict zone and even more so regarding their capacity for future terrorism upon their return home. As a result, there has been a call to take action against violent extremism on the internet by the United Nations Security Council Resolution (UNSCR) 2178 of 24 September 2014. “Addressing the growing issue of foreign terrorist fighters” in Iraq and Syria, Article 17, urges Member States, in this context, to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications and resources, including audio and video, to incite support for terrorist acts, while respecting human rights and fundamental freedoms and in compliance with other obligations under international law.
The remainder of this paper will describe and analyse the responses to the foregoing extremist uses of the internet, with emphasis upon legal responses — “online laws”. Much of the following is therefore concerned with what is called “content control”: efforts on the part of regulators to regulate what sort of material is made available on the internet, including the removal of “objectionable” materials currently accessible and the erection of barriers to the uploading of such materials. As already indicated, the latter so-called “negative” measures may be contrasted with more “positive” approaches. “Negative” measures describe all those approaches that advocate for, or result in, the deletion or restriction of violent extremist online content and/or the legal sanctioning of its online purveyors or users; “positive” measures refer to those online initiatives that seek to make an impact through digital engagement and education.

Content control issues in general

Online laws may be a tempting option for regulators, but they must operate within normative boundaries, which require consideration of efficacy (even if achieved only in symbolic terms) and regard to constitutionalism which points towards values such as the rule of law and human rights. On the latter point, both Article 19 of the UN’s Universal Declaration of Human Rights (UNDHR) 1948 and Article 10 of the European Convention on Human Rights 1950 (ECHR) identify freedom of expression and the right to seek, receive, and impart information (including from foreign countries, as confirmed by the European Court of Human Rights in Khurshid Mustafa and Tarzibachi v Sweden and Ta’rsasa’g a Szabadsa’gjogoke’rt v Hungary) as fundamental human rights. The conferment of rights nonetheless recognizes that freedom of expression can be counterbalanced by limitations for the sake of, inter alia, “public order” (UNDHR, Article 29) or “national security, territorial integrity or public safety, for the prevention of disorder or crime” (ECHR, Article 10(2)). This dichotomous international regime, in conjunction with states’ widely differing social, political, and religious contexts, added to the absence of any comprehensive international law definition of terrorism, opens a wide discretion for variant interpretations and levels of tolerance (for surveys, see Akdeniz, 2010; Golumbic, 2008; Sieber & Brunst, 2007).

Uncertainties as to the boundaries of online laws can also arise through differences between the “real” and “cyber” worlds. Existing rules about speech, promulgated for application to meetings, marches, and printed materials in the real world, can be applied to the internet, as adopted in the EU for racist speech (European Commission, 2001). However, it is arguable that the internet requires specific legislation tailored to its specific characteristics which impart differences in terms of risk and legal attributes. The risk factors include quantity (potential audience size and accessibility without the intercession of editors or otherwise) as well as quality (the intensity and instantaneity of messages and the facility for personal interaction). The special legal attributes include the complexities of trans-jurisdictional impact, the potential for anonymity, and the technical expertise and specialist equipment required to gather evidence against wrongdoers (Spiecker genannt Döhmamnn, 2013). These risk factors and legal attributes become especially troubling when the effects of online extremism may prove so pernicious.

It follows that many countries have enacted online laws, many of them prompted by terrorism developments, such as 9/11 and 7/7. The online laws secure some tangible benefits in terms of resolving the boundaries of forbidden conduct in accordance with the requirement of the rule of law. However, criticisms also arise about the creation of a disproportionately blanket “surveillance society” (Fuchs et al., 2011; House of Commons Home Affairs Committee, 2008; House of Lords Select Committee on the Constitution, 2009; Lyon, 2005; Scheinin, 2009) affecting the human rights of all and not just suspects.
(Joined Cases C-293/12 and C-594/12, 2014; Walker & Akdeniz, 2003), the dubious efficacy of many provisions, and the absence of more innovative responses. Even the security authorities appear dissatisfied with the regime, and so, as revealed by Edward Snowden, they allegedly practice “dataveillance” on a vast scale in ways which may transgress the often generous boundaries of existing online law (Liberty v GCHQ, 2014, 2015).

“Negative” online measures

States seek to abate the use of the internet for violent radicalization and other violent extremist purposes by limiting user and audience access, either by *ex ante* or *post hoc* censorship of content (such as by criminal law or take-down measures) or by controls over internet infrastructure (such as by filters and firewalls), or by combination of the two. As for controls over internet infrastructure, states, especially powerful states with large defence budgets and advanced technological capabilities, can seek to constrain the effectiveness of terrorist cyber-based strategies by limiting user and audience access to online platforms through control of the internet infrastructure. A common element for governmental filtering is generally an index of websites that are blocked. Such filtering of content is carried in countries such as China, Iran, Saudi Arabia, and Singapore, though more often related to the suppression of political dissent or unacceptable cultural intrusions than because of terrorism. However, an exceptional instance of terrorism filtering arose in December 2014, when the government of India instituted a block on 32 major websites on the basis of their hosting what Arvind Gupta, head of Information Technology for India’s ruling Bharatiya Janata Party, called “Anti India content from ISIS”. Five sites (weebly.com, vimeo.com, Pastebin, dailymotion.com, and gist.github.com) were unblocked after agreeing to remove “Anti-India” content (Panigrahi, 2015).

A survey will now be undertaken which will concentrate upon online laws in the US, UK, and Europe. As well as “negative” online national and international laws, some counter-measures involve quasi-legal or “soft law” voluntary codes or regulatory dialogue with communication service providers (CSPs).

*US online laws*

Any effort to impose negative controls over internet-based speech will be especially contentious in the US context because the First Amendment to the US Constitution prioritizes freedom of expression, including the right to publish extreme and offensive materials on the internet (Walker & Weaver, 2013). As a result, many extremist and terrorist websites have been hosted in the US. For example, in 1997, controversy erupted when it was revealed that the State University of New York (SUNY) at Binghamton was hosting the website of the Revolutionary Armed Forces of Colombia (FARC), and that a Tupac Amaru (MRTA) solidarity site was operating out of the University of California at San Diego (UCSD) (Conway, 2007a). SUNY officials promptly shut down the FARC site. In San Diego, officials decided in favour of free speech, and the Tupac Amaru site remained operative for some years. It was not illegal at that time to host such a site, even if a group was designated a foreign terrorist organization by the US Department of State, as long as a site was not seeking financial contributions or providing financial support. This toleration persists even after 9/11. For instance, though listed in 2011 by the UN 1267 Committee and by the US as a Specially Designated Global Terrorist (SDGT) under US Executive Order 13224, and proscribed in the UK under the Terrorism Act 2000 (Proscribed Organizations) (Amendment) (No. 2) Order 2013, SI 2013/3172, Imam Kavkaz (Caucasus Emirate) remains available on the internet through the sympathetic Kavkaz Centre (http://www.kavkazcenter.com) which is hosted by Cloudflare in the US.
The principal qualification to free speech made by online laws since 9/11 has been the aggressive usage of the anti-terrorist offences of material support (Chesney, 2005, 2007; Cole, 2008; Ward, 2008). First, 18 United States Code (USC) section 2339A, enacted originally by the Violent Crime Control and Law Enforcement Act 1994, Public Law 103-322 section 120005, addresses the provision directly or indirectly of financial or other material support or resources knowing or intending their use for terrorist activities in contravention of 36 listed offences. Proof of intent is required that the recipient is a terrorist group (even recklessness is not sufficient and certainly not negligence: US v Lakhani, 2007). By 18 USC section 2339B, enacted originally by the Antiterrorism and Effective Death Penalty Act 1996, Public Law 104-132, section 303, it is an offence without any requirement of intent or belief as to the terrorist nature of the acts to be aided to provide material support or resources (including to oneself) to a designated foreign terrorist organization under 8 USC s 1189(a)(1), a concept which was inserted by the Antiterrorism and Effective Death Penalty Act 1996, section 302 and elaborated by the Code of Federal Regulation volume 31, sections 597.101-901. Al-Qaida was listed in 1999. The Intelligence Reform and Terrorism Prevention Act 2004, Public Law 108-458, section 6603(c)(2), clarified that knowledge (but still not recklessness or negligence) is confined to the fact that the group is designated or has engaged in terrorism. Title III of the USA Patriot Act, sections 803 to 815, also known as the International Money Laundering Abatement and Anti-Terrorist Financing Act 2001 (Public Law 107-56), augmented sections 2339A and 2339B. It widened the notion of “material support or resources” by including, for example, expert advice or assistance and increased the penalties to up to 15 years and up to life if the death of any person results.

Though just a handful of truly speech-related prosecutions have arisen, free speech activists fail to be convinced that the normal constitutional test of clear and present danger of imminent harmful action, the classic test used in Brandenburg v Ohio (1969), is met. In 32 County Sovereignty Committee v Department of State (2002), a number of Irish dissident republican groups linked to the Real IRA sought to contest their designation as foreign terrorist organizations. The US Court of Appeals concluded that the groups demonstrated neither a property interest nor a presence in the jurisdiction, and so the Secretary therefore did not have to provide 32 County or the Association with any particular process before designating them as foreign terrorist organizations, and that the decision had been taken on the basis of enough information. In US v Iqbal and Elahwal, Iqbal pleaded guilty to providing material support to Hizbollah (a designated foreign terrorist organization) by operating a satellite television service known as HDTV Limited, which carried the Al Manar television channel and for which Iqbal was directly paid thousands of dollars by Al Manar. Next, in 2012, Tarek Mehanna was sentenced to more than 17 years’ imprisonment for conspiracy to provide material support to Al-Qaida, providing material support to terrorists (and conspiracy to do so), conspiracy to commit murder in a foreign country, conspiracy to make false statements to the FBI, and two counts of making false statements. His internet-related material support arose from, among other things, translating and posting on the internet Al-Qaida recruitment videos and other documents, including some that encouraged violence against American military forces. A number of criticisms were voiced about this curtailment of free speech (Abel, 2013; Brown, 2012; Knox, 2014).

The constitutionality of the material support offences was upheld by the US Supreme Court in 2010 against challenges based on free speech and vagueness in Holder v Humanitarian Law Project (2010), a decision which provoked further criticism (Cole, 2012; Marguiles, 2011–2012; Tomkins, 2011). The Humanitarian Law Project planned to train the Kurdistan Workers’ Party and the Liberation Tigers of Tamil Eelam in peaceful modes of conflict resolution. The Supreme Court confirmed that Congress had intended to prohibit aid to such groups, even if for the purpose of facilitating peace negotiations or United Nations processes, because such assistance fell within the definitions used by the section and
because, as a matter of policy, any assistance could help to legitimize the terrorist organization and allow it to allocate its own resources for purely violent activities. Seeking to justify the decision, Chief Justice John G. Roberts Jr argued that “under the material support statute, plaintiffs may say anything they wish on any topic” and pointed out that “Congress has not sought to suppress ideas or opinions in the form of ‘pure political speech’” (pp. 20–21). Despite these statements, individuals can be convicted of terrorism offences on the basis of online speech acts with very tenuous links to notions of financing or support by deed. As an editorial in *The Washington Post* (2010) put it:

Which of the following is illegal under the law that bars providing “material support” to terrorists?:

1. Giving money to a terrorist organization.
2. Providing explosives training to terrorists.
3. Urging a terrorist group to put down its arms in favor of using lawful, peaceful means to achieve political goals.

After Monday’s Supreme Court ruling in Holder v. Humanitarian Law Project the answer is: all three.

A commitment to First Amendment rights is equally the reason proffered by major US social media companies, such as Facebook, Twitter, and YouTube, for their decisions to decline to censor some of the violent extremist content posted to their sites. In 2011, US lawmakers exhorted Twitter and YouTube to cancel accounts linked to al-Shabab (Subcommittee on Counterterrorism and Intelligence, 2011). In response, Twitter has adopted the mantra of being “the free speech wing of the free speech party” (Barnett, 2011) and has in the past refused requests from government officials, activist organizations, and concerned individuals to cancel the accounts of other extremist groups. However, its policy began to shift in 2012 towards a more country-specific approach (Taylor, 2012, p. 10), and in January 2013, Twitter cancelled the account of al-Shabab following the group tweeting photographs of the body of a French commando whom they had killed followed by explicit threats to execute Kenyan hostages (Howden, 2013). In the event, al-Shabab quickly re-established their Twitter account, under a slightly different name, and Twitter was once again embroiled in controversy when the group live Tweeted their attack on the Westgate shopping mall in Nairobi, Kenya in September 2013 (Alexander, 2013). Twitter appears to have shifted its position since then, engaging in a wholesale cull of violent jihadi accounts from mid-2014 possibly, according to one analyst, at the behest of the US government and almost certainly also influenced by the use of these accounts to spread images from and links to beheading videos (Friedman, 2014).

These verdicts by CSPs of life and death over social media accounts highlight the lack of transparency surrounding how decisions are taken as to which accounts are cancelled and why. Twitter has no detailed and publicly available guidelines on the matter but merely reports on requests (which are posted at http://www.chillingeffects.org), as does Google (http://www.google.com/transparencyreport/removals/government/). The Edward Snowden revelations also alleged on-going interchanges with state agencies which have become so embarrassing for CSPs that they have proposed greater use of encryption (Yadron, 2014).

**UK online laws**

Compared to the US, the UK anti-terrorism online laws contain a more comprehensive catalogue of criminal offence and take-down measures, with less restraint in their application, though the results often remain controversial (Carlile & Macdonald, 2014; Conway, 2006; Cram, 2009; Walker, 2014, chaps 2, 6). These incursions into online activities are unashamedly more restrictive, in line with the more qualified expressive rights under Article 10 of the European Convention on Human Rights, as
implemented by the Human Rights Act 1998, compared to the more forthright statements in the US Constitution.

Reflecting the “Pursue” element of CONTEST, the UK legislature has developed the use of “precursor crimes” in order to allow for early intervention against terrorist threats without having to await the conclusion of an outrage. The mainstay precursor offences dealing with extremist materials on the internet are sections 57 and 58 of the Terrorism Act 2000. Section 57(1) is contravened by possession of an article in circumstances which give rise to a reasonable suspicion that the possession is for a purpose connected with terrorism. The articles possessed will often be lawful in themselves and even commonplace – such as rubber gloves, batteries, and wires. Regarding multiple-use articles such as computer disks or cars, section 57(1) only requires “a” purpose to be nefarious, not a main or sole purpose. In R v Omar Altimini (2008), computer materials held by a “sleeper” contravened section 57. Recognizing possible overreach, section 57(2) offers a defence by proof on an evidentiary basis according to R v Director of Public Prosecutions, ex parte Kebilene (2000) that possession of the article was not for a purpose connected with terrorism. Section 57 is highly valued by police and prosecutors. Since 2006, sentences have increased and include an award of 12 years (“the top of the spectrum”) for a vast collection of propaganda and instructional guides, observations of security at Manchester Airport, and musings about attacks (R v Sultan Muhammed and Aabid Hassain Khan, 2009).

Even more relevant are the offences under section 58. Section 58(1) contains two variants of actus reus: collecting or making a record of information likely to be useful to terrorism or possessing a document or record containing information of that kind. A “record” includes electronic formats: section 58(2). The defendant must be aware of the nature of the contents, according to R v G and J, 2009, paras. 47, 48. However, the Crown is also not required to show that the defendant harboured a terrorist purpose. In RvK, the defendant, Khalid Khaliq, argued boldly that section 58 was insufficiently certain to comply with Article 7 of the European Convention. In response, the Court of Appeal sought to remedy any imprecision by reading in the requirement of a purpose useful to terrorism. Thus, the purpose of the information (rather than the possessor) is at stake – it intrinsically “calls for an explanation”, which goes further than previous interpretations (see Hodgson & Tadros, 2009; R v G and J, 2009, paras 43, 44). The information must be of an intrinsic kind which gives rise to a reasonable suspicion that it is likely to provide practical assistance to a person committing or preparing terrorism rather than simply encouraging the commission of terrorism. To illustrate, the A–Z of London could be useful to a terrorist in the location of a target, but that use would not fall within section 58 since that document does not intrinsically arouse suspicion. In R v Terence Roy Brown (2011, paras 17, 34), an internet seller of literature, such as The Anarchist Cookbook, which he admitted was useful to terrorists, was convicted even though he depicted his activities as a non-ideological business on which he paid taxes. By section 58(3), it is a defence to prove a “reasonable excuse”. Section 58 is commonly invoked against those who download and disseminate extremist internet material. In R v Khuram Shazad Iqbal (2014), the defendant (aka “Abu Irhaab”) had used Facebook and Twitter to post links to 848 examples of extreme content (videos and articles) on the internet and was found with nine copies of the Al-Qaida magazine Inspire on his laptop.

There have been 76 charges under section 57 and 44 under section 58 from 11 September 2001 to 31 March 2013 (out of 375 under anti-terrorism legislation) (Home Office, 2013, Tables A05a and b). The main controversies surrounding these offences concern the equivocal nature of the actions involved and the switched burden of proof of reasonable excuse. Journalists and even scholars (as in the case of Nottingham University student Rizwaan Sabir, 2011) can in theory fall foul, as can self-proclaimed freedom-fighters, such as another student in R v Gul, 2013, para. 54). Despite the shifts in judicial interpretation which have occurred, the European Court of Human Rights in Jobe v United Kingdom
rejection of a complaint that section 58(3) had resulted in the application of a retrospective criminal penalty. The Court was of the view that the complaint about the interference with free expression was also “manifestly ill-founded”:

It was clearly justified by the legitimate aims of the interests of national security and the prevention and disorder of crime. It was also necessary in a democratic society, particularly when s. 58 did not criminalise in a blanket manner the collection or possession of material likely to be useful to a person committing or preparing an act of terrorism; it only criminalised collection or possession of that material without a reasonable excuse. In the Court’s view, this is an entirely fair balance to strike. (para. 35)

Countering the ideology of terrorism, often in the guise of online terrorism, is further addressed by offences against extremist speech and publications in sections 1 and 2 of the Terrorism Act 2006. These offences react not only to the July 2005 London bombings but also in some respects to the UN Security Council Resolution 1624 of 14 September 2005 and the Council of Europe Convention on the Prevention of Terrorism 2005, both of which are described later.

The principal offence in section 1(1) relates to the publication of statements that are “likely to be understood by some or all of the members of the public to whom it is published as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism” or specified offences which are referred to as “Convention offences”. As for the mens rea, in section 1(2)(b), the publisher must either intend members of the public to be directly or indirectly encouraged or otherwise induced by the statement to commit, prepare, or instigate acts of terrorism or specified offences, or be subjectively reckless as to whether members of the public will be so directly or indirectly encouraged by the statement. The most controversial facet of the offence is “indirect” encouragement. By sub-section (3), the indirect encouragement of terrorism includes a statement that “glorifies” the commission or preparation of acts of terrorism or specified offences (either in their actual commission or in principle) but only if members of the public could reasonably be expected to infer that what is being glorified in the statement is being glorified as conduct that should be “emulated by them in existing circumstances”. “Glorify” is partly defined in section 20(2) as including “praise or celebration”. Having targeted the originators of statements in section 1, section 2(1) deals with secondary dissemination. The offence may be committed by a “terrorist publication” by electronic transmission, for example. It is a defence under section 2(9) to show that the statement neither expressed the publisher’s views nor had his endorsement. This defence can benefit “all legitimate librarians, academics and booksellers” (Baroness Scotland, 2005a) (and broadcasters and bloggers) who may have examined the article but do not endorse its contents. There were only 10 prosecutions up to 31 March 2013 (Home Office, 2013). As with section 58, challenges on human rights grounds were given short shrift by the Court of Appeal in Iqbal v R (2014, para. 41):

The right to freedom of expression protected by Article 10 is of course not an absolute right, but is a qualified right. Article 10(2) provides in its material parts, that this freedom is subject to such restrictions and penalties as are prescribed by law and are necessary in a democratic society in the interests of national security, public safety, for the prevention of disorder or crime and for the protection of the rights of others. All those interests are engaged by acts of terrorism which violate the fundamental rights of others... it is proportionate and legitimate to interfere with the right to freedom of expression in order to reduce, diminish or extinguish such acts.

A more pre-emptive approach than prosecution is set out in section 3, which seeks to apply these offences in the context of unlawfully terrorist-related articles or records on the internet and to devise a short-circuit enforcement power. In justifying this measure, it was claimed that “extremist” websites have proliferated (Home Office, 2009b, para. 5.14), and that communication technologies represent both an important terrorist target and logistical aid. Section 3(1) applies where the publication under
section 1 or the dissemination under section 2 was produced electronically. The impugned materials are those which are “unlawfully terrorism-related” under section 3(7). The short-circuit process under section 3 (3) arises where a constable forms the opinion that material held on the system of the service provider is “unlawfully terrorism-related”. A notice can be issued which requires the provider to arrange for the material to become unavailable to the public and also warns the provider that failure to comply with the notice within two working days under section 3 (2) and (9) will result in the matter being regarded as being endorsed with consequent potential liability under sub-section (4). Critics argued that these restrictions on freedom of expression should engage a judicial officer at some stage so that the value of rights could be considered more explicitly than in the likely calculations of a commercial service provider. The government retort was that judicial process would cause undue delay in a “fast moving world” (Baroness Scotland, 2005b), though the Home Office Guidance on Notices Issued under Section 3 of the Terrorism Act 2006 does seek to confine the initiation of notices to expert officers of the Metropolitan Police Service Counter-Terrorist Command.

By 15 January 2015, the removal of 72,000 web items (at an increasing rate per year) had been prompted (James Brokenshire, 2015), though how this figure relates to alerts is not revealed (House of Commons Home Affairs Committee, 2012, para. 53). The potential operation of section 3 is curtailed by the impact of the Electronic Cabinet Office, 2009s/31/EC, as implemented by the Electronic Commerce (European Communities Directive) Regulations 2002, SI 2002/2013. More importantly, section 3 is bypassed by responsive action by CSPs in response to informal police requests. Indeed, the Guidance suggests dialogue and that a “voluntary approach” should be taken where the provider is not viewed as encouraging publication (paras 20, 27, Annex C). In consequence, section 3 has never been formally invoked. The public are also invited to sound an alert about extremism and terrorism via a government website which feeds into the Counter Terrorism Internet Referral Unit (CTIRU), launched by the Association of Chief Police Officers (ACPO) in 2010 (Blain, 2011; https://www.gov.uk/report-terrorism), to encourage “a civic challenge against material that [the public] find offensive, even if it is not illegal”.

The shortcomings of these warning systems were highlighted by the head of Government Communications Headquarters (GCHQ) and the UK Prime Minister in November 2014. The head of GCHQ, Robert Hannigan, stated that social media companies are “the command-and-control networks of choice for terrorists”, with some technology companies “in denial” about the internet’s misuse (Hannigan, 2014). Following added criticism by the Prime Minister (Wintour, 2014), several UK operators (BT, Virgin, Sky, and TalkTalk) agreed to install public reporting buttons to flag terrorist material on their services whilst Facebook, Google, Yahoo, and Twitter agreed to mentor smaller internet companies on standards of content monitoring.

It is more difficult to contend with overseas CSPs. No international system replicates these UK take-down measures elsewhere, despite the dangers recognized by the EU Framework Directive on Combating Terrorism, 2008/919/JHA, paragraph 4. As previously explained, most extremist content is hosted by US-based CSPs. Their receptivity to self-censorship is lower than for European-based companies, as highlighted by the Intelligence and Security Committee (ISC, 2014) Report on the intelligence relating to the murder of Fusilier Lee Rigby. One of the soldier’s killers, Michael Adebowale, had several of his multiple social media internet accounts (later revealed by the media to be operated through Facebook) closed proactively without official request by the CSP using an automated process because, according to GCHQ, “they hit triggers ... related to their criteria for closing things down on the basis of terrorist content” (para. 384). Facebook also learned, on completion of a retrospective review of all his 11 accounts (para. 390), that Adebowale had also discussed “in the most explicit and emotive manner” over Facebook’s instant messaging service his desire to murder a soldier (para. 384). The ISC was critical of monitoring procedures by CSPs (para. 389), though serial investigations by the Security
Service were excused as sufficiently thorough, especially because, as pointed out even by GCHQ (para. 393), true intent can be very difficult to discern from online communications. Putting aside other relevant issues around data privacy, accountability for surveillance, the duty of care to users, and the economic efficiency, were social media companies to be obliged to proactively monitor and share all postings of a violent extremist nature with security authorities, the former would have little time or money for anything else and the latter would be deluged with information and most likely rendered unable to function on an economic basis.

European online laws

The UN has achieved almost no impact in the field of online laws against violent online extremism, a position in part attributable to US and other Western reluctance to invite and sanctify restrictions by undemocratic states on freedom of expression on the web. However, the UN has occasionally called for specific action against online terrorism, such as via the UNSCR 2178 which has already been described. A similar call to action was issued through UNSCR 1624 of 14 September 2005, “Prohibition of incitement to commit terrorist acts”, calling upon states in Article 1(a) to “[p]rohibit by law incitement to commit a terrorist act or acts”. In the background, UNSCR 1535 of 26 March 2004 creates the Counter Terrorism Committee Executive Directorate (CTED), which can provide technical assistance to states. Another technical body, the UN Office on Drugs and Crime has produced a useful guidance (2012) in collaboration with the United Nations CounterTerrorism Implementation Task Force (CTITF) which has also produced its own guides and analysis (2009 and 2011).

Within Europe, the Organization for Security and Co-operation in Europe (OSCE) has additionally performed similar advisory and exhortatory roles. Its Sofia Ministerial Council decided in 2004 that participating States will exchange information on the use of the Internet for terrorist purposes and identify possible strategies to combat this threat, while ensuring respect for international human rights obligations and standards, including those concerning the rights to privacy and freedom of opinion and expression. (OSCE, 2004)

A follow-up decision from the OSCE’s Brussels Ministerial Council in 2006 invited participating states to “increase their monitoring of websites of terrorist/violent extremist organizations and their supporters and to invigorate their exchange of information” (OSCE, 2006). Since that time, numerous OSCE events have aired various policy views addressing internet controls, some of the latest being published in 2013 (OSCE, 2013), though no legal rules have been instituted as a result of this platform for discussion.

The legal innovations within Europe have emerged from the Council of Europe and the European Union. As for the Council of Europe, which has engaged in the issuance of guidance too (2008), the Convention on the Prevention of Terrorism 2005 (European Treaty Series 196) was mentioned earlier, and Article 5 called for action against “public provocation to commit a terrorist offence”, much of which took place online (see Barendt, 2009; Parker, 2007; Walker, 2011, chap. 8). Of still wider application is the (Budapest) Convention on Cybercrime 2001 and the Additional Protocol 2002 (European Treaty Series 185, 189). These international law measures take action on a broad front, but without any specific reference to terrorism. For example, the Protocol specifies various types of hate speech that should be prohibited on the internet, including racist and xenophobic materials, justification of genocide, and crimes against humanity. The documents are also wide in the sense that they can be ratified by non-European states that participated in its elaboration; included in this category is the US, which has ratified the former but not the latter on First Amendment grounds, a stance shared by the UK. The limited nature of these instruments has only been discussed once by the Cybercrime Convention Committee (T-CY), at its third Plenary in 2008, where it was concluded that it would be better to
concentrate on fuller state implementation of the 2001 and 2005 conventions before venturing with any further law-making.

As regards the EU, terrorist uses of the internet and the risks posed by them have not been the subject of serious attention by its policymakers until quite recently because it is viewed as a relatively new issue and because the gestation of EU policy occurs at a glacial pace (Argomaniz, 2014, p. 5). Amongst the measures which have emerged, the most concrete in legal terms is Council Framework Decision 2008/919/JHA of 28 November 2008, amending Framework Decision 2002/475/JHA on combating terrorism, which requires state action to criminalize incitement of terrorism via the internet, including “public provocation to commit a terrorist offence”, as well as the use of the internet for recruitment for terrorism and training for terrorism. Though the UK had passed such legislation in 2006, in response to overlapping UN demands, some other EU member state countries were thus prompted to take action (Galli & Weyembergh, 2012). Other initiatives undertaken by the EU include “Check the Web”, which was launched in 2007 and allows states to pool data on terrorist propaganda and internet chatter at the European Police Office (Europol) (Article 36 Committee, 2007). The EU Commission also funded a project titled CleanIT (http://cleanitproject.eu/) to initiate “a structured public–private dialogue between government representatives, academics, Internet industry, Internet users and non-governmental organisations in the European Union” on “Reducing terrorist use of the Internet”. Its final product was a report on conditions for action, plus best practices (2013). It has been argued that the real value of the CleanIT project resided in the fact that “it has turned the spotlight on a wider problem: the [European] Commission’s reliance on industry solutions to address problems that are badly defined by policymakers from the very beginning” (Argomaniz, 2014, p. 11).

“Positive” online measures

Generally less contentious are “positive” online counter-terrorism measures that employ online engagement and outreach rather than content controls to stem the encouragement of violence. There are few hard laws in this area, but the UK’s Counter Terrorism and Security Act 2015, section 26, does impose a legal duty to “have due regard to the need to prevent people from being drawn into terrorism”. The extent to which this duty will require official online activity remains to be determined by ministerial guidance, though it might be predicted that most requirements will be negative rather than positive – such as requirements for educational establishments to warn students and even to filter out materials.

Existing positive campaigns have tended to focus upon social media which target youth, since they are believed to be particularly vulnerable to violent online political extremist rhetoric. This work is often undertaken by non-governmental organizations and individual activists, including young people themselves; although some such campaigns have also been undertaken by state agencies.

Within the realm of state interventions, shortly after 11 September 2001, the UK domestic Security Service (MI5) took the unprecedented step of posting an appeal for information about potential terrorists on dissident Arab websites (Conway, 2007b). The message, in Arabic, was placed on sites that the authorities knew were accessed by extremists, including Islah.org, a Saudi Arabian opposition site, and Qoqaz.com, a Chechen site that advocated jihad. MI5 were hopeful of eliciting information from persons on the margins of extremist groups or communities who were sufficiently shocked by the events of 11 September 2001 to want to contact the agency. The agency had intended to post the message on a further 15 sites known to be accessed by radicals, but many of these were shut down by
the FBI in the aftermath of the attacks. The security agencies continue not only to monitor traffic but also to intervene actively in extremist blogs and forums. The FBI has been especially aggressive in its use of enticement tactics, often beginning with internet-based contacts (Human Rights Watch and Columbia Law School, 2014; Laguardia, 2013; Sherman, 2008–2009; Stevenson, 2008).

More open and positive institutional interventions have also been revealed. In 2007, the UK Home Office established the Research Information and Communications Unit (RICU) as a cross-departmental strategic communications body based at its Office for Security and Counter-terrorism; RICU seeks to coordinate government communication activities to counter violent extremism while promoting inter-community relations (see https://www.counterextremism.org/download_file/106/134/413/). The government has also proposed to establish in 2015 the 77th Brigade within the British Army, dubbed “Facebook warriors” by one newspaper:

77th Brigade is being created to draw together a host of existing and developing capabilities essential to meet the challenges of modern conflict and warfare. It recognises that the actions of others in a modern battlefield can be affected in ways that are not necessarily violent. (MacAskill, 2015)


Another “positive” government agency initiative is the US State Department’s Center for Strategic Counterterrorism Communications’ (CSCC) “Think Again Turn Away” social media campaign. The CSCC was established in 2010, to coordinate, orient, and inform government-wide foreign communications activities targeted against terrorism and violent extremism, particularly al-Qaeda, and its affiliates and adherents... The Digital Outreach Team actively and openly engages in Arabic, Urdu, Punjabi, and Somali to counter terrorist propaganda and misinformation about the United States across a wide variety of interactive digital environments that had previously been ceded to extremists. (http://www.state.gov/r/csccl)

The CSCC is both praised and vilified for “Think Again Turn Away”, an English language social media campaign that commenced in 2013, whose mission is described on its Facebook page as “to expose the facts about terrorists and their propaganda”. In addition to its Facebook presence, the campaign is also active on Ask.fm, Google+, Tumblr, Twitter, and YouTube, where it disseminates content that addresses the same grievances as those in extremist content, including in some instances creating “mash-ups” of IS content and recirculating it. Some commentators have viewed the CSCC’s online activity as “embarrassing” and “ineffective” (Katz, 2014).

In 2012, the EU established its Radicalisation Awareness Network (RAN) under Directorate General Home Affairs to dissuade people from participating in violent extremism and terrorism or to persuade them to separate themselves from such ideas and methods in the first place (http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/index_en.htm). The RAN is composed of eight working groups, one of which, RAN@, is tasked with “develop[ing] frontline partnerships around the collation, creation, and dissemination of counter-[violent extremist] and alternative-narratives through the Internet and social media”. Other RAN working groups have also discussed using the internet to reach out to publics; RAN Voices of Victims of Terrorism, for example, seeks to have the voices of terrorism victims amplified via the internet and social media.

Finally, private actors have challenged violent jihadism online. Some are heavily backed by government, such as the Quilliam Foundation (http://www.quilliamfoundation.org), but others have been initiated by individuals and non-governmental organizations. Their denunciations or alternative interpretations
have taken many different forms, ranging from online video and other online responses denouncing violent extremism by scholars and imams to wide-ranging multimedia campaigns such as “My Jihad” (http://myjihad.org/), from ordinary individuals uploading videos to YouTube to more general macro-level positive messaging about Islam targeted at children and youth such as Naif alMutawa’s comic and animated series, “The 99” (http://www.the99.org/). A particularly interesting example is Abdullah-X, a series of online animated shorts developed by a former extremist, which received support from RAN@ and Google (https://www.youtube.com/user/abdullahx). The developer’s status as a former extremist probably lends the project greater credibility than some of those described earlier, and the site may be more accessible and appealing to youth than most state-sponsored campaigns. The range of private action has extended into more negative attacks and forms of vigilantism. In this category are Internet Haganah (Weimann, 2006, p. 199) and Anonymous, which in 2015 launched “Op Charlie Hebdo” with the purpose of disabling jihadi forums and social media accounts. Such attack strategies have been criticized by those who argue that violent extremist online forums and other violent extremist cyberspaces can serve as valuable providers of open source intelligence for states’ intelligence agencies (Lasker, 2005; McCants, 2011; Torres Soriano, 2012; Zelin, 2013).

Conclusion

Given that the internet is part of the infrastructure of contemporary everyday life in the same way as supermarkets and motorways, it is misguided to place responsibility on the internet for the aberrant terrorist usage of a small minority or to require that CSPs should treat everyone as an equal risk and potential suspect. In response to criticisms of failures by MI5 in averting the murder of Lee Rigby in Woolwich by Adebolajo and Adebowale, the government expressed itself “confident that MI5 prioritises available resources and deploys them proportionately to the level of risk represented and as necessary to satisfactorily mitigate the risk, based on the information known at the time” (Cabinet Office, 2015, p. 7). Yet it seems, by contrast, that CSPs are expected to perform to a higher duty of care with no margin for error or discretion: “Communications Services Providers (CSPs) have a responsibility to ensure their networks are not used to plot terrorist attacks” (p. 5). A more realistic understanding is that even with extensive criminal offences, intrusion into free speech activities, and the running of new bureaucracies and programmes of funding, one can feel assured that not all terrorism will be averted and that it is unrealistic to expect the CSPs to act as better all-seeing and all-doing state agents than the security agencies themselves. More generally, the acculturalization of immigrant communities in Western values and lifestyles will prove very difficult owing to the perceived shallowness of those lifestyles and the hypocrisy in the official adherence to proclaimed values. It is also difficult to compete in the marketplace of ideas against the narratives of jihadism which speak in simplistic, hedonistic, and graphic language not available to official spokespersons. As a result, the dismal prospect is that, no matter how much the state strives to counter international terrorism or demands that the internet becomes perfectly self-policing, current emanations of violent extremism will take generations to assuage.

Disclosure statement

No potential conflict of interest was reported by the authors.
References

32 County Sovereignty Committee v Department of State. (2002). 292 F 3d 797 (USCA, DC).


*Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others*. (2014, April 8). European Court of Justice.


Martin v R. (1848). 3 *Cox’s Criminal Cases* 318.


*R v Morrison.* [2009]. Northern Ireland Court of Appeal 1.


*R v Sullivan and Pigott.* (1868). 11 Cox’s Criminal Cases 44.


