©2015, Elsevier. Licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International http://creativecommons.org/about/downloads

Offending and being offended online: vile messages, jokes and the law

Lisa Collingwood (Kingston University)

Graeme Broadbent (Kingston University)

Abstract

The volume of internet traffic on social media grows exponentially. Exploring this phenomenon from a behavioural perspective, it is evident that the law can only play a marginal role in its regulation. The gap between no regulation and the reach of the criminal law is significant, made higher following the publication of guidance from the Director of Public Prosecutions on prosecuting social media cases. Additionally, the civil law is incapable of filling this gap in part due to the need for individual action and the impetus required to pursue it. Whilst recognising that the law will inevitably continue to play a marginal role in the regulation of social media, it is argued that the creation of a new tort enforced by a suitable body might go at least some way to deal with inappropriate postings falling short of the criminal law standard but justifying some legal intervention.

Keywords:

Social media, oversharing, legal liability, regulation, guidelines, reform

Introduction

Online abuse or abusive behaviour involving social media can take a variety of forms[1]. It is a growing phenomenon that has become punctuated by an increase in charges and convictions brought against users of social media[2]. This article focuses on two particular aspects of online abuse : the publication of menacing communications[3] and those that, although of a trivial nature, infringe privacy. It does so in order to explore the development of these types of online abuse, highlighting the ease with which communicators may cause harm and the avenues of legal redress (both criminal and civil) that are potentially available to victims of

[1] There are several forms of online abuse, the criminal sanction of which is recognised in guidelines provided by the UK's Director of Public Prosecutions. These have been updated and are currently available at http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/index.html#content (last accessed 2 April 2015).

[2] "Careless Whispers: How speech is policed by outdated communications legislation" Big Brother Watch report, February 2015, 5, available at http://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/02/Careless-Whisper.pdf (last accessed 2 April 2015).

[3] Captured under s 127 Communications Act 2003.

unsavoury communications[4]. In so doing, the authors explore the utility of the legal environment in this context arguing that there ought to be a review of how social media law operates. The article therefore begins by applying behavioural analysis in order to develop an overview of the reasons why individuals choose to communicate online before exploring the consequences of this oversharing[5] in terms of the ensuing online abuse. To this end, the article highlights the mismatch between the way in which people behave online and the law regulating that behaviour. The argument is made that, in the absence of clearly defined indicators, the law as currently developed is, and will remain, ill-judged, ineffective and confusing. Following this, some ideas for improvement are put forward.

Overview

Why do people communicate so extensively online?

According to a recent report from the House of Lords Select Committee on Communications, 1.2 billion people regularly use Facebook, 34 million of them in the UK; 255 million regularly use Twitter, 15 million of them in the UK[6]. It is, therefore, unsurprising that hardly a week goes by without media reports of some controversy generated by postings on Twitter, Facebook or other social media or blogs. This may not necessarily be a new phenomenon: as Solove has commented, "from the dawn of time, people have … shamed others" [7]. On the internet, however, these social practices and their consequences have taken on new dimensions.

Nonetheless, individuals continue to communicate images, thoughts and personal information about themselves and others online. This begs the question of why users of social media appear to be naïve about the repercussions of their online footprints and hence fail to appreciate the potential liability to which they expose themselves. Five principal explanations for this may be identified. The first involves a lack of informed knowledge. Jarvis argues that individuals may be agreeable to revealing information online because they do not know what

[4] In this piece, "unsavoury communications", "unwise communications", and "undesirable behaviours" and are synonymous with "online abuse".
[5] By "oversharing", we mean the habit, particularly among young people, of sharing, online, details of their everyday life : See J. Palfrey and U. Gasser, "Born Digital: Understanding the First Generation of Digital Natives" (Basic Books, 2008), at page 26.
[6] House of Lords Select Committee on Communications 1st Report of Session 2014-15, *Social media and criminal offences*, HL paper 37, TSO 2014, at p.7.
[7] D. Solove, *The Future of Reputation: Gossip, Rumor and Privacy on the Internet* (Yale University Press, 2007) at p.11.

it adds up to[8]. It is questionable, for example, how many people know about or have ever read the Information Commissioners' recommendations regarding safe sharing practices[9] or are familiar with the myriad of regulations that might apply to their online footprints or even think about the consequences of their postings[10]. Such individuals are, therefore, lacking in crucial knowledge relating to the consequences they may expose themselves to, both at criminal and civil law, to say nothing of the potential that they themselves may become victims of unlawful behaviour online. Given the increased affordability, capacity and usage of digital and mobile technology, teenagers, for example, regularly communicate online. In particular, teenage users of Social Networking Sites (SNSs) have been identified as being unaware or ignorant of the public nature of the content they share online[11]. The decision to post a communication might not, therefore, always be a truly educated one and it is this that has allowed some users to adopt an almost wild abandon when circulating material on the internet.

A second reason lies in the fulfilment of online goals, in that people may choose to communicate online as a direct consequence of the fact that internet usage offers advantages and gratifications that appear to increase in direct proportion to the degree of self-disclosure[12]. Accordingly, online communicators appear willing to reveal their innermost selves to fulfil these online goals, fully reaping the benefits that technological tools have made possible[13]. In this way, information is effectively "exchanged as currency"[14] being readily traded in exchange for the latest technological service. This proposition is reinforced by the observation that many of the core features of communicating via SNSs, for example, are explicitly designed to facilitate the formation and maintenance of connections amongst users – connections that are sustained through communication about the self[15].

---

[8] J. Jarvis, *Public Parts : How sharing in the digital age improves the way we work and live* (Simon and Schuster, 2011) at p.100.

[9] Information Commissioner's Office, *Personal information online code of practice*, 2010. Available at https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf (last accessed 2 April 2015).

[10] See below.

[11] N. Ellison et al, 'Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment' in S. Trepte and L. Reinecke (eds), *Privacy Online : Perspectives on Privacy and Self-Disclosure in the Social Web* (Springer, 2011) at p.23.

[12] B. Walther "Introduction to Privacy Online" in Trepte and Reinecke, op. cit., at p.7.

[13] N. Ellison et al, "Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment" in Trepte and Reinecke, op. cit., at p.20.

[14] Z. Papacharissi and P. Gigson "Fifteen Minutes of Privacy: Privacy, Sociality, and Publicity on Social Network Sites" in Trepte and Reinecke, op. cit., at p.84.

[15] Ellison et al, op. cit., at p.21.

Thirdly, some of the attraction of online communicating is afforded by a perceived promise of "psychological privacy"[16]; that is, the sense of empowerment associated with feelings of choice created by managing the quantity and quality of personal information that is shared with other users. For example, communications to SNSs, since they are, at least initially[17], restricted to a distinct group of the general public, allow users to make decisions about whom to connect with as "friends"[18]. A high level of psychological privacy therefore exists online since, in controlling audiences through the selection of online "friends", users decide with whom to share their private information. The psychological privacy afforded by online communication channels makes users more amenable to trading their private information[19].

Fourthly, the motivation for users to post frequently is driven by the informal character and user-friendliness of online social networking, which positively encourages users to communicate private information, both voluntarily and regularly [20]. This, coupled with the socially active nature of people and their "natural … desire to connect with others"[21] makes users less discriminating when divulging personal information online. The sense of intimacy created by being among digital "friends" may often lead to an over-sharing of information[22]. Accordingly, online communicators may not weigh up the risks of being sued by others, but, as the recent case involving Lord McAlpine has shown, this is unsafe territory[23].

[16] S. Trepte and L. Reinecke, 'The Social Web as a Shelter for Privacy and Authentic Living' in Trepte and Reinecke, op. cit., at p.65.
[17] Whilst "friends" represent a communicators' intended public, this does not mean that the actual public are prevented from receiving the communication should it subsequently be forwarded. See D. Boyd "Social network sites as Networked Publics: Affordances, Dynamics and Implications", in Z. Papacharissi (ed), *A Networked Self* (Routledge, 2011) at p.44.
[18] Ellison et al, op. cit., at p. 22.
[19] This may be especially so when people are intoxicated. See "John Grisham: sentences too harsh for viewing child abuse images", *The Guardian*, 16 October 2014, available at http://www.theguardian.com/books/2014/oct/16/john-grisham-prison-sentences-child-abuse-images (last accessed 2 April 2015).
[20] B. Debatin "Ethics, Privacy and Self-Restraint in Social Networking", in Trepte and Reinecke, op. cit., at p.54.
[21] G. Hogben, "Security Issues and Recommendations for Online Social Networks", The European Network and Information Security Agency (ENISA), Position Paper No. 1(2007), at p.3. Available at www.ifap.ru/library/book227.pdf (last accessed 2 April 2015).
[22] Ibid.
[23] *Lord McAlpine v Bercow* [2013] EWHC 1342 (QB).

Similarly, empirical findings suggest that individuals are highly motivated to use SNSs for presenting themselves[24]. This may also be driven by a misplaced presumption that online behaviour is private and therefore users do not anticipate that information will be seen by countless others[25]. In other words, perceptions of private space online may be flawed[26]. This standpoint is further entrenched because of the ease by which online communicators are able to achieve anonymity online. Anonymity has, of itself, become an integral feature of cyber culture, with online participants relying on their anonymity as "a disinhibiting factor affecting what people are prepared to say in this special environment"[27]. Accordingly, anonymity may be credited with being one of the driving forces behind the popularity of SNSs and, because anonymity provides an opportunity for individuals to participate in society without being identified, and, therefore, without needing to be accountable[28], it provides a means by which individuals can more easily violate the privacy of others[29].

It is contentious to suggest that users are unaware of the risks associated with social media. Young and Quan-Haase, for example, observe that "Users, however, are not necessarily naıve in their disclosure practices… users are actively engaged in guarding their data and are not passive..."[30]. Similarly, Palfrey and Gasser suggest that the younger generation of "digital natives" are becoming increasingly aware of the threats associated with the use of modern information technologies and adjust their behaviour accordingly, such that "the habit among young people of sharing many of the details of their everyday life … is neither random nor uncontrolled. They are … more conscious of what they are doing than they are perceived to be"[31]. However, the authors also acknowledge that "rarely do they have in view the full impact of their decision to disclose…"[32] Therefore, it is reasonable to suggest that the facility for communication afforded by modern technology, particularly the ease with which

[24] N. Kramer and N. Hakerkamp "Online Self-Presentation: Balancing Privacy Concerns and Impression Construction on Social Networking Sites", in Trepte and Reinecke, op. cit., at p.127.
[25] B. Walther, op. cit., n.12 at p.3.
[26] L. Edwards "Privacy and Data Protection Online: The Laws Don't Work" in L. Edwards and C. Waelde (eds), *Law and the Internet* (3rd ed., Hart Publishing, 2009), at p. 484.
[27] Per Mackay J., *Smith v ADVFN Plc* [2008] EWHC 1797 (QB), at para. [15].
[28] K. Oqvist *Virtual Shadows* (British Computer Society 2009), at p.56. See also K. Hughes, "No Reasonable Expectation of Anonymity" (2010) 2(2) *JML*169, at p.181 and E. Barendt "Bad news for bloggers" (2009) 1(2) *JML* 141, at p.144.
[29] Solove, op. cit., n.7, at pp.140-142.
[30] A. Young and A Quan-Haase, "Privacy Protection Strategies On Facebook", *Information, Communication & Society*, 16:4, 2013, 479-500, 480. See also B. Debatin, J. Lovejoy, A.Horn and B. Hughes, "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences", *Journal of Computer-Mediated Communication*, Volume 15, Issue 1, pages 83–108, October 2009.
[31] J. Palfrey and U. Gasser, op. cit., at page 26-7.
[32] Ibid, page 36.

communications may be sent and the possibilities for wide – even world wide – dissemination carry with them dangers for the unwary and unwise in choosing not only what they communicate but how they do so.

In practice, therefore, we effectively live in a world of information overload. However, whilst much of what is posted is trivial information created to encourage the nurturing of online relationships, it is very easy to publish material that could lead to online abuse. It appears that an increasing number of transgressions are being carried out using this medium[33]. Nonetheless, whilst the law may penalise people if they send ill-advised messages, with perpetrators possibly facing court proceedings over their online behaviour, people send them regardless and in great number, in part due to the ease with which the internet and social media facilitate communications.

Consequently, the law appears marginal and this begs two principal questions, which are addressed below, namely:-

i. How far are the contours, customs and practices associated with online transgressions understood by those responsible for formulating law so as to make legal measures effective? and
ii. How might improvements in the protections afforded at law be developed going forward?

These questions are considered below by looking firstly at the reach of criminal sanction following the publication of a menacing communication and secondly at civil law remedies following a communication that violates privacy.

[33] The Big Brother report, op. cit., n.2, p. 10 suggests that between 1st November 2010-1st November 2013, there was an increase of 217% in the number of cases heard under Section 127 of the Communications Act 2003 and Section 1 of the Malicious Communications Act 1988 (the related offence of sending letters etc. with intent to cause distress or anxiety, which also applies to electronic communications) involving social media users . See also Geach N and Haralambous N, 'Regulating Harassment : Is the Law Fit for the Social Netwoking Age?' (2009) 73(3) *The Journal of Criminal Law* 241.

Liability in law

Criminal Law

The Big Brother report suggests that "the social media revolution has changed the way people communicate with each other. Yet, whilst our communications have evolved the way crimes are dealt with has not … we find ourselves using archaic legislation to police modern day crimes.… the laws that regulate what is said on social media … are woefully out of date"[34]. It is indeed the case that this arm of law was almost entirely enacted before the intervention of social media and is therefore arguably actually inappropriate for the prosecution of offences committed using social media.

Not all commentators agree that the criminal law is out of pace with technological development. A recent report from the House of Lords Select Committee suggests that the criminal law is "generally" apposite[35]. Yet, despite figures suggesting that over 14,000 alleged crimes specifically linked to social media and reported to police in 2011[36], a total of only 653 people faced criminal charges in England and Wales in 2012 in connection with comments on Twitter or Facebook[37]. The consequence is that there is every chance that offences which deserve to be prosecuted will not be, due simply to the volume of online traffic[38]. Moreover, there are several clear examples that both communicators and prosecutors appear not to have understood the parameters necessitating punishment by the State, meaning that the appropriateness of the application of the criminal law may be challenged.

This is not least because there are significant differences between the written and spoken word. Although the written word has the merit of certainty as to what the actual words used were, it is difficult to discern matters such as tone or emphasis, which are immediately apparent when spoken. This has a particular resonance with regard to *Chambers v DPP*[39], which is discussed at length as it raises a number of pertinent issues. Chambers was due to fly to Belfast from Doncaster Robin Hood Airport to meet a friend. Robin Hood Airport was,

[34] Op. cit., n.2, p. 5.
[35] House of Lords Select Committee on Communications, op. cit., n.6, at p.6.
[36] K. Dowling and J. Harlow, "Tweet this. Is it time to tame Twitter?" *The Sunday Times*, 5th August 2012.
[37] B. Wheeler, "Twitter users: A guide to the law", BBC News, 26 February 2013, available at http://www.bbc.co.uk/news/magazine-20782257 (last accessed 2 April 2015).
[38] House of Lords Select Committee on Communications, op. cit., n.6, at p.20.
[39] [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833. For comment, see R. Griffiths "Social media and the criminal law" (2013) 24 Ent. L.R. 57.

however, closed due to bad weather. He posted this message on Twitter: "Crap! Robin Hood Airport is closed. You've got a week and a bit to get your shit together otherwise I am blowing the airport sky high!" Chambers was subsequently arrested on suspicion of involvement in a bomb hoax. When interviewed by the police, he insisted throughout that the tweet was meant as a joke. He was charged under s.127 of the Communications Act 2003 of sending, by means of a public electronic communications network, a message of a menacing character.

Despite his protestations that the tweet was intended as a joke and was not of a "menacing character" as required by the Act, he was convicted by the magistrates and unsuccessfully appealed to the Crown Court. A further appeal to the Divisional Court of the Queen's Bench Division by way of case stated was, however, successful. Giving the judgment of the court, Lord Judge CJ noted that there was no evidence that any of Chambers' Twitter followers, of whom there were some 600, who might have read the tweet found it to be of a menacing character[40]. It was, however, taken seriously by airport staff and, crucially, by the police. On the possible restriction on free speech brought about by s.127, he observed[41]:

"Satirical, or iconoclastic, or rude comment, the expression of unpopular or unfashionable opinion about serious or trivial matters, banter or humour, even if distasteful to some or painful to those subjected to it should and no doubt will continue at their customary level, quite undiminished by this legislation ….. Shakespeare can be quoted unbowdlerised, and with Edgar, the end of King Lear, they are free to speak not what they ought to say but what they feel."

On the meaning of "menacing", he observed that help could not be derived from legislation relating to threats in other contexts. He went on to say[42]:

"….a message which cannot or is unlikely to be implemented may nevertheless create a sense of apprehension or fear in the person who receives or reads it. However, unless it does so, it is difficult to see how it can sensibly be described as a message of a menacing character.

[40] There was an issue raised on appeal as to whether Twitter fell within the definition of a "public electronic communications network" as required by s.127. The Crown Court and the Divisional Court both took the view that it was as it was accessible to all internet users.
[41] At para. 28. Compare the remarks of Lord Reid in *Brutus v Cozens* [1973] AC 854 at p.862 and Viscount Dilhorne at p.865.
[42] At para. 30.

So, if a person or persons who receive or read it, or may reasonably be expected to receive, or read it, would brush it aside as a silly joke, or a joke in bad taste, or empty bombastic or ridiculous banter, then it would be a contradiction in terms to describe it as a message of a menacing character. In short, a message which does not create fear or apprehension in those to whom it is communicated, or who may reasonably be expected to see it, falls outside this provision, for the very simple reason that the message lacks menace."

He pointed out that the meaning of a message had to be considered in both its context and with reference to the means by which the message was sent. He noted that the Crown Court had been concerned that it was sent at a time of public concern about the threat of terrorism. Even when examined in context, however, it did not, he thought, constitute a threat. It had been posted on Twitter for general reading and was not directed to any staff at the airport. He was of the view that the language and punctuation were inconsistent with it being a threat and that, in any event, it was unusual in a terrorist threat for the writer to be readily identified. The reaction of readers was also relevant. There was no reaction from readers at large and the airport staff did not take it seriously. The fact that the airport staff reported it was more a matter of procedure than alarm. Only when South Yorkshire Police became involved did the matter escalate and, even then, there was a lack of urgency in their response.

The approach of the Divisional Court is surely correct in insisting that the words used must be examined, not in isolation, but with reference to their context and the medium through which the message containing them is promulgated. What it does not do, and cannot do, is to provide a guide as to the interpretation of any given message. This remains a matter for individual judgement on the part of those reading the message.

The root of the problem in *Chambers* was the way in which his tweet was interpreted and the consequent decisions that were taken in respect of it. In the initial task of interpretation, the Lord Chief Justice urged the adoption of common sense. It is undoubtedly difficult, in some instances, to distinguish between the genuine threat and the attempt at humour in the written word. This is an exercise, though, that a range of organisations and individuals have to undertake on a daily basis, not least of whom are the security services. There are historical precedents for large scale issues of this kind. By way of example, the original prohibition on

sending indecent or obscene material through the post[43] was to protect post office officials from exposure to such items[44]. In the 1970s, a spate of bomb hoaxes caused not only legislation[45] to attempt to deal with the phenomenon but also required the exercise of judgement on the part of the police, and those in places such as schools and public buildings, as to which were genuine threats and which were hoaxes that could safely be ignored. Major differences between then and now are, however, significant. The majority of the bomb threats or hoaxes in the 1970s were made by telephone. Telephone calls are targeted individual communications addressed to a particular person or to a representative of an organisation, while messages posted on social media are at large across the network and may be accessed by users, whether known personally to the poster or not and whether the target of the poster or not. The nature of the caller helped to filter the serious threat from the hoax. An Irish accent[46] might suggest that the threat ought to be taken seriously, at least initially; giggling schoolchildren could safely be ignored. In prose, without those sorts of indicators (which are not, of course, conclusive) that distinction is much more difficult to draw. Tone is particularly difficult to convey unless the writer is skilled, although the choice of words and punctuation may be indicative of that person's intention, as *Chambers* illustrates.

For these reasons, in *Chambers*, the Lord Chief Justice was of the view[47] that the tweet was of a trivial nature and was inconsistent with a credible threat. He was fortified in this conclusion by three other factors. First, the words were posted on Twitter, where they could be read by anyone[48]. Secondly, that it was unusual for a terrorist threat to enable the writer to be readily identified. Thirdly, that it would be difficult to imagine a serious threat that was accessible by a large number of people in plenty of time to enable the action threatened to be prevented. It is at this point, it is suggested, that the Divisional Court veered off into dangerous territory, for this passage contains assumptions about the way people behave. These assumptions may be grounded in experience but stray from the central issue of the meaning and import of the words actually used. Suppose a clever terrorist who decides to engage in a form of double bluff by using social media (having of course taken steps to

[43] S.4 Post Office (Protection) Act 1884.
[44] C. Manchester, "Obscenity in the mail" [1983] *Criminal Law Review* 64-77, at p.65
[45] S.51 Criminal Law Act 1977 created a series of criminal offences to deal with this phenomenon.
[46] This was in a period in which the disputes over Northern Ireland were particularly intense with quasi-military groups engaging in all manner of disruptive activity, of which planting bombs was just one extreme example.
[47] At para. 31.
[48] It might be observed that Chambers could have saved himself a lot of bother if he had simply sent a text message rather than posting on Twitter.

ensure anonymity, though this may not matter if he is a suicide bomber) and imitating the language of the faux outraged would-be traveller. It is surely much safer to rely on actualities in order to determine the meaning and import of words than to stray outside this approach and rest on assumptions, however well intentioned, even as secondary fortification for a conclusion that has been arrived at by examination of concrete evidence.

The Divisional Court did not need to go beyond its interpretation of the words used by Chambers to arrive at the conclusion that this was not a message of a menacing character as required by s.127 of the Communications Act 2003 given the medium and the way the message was expressed. It is unfortunate that it did so, as it may offer an invitation to courts, police and prosecutors in the future to use such assumptions in their analysis of communications: what constitutes common sense is not universally agreed.

Moreover, courts and prosecutors alike need to be able to grasp contemporary discourse styles, irony, banter or jokes as well as the context in which a communication has been made so as to avoid police, prosecutors or courts being overwhelmed with millions of trolling-type cases. There is already some evidence of this. In June 2014, it was reported that social media crimes now make up "at least half" of the calls that British police receive every day[49] and figures suggest that, last year, 10,535 people in England and Wales were prosecuted for stalking and harassment, compared to 8,648 people in 2012/13[50]. However, there is no breakdown detailing offences committed online as against those using traditional means of communication. Whilst anecdotal evidence exists as to the scale of the problem, there are relatively few facts. Better statistics would help to inform the debate as to the appropriateness of the criminal law in relation to online transgressions[51].

There is self-evidently a role for the criminal law to play in relation to social media and other forms of electronic communication to distinguish between malice and joviality. This enables those posting tweets, such as Peter Nunn, who recently sent messages[52] threatening to sexually assault MP Stella Creasy, to face due sanction. His justification for the messages he sent was that they were "… just a joke. It came into my mind and I thought it was really,

[49] BBC News, 24 June 2014, available at http://www.bbc.co.uk/news/uk-27949674 (last accessed 2 April 2015).
[50] BBC news, 11 September 2014, available at http://www.theguardian.com/law/2014/sep/11/stalking-prosecutions-rise-new-law-cps-acpo-victim-support (last accessed 2 April 2015).
[51] House of Lords Select Committee on Communications, op. cit., n.6 at pp.9, 19.
[52] Including : "If you can't threaten to rape a celebrity, what is the point in having them?".

really funny"[53]. Unlike Chambers, Nunn's messages were targeted at specific individuals and did not lack malice. He was found guilty under Section 127 Communications Act 2003. In a similar vein, criminal prosecution may well arise following the catalogue of vile internet abuse targeting the family of the missing child Madeleine McCann[54].

The *Chambers* case provoked considerable media attention, as well as wider discussion, not least on Twitter itself. A particular strand in the discussion was the question of whether the prosecution should have been brought in the first place. The Director of Public Prosecutions has subsequently issued new guidance on prosecutions involving social media[55]. These identify four particular categories which could potentially invoke the criminal law: credible threats (the issue in *Chambers*); communications which specifically target an individual or individuals and fall within the Protection from Harassment Act 1997; communications in breach of a court order; and communications not within the previous categories but which may be considered grossly offensive, indecent, obscene or false and potentially falling within s.1 Malicious Communications Act 1988 or s.127 Communications Act 2003. The guidance requires that cases falling within the first three categories should be "prosecuted robustly"[56] as long as they also satisfy the general test (i.e. that there is sufficient evidence to provide a realistic prospect of conviction and that the prosecution is in the public interest[57]). Those in the fourth category, however, are to be subjected to a "high threshold"[58] at the evidential stage. The guidance recognises that the law and the way it is used may conflict with the right to free speech in Article 10 of the European Convention on Human Rights. It therefore advises that the discretion to prosecute should be exercised carefully and be based on an interpretation of the relevant legal provisions to ensure that complies with Article 10;[59] so, for

[53] "Troll Peter Nunn guilty of MP Stella Creasy rape tweets", BBC News, 2 September 2014. Available at http://www.bbc.co.uk/news/uk-england-london-29034943 (last accessed 2 April 2015).
[54] It was reported that Metropolitan Police Officers were in talks with the Crown Prosecution Service after being handed a dossier of more than 80 pages of Tweets, Facebook posts and messages on online forums aimed at Kate and Gerry McCann. See "'Evil' Trolls In Hate Campaign Against McCanns", Sky news 2 October 2014, available at http://news.sky.com/story/1345871/evil-trolls-in-hate-campaign-against-mccanns (last accessed 2 April 2015). Subsequently, one of the identified trolls, Brenda Leyland, tragically committed suicide.
[55] These have been updated and are currently available at http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/index.html#content (last accessed 2 April 2015).
[56] Ibid, para 13.
[57] This is contained in the Code for Crown Prosecutors, available at http://www.cps.gov.uk/publications/code_for_crown_prosecutors/ (last accessed 2 April 2015).
[58] Op. cit., n. 55, at para. 13.
[59] See, for example, *Sunday Times v UK (No 2)* [1992] 14 EHRR 123: "Freedom of expression constitutes one of the essential foundations of a democratic society ... it is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also as to those that offend,

example, prosecutors are reminded that s.1 of the Malicious Communications Act 1988 requires that an item is *grossly* offensive, not simply offensive. Further, in many cases, the guidance continues, a prosecution in such a case is unlikely to be in the public interest unless this is a necessary and proportionate response[60]. The guidance further cautions that use of the offences contained in Part I of the Public Order Act 1986[61] for social media cases may not be appropriate, as that Act is primarily concerned with words spoken or displayed in the presence of others[62]. Further, there is an exception where the words are spoken or displayed by a person within a dwelling where the potential victim is inside that or another dwelling[63] which is inappropriate in the context of social media.

The guidelines are primarily intended for the Crown Prosecution Service. This is not, however, the only stage of criminal proceedings at which discretion is exercised and they will undoubtedly influence police practice. This is important for, as *Chambers* illustrates, the initial decision taken by the police can either bring incidents within the criminal process or filter them out.

At what point the criminal law should be engaged is, therefore, open to legitimate debate, given an observed failure of courts and law makers to fully grasp contemporary discourse styles. Whatever conduct on social media and other electronic communications legislators choose to penalise, any legislation should be appropriate to the (new) media. Whilst there may be a desire to penalise communications in the same way through whatever medium it occurs, whether real or virtual, this may not always be appropriate to the different types of harm caused. It is also significant that, where a person is convicted of a criminal offence, there is not only the sentence that goes with it but also possibly more far reaching consequences for employment, particularly impacting on those that are subject to criminal record checks by the Disclosure and Barring Service.

---

shock or disturb ..." See also the discussions in *Chambers*; *DPP v Collins* [2006] UKHL 40; [2006] 1 W.L.R. 2223; and *Connolly v DPP* [2007] EWHC 237 (Admin); [2008] 1 W.L.R. 276, noted in (2007) 71 J.C.L. 288.

[60] Op. cit., n. 55, at para. 43.

[61] Such as the offences of using threatening or abusive words or behaviour likely to cause harassment, alarm or distress contained in s.5. S.57(2) Crime and Courts Act 2013 removed the word "insulting" from s.5 which may have an impact on its usefulness in the present context in those cases to which it is applicable.

[62] The guidance refers to the people being targeted, but the ambit of s.5 is wider than this.

[63] For an offence under s.5, the relevant provision is s.5(2).

The effect of all this is that the consequences of criminal sanction are potentially vast, particularly following the DPP's guidelines and this may not be entirely welcome, particularly given that much of what is shared online is trivial, as detailed above. The current state of the law in this area, therefore, suggests that lawmakers have failed to fully appreciate some of the conventions associated with online communications media. Whether the civil law fares better is addressed below.

Civil Law

The above focused on the possible criminal law implications in sending menacing communications and the perceived inability of courts and, especially, prosecutors to accommodate contemporary discourse styles as well as to differentiate between the written and spoken word. Taking an online user to task is not, however, the exclusive domain of the criminal law. In addition to criminal law, civil law may be invoked to deal with certain aspects of online communications.

In respect of the civil law, online communicators may incur liability in relation to, inter alia, Data Protection, Intellectual Property and Defamation[64] legislation. Aggrieved individuals can rely on private law to bring actions under the Data Protection Act 1998 or for misuse of private information[65]. Since *Google Spain*[66], it may also be possible to have a search engine remove a link to such data[67].

However, the emphasis for this article is misuse of private information or, put simply, the liability that may arise following exposing or sending private information. In respect of this area of law, there is no statutory privacy legislation to call on. Whilst English law does not recognise a general right to privacy, there have been considerable developments in the area of privacy protection. Of most significance, with the passing of the Human Rights Act 1998, a general *right to respect* for private and family life under Article 8 is incorporated into English

[64] For example, Data Protection Act 1998, Digital Economy Act 2010, Defamation Act 2013. See, for example, *McAlpine v Bercow* [2013] EWHC 1342 (HC).
[65] *Contostavlos v Mendahun* [2012] EWHC 850 (QB) and *Contostavlos v News Group Newspapers* [2014] EWHC 1339.
[66] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] 3 WLR 659. The judgment does not, however, intend to protect individuals against all negative communications on the internet, but only against 'being pursued' for a long time by 'irrelevant', 'excessive' or 'unnecessarily defamatory' expressions.
[67] It is widely thought that the judgment does not give individuals an unfettered right to have their personal information deleted from search engine results. See "Peers say 'right to be forgotten' principle unreasonable", BBC News, 30 July 2014, available at http://www.bbc.co.uk/news/uk-politics-28551845 (last accessed 2 April 2015).

law. In addition to Article 8, however, Article 10 provides for an explicit right to freedom of expression to which the courts of this country must pay appropriate respect[68]. The significance of this is reinforced by s.12 of the Human Rights Act, which stresses the particular importance of freedom of expression when journalistic, literary or artistic material is involved[69]. In undertaking a rigorous balancing exercise of the competing rights to privacy and freedom of expression, domestic courts have developed a cause of action in "misuse of private information"[70]. Here, courts make a 2-stage assessment in consideration, firstly, of whether the claimant has a reasonable expectation of privacy in respect of the subject matter in question and secondly, whether the balancing of Articles 8 and 10 comes down in favour of protection of this privacy or in favour of publication of the information. When applied to online forums, in which, as suggested earlier, public and private boundaries have effectively become blurred and in which trivial information may tend to be posted, what should be included within the ambit of a reasonable expectation of privacy in relation to online communications remains open to debate.

Essentially, the biggest problem with civil actions in the context of online communications is arguably whether trivial information would ever be afforded a reasonable expectation of privacy. Defamation law is more developed in this regard and has differentiated "often uninhibited, casual and ill thought out"[71] "pub talk"[72] and "saloon-bar moanings"[73] from sufficiently "serious"[74] postings. However, in relation to proceedings for misuse of private information, the fate of the often trivial information that is posted online remains to be seen. In the *Applause Stores* case[75], in which a user was ordered to pay damages for misuse of private information and for libel following the creation by him of a false profile of the claimant on *Facebook*[76], the court determined that a person's date of birth would constitute information over which an individual would have a reasonable expectation of privacy. This

[68] Inter alia, *Weller v Associated Newspapers Limited* [2014] EWHC 1163 (QB), 2014 EMLR 24; *Murray (by his litigation friends) v Express Newspapers plc* [2008] EWCA Civ 446, [2009] Ch. 481; and *Douglas v Hello! Ltd (No.1)* [2001] QB 967 (CA).
[69] See, for example, *Cream Holdings v Banerjee* [2005] 1 AC 253.
[70] Post- *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22, [2004] 2 AC 457.
[71] Mackay J., *Smith v ADVFN Plc* [2008] EWHC 1797 (QB) at para. [14].
[72] Sharp J., *Clift v Clarke* [2011] EWHC 1164 (QB), [2011] Info. TLR 13 at para. [36].
[73] Richard Parkes QC, *Sheffield Wednesday v Hargreaves* [2007] EWHC 2375 (QB) at para. [17].
[74] *Applause Store Productions Ltd. v Raphael* [2008] EWHC 1781 (QB) at para. [18].
[75] ibid
[76] The claimant had previously obtained a *Norwich Pharmacal Order* for disclosing the registration data of the user responsible on the *Facebook* site. For commentary, see B. Jordan "Case Comment : *Applause Store Productions Ltd v Grant Raphael*" (2009) 20(2) *Ent LR* 60.

element of the judgment in particular has been criticized as being overly broad[77] given that this type of information could be judged as fundamentally trivial and notwithstanding that birth certificates reside in the public domain. The treatment of relatively trivial information therefore remains unresolved and, given the propensity to post information of this type online, this uncertainty is problematic and helps to explain why the number of online misuse of private information cases remains small. There have only been a handful of these cases brought through the court. Therefore, whilst the effect on the victim can be as devastating, it remains that the reach of the civil law in relation to the online misuse of private information is underwhelming, ineffective and vague. Accordingly, the role of the civil law in this context is somewhat remote and this lends support to the argument that further development in the legal arena of online abuse is necessitated so as to find some neutral ground between the excesses of the criminal law and the luke warm, ambiguous and piecemeal involvement of the civil law, particularly when it comes to trivial information.

Conclusions

The use of Social Networking as a tool for knowledge communication is a growing trend[78], but the development of means of communication throws into sharp relief the limitations of the law as a means of controlling, or even influencing, undesirable behaviour, given its limited influence on those engaging in such activities. This is not least because those who make inappropriate online postings may not fully appreciate or be confused about whether what they are doing is against the law – particularly given the multitude of regulations that might apply to their activities. The question is: can a legal tool address online abuse in a meaningful and effective way? In order to begin to answer this question, this article has examined the reach of criminal and civil law tools following online abuse. It may be summarised that the penalties under criminal law can be extremely harsh, particularly when much of what is written is trivial, whereas, by contrast, the common law remedies which can be awarded largely fail to have real impact. In respect of the latter, enforcement itself is problematic because individuals may not only need to bring to account faceless, anonymous communicators, but they have to pursue their own cause and not every aggrieved individual is inclined, or able, to do so.

[77] Bennett, T, "Horizontality's new horizons - re-examining horizontal effect: privacy, defamation and the Human Rights Act: Part 1" (2010) 21(3) *Ent LR* 96, 103.
[78] S. Miller "The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet" (2009) 97(3), *The Kentucky Law Journal* 541, at p.542.

A common principle of both arms of law considered in this article is that there is a lack of clarity about the scope of acceptable disclosure, particularly in relation to the posting of trivial information, which causes individuals to be ill-informed about the law and causes judges to misinterpret online commentary. The result is one of fragmentation rather than a coherent body of law founded on clear and appropriate principles fit for the purposes of 21st century communications. The present legal landscape attaching to online communications is, therefore, ill-judged, ineffective and confusing. However, the law can be made meaningful and effective and, in pursuit of this outcome, various recommendations follow, each of which is built on the premise that the law is rightly confined to only the most serious cases.

As far as the criminal law is concerned, there are clearly instances where criminal sanctions are appropriate. However, the remit of criminal sanction must not be too overbearing and stifling of free speech. Cases like *Chambers* fall short of the requisite balancing act that criminal regulation must achieve if it is to offer protection without being too oppressive. As the European Court of Human Rights has reiterated throughout its body of case law[79] ever since its landmark 1976 *Handyside* judgment[80], freedom of expression protects not only "favourable" expression but also that which "shocks, offends or disturbs". We suggest that a nuanced approach is called for in which allowance is made for assessing how 'credible' threats are in varied contexts of online communication and according to contemporary societal standards – effectively an attempt to guide the rising generation of users of social media[81]. We suggest that the old fragmented approach should be abandoned in favour of a more coherent set of offences which are designed specifically for social media rather than being adapted from existing laws designed for different circumstances. They should take into account the ways in which the medium is used: writing a letter is a very different form of activity to tweeting, for example. Such offences should also take account of the type of user: users of a platform such as Facebook, for example, are more likely to be younger rather than older people.

[79] See the cases referred to at n.59.
[80] Reported at (1979-80) 1 EHRR 737.
[81] The Department for Education has produced a guide in an attempt to tackle cyber bullying: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/368340/preventing_and_tackling_bullying_october14.pdf (last accessed 2 April 2015).

Additionally, we envisage an increased role for the civil law to deal with the lower level of inappropriate communications in order to avoid such communications being beyond the reach of the law. In order to address matters of clarity, this would involve the creation of a specific civil wrong underpinned by statute. One of the major benefits of a new and independent tort is that it would both allow for a more structured decision-making framework, which would assist a court in assessing when information, even that which is trivial, is judged as intrinsically private[82] and help to clarify the consequences of sharing private information. We envisage that the creation of a statutory tort would, therefore, assist in the identification and appreciation of what, in the light of evolving social tools and behaviours, might be regarded as private and covered by legislation.

Whilst the details of such a tort are open to debate[83] and are complicated by the fact that privacy does not lend itself to precise definition, it is possible to consider how private information might be demarcated based on academic authority. In his future ideology of privacy protection in which "A statute is the best option"[84], Raymond Wacks proposes an approach that seeks to ascertain what *specific interests* of the individual the law ought to protect[85]. To this end, we apply the analysis of Wacks so as to identify what *specific interests* of the individual we think the law ought to protect and we use as our basis Wacks' domestic scholarly taxonomy of such matters[86]. This categorises information as sensitive or not based on the extent to which the collection and use of it holds a potential for *serious harm* to the individual. The approach of Wacks, therefore, aligns with the notions of abuse which are a central theme of this article. Wacks determined that, inter alia, medical history, sex life, political opinions and criminal convictions constituted highly sensitive information and were therefore deserving of privacy protection. By contrast, an individual's name and address represented information of low sensitivity and was, therefore, not deserving of privacy protection[87].

On analysis of the taxonomy developed by Wacks, it is possible to argue that there would be

[82] Warby, M, Moreham, N and Christie, I (eds) and Tugendhat, Hon M (Consultant Editor), *The Law of Privacy and The Media* (2nd edition, Oxford University Press, 2011), at p. 235.
[83] The problems of structuring a tort of privacy were addressed at length in *Kaye v Robertson* [1991] FSR 62 (CA), 70. See, further, Moreham, N, 'Privacy in the common law: a doctrinal and theoretical analysis' (2005) 121 *Law Quarterly Review* 628, 653.
[84] Wacks, R, "Privacy and Media Freedoms" (OUP 2013) 256.
[85] ibid 245.
[86] Wacks, R, *Personal Information: Privacy and the Law* (Clarendon Press, 1989).
[87] ibid 230.

no private information in one's date of birth and, on this basis, one may challenge the finding in the alternative in *Applause Stores*. Wacks' taxonomy therefore provides a means by which one could assess the types of information that might be regarded as private in nature, including trivial information (even though Wacks asserts that trivial or innocuous information would fall outside the law's aegis[88]), and it does so based on a pragmatic approach. However, Wacks' taxonomy is not devoid of problems, not least because it lacks sufficient subjectivity. By way of example, an address may have the potential for serious harm for someone who is building a new life away from a partner who has inflicted domestic abuse, which does not sit comfortably with its (low sensitivity) categorisation within the taxonomy[89]. Moreham argues that, since Wacks provides no way of working out what "intimate" or "sensitive" means, his taxonomy simply replaces the word "private" with two concepts which are equally difficult to define[90], though these could be simply interpreted as ordinary English words. Wacks himself recognizes that the classification may be in need of refinement and is, therefore, neither definitive nor complete[91]. Further, as Solove notes, any taxonomy is an attempt at categorization and all attempts at categorization are artificial[92] particularly given that, in the future, new technologies and ways of living will create new privacy problems and transform old ones[93], making any contribution dated. Hence, any privacy tort would have to keep pace with developments in society and the evolving perceptions of privacy applied by individuals. It will, however, also need to be malleable enough to remain stable and useful without being unnecessarily broad and uncertain[94]. It would, moreover, require the identification of a moving target and attempting to identify foreseeable future infringements of privacy is, therefore, extremely problematic. Accordingly, as Eady has argued extra-judicially, "it would be wholly impractical to descend to the level of micro-management and to anticipate every situation that is likely to come before the courts. One never ceases to be amazed by the extraordinary range of scenarios that present themselves. No legislator could possibly think them up in advance"[95]. Similarly, since we also lack the language for the technological future, the technical complexity and pace of change is so great that the structuring of a

[88] Wacks, R, op. cit., n 84, 245.
[89] Wacks, R op. cit., n 85, 230.
[90] Moreham, N, 'Privacy in the common law: a doctrinal and theoretical analysis' (2005) 121 *Law Quarterly Review* 628, 642.
[91] Wacks, R, op. cit., n. 85, 238.
[92] Solove, D, *Understanding Privacy* (Harvard University Press, 2008) 105.
[93] ibid 197.
[94] Moreham, N, 'Privacy in the common law: a doctrinal and theoretical analysis' (2005) 121 *Law Quarterly Review* 628, 653.
[95] Eady D, 'Injunctions and the protection of privacy' (2010) 29(4) *Civil Justice Quarterly* 411, 420.

statutory tort would require to be drafted at a level of generality that would still require some degree of judicial intervention to resolve disputes[96]. Nonetheless, the type of demarcation that could be envisaged based on Wacks' taxonomy might make a positive impact at addressing the uncertainty that particularly surrounds trivial information.

Whilst the threshold for what might constitute private information would need to be determined on the basis of consultation, it might arguably fall below the current threshold of the criminal law. Given the lower level of legal intervention, this might catch those who may be on the road to more seriously inappropriate conduct and might also cause individuals to think about what they send or post in future. The lower threshold and lower standard of proof would enable individuals to be brought within the system without the need for criminal proceedings, without the consequences attaching to a criminal conviction and without the intervention of the police.

In keeping with other areas of the civil law, in which enforcement is in the hands of bodies such as local authorities, we consider that a body specifically charged with enforcement should be established[97] and that, rather than an award of compensation, individuals should be required to attend a course designed to educate them as to appropriate usage[98]. This would go some way to meeting one of the major issues relating to the use of social media, namely the idea that anything can be posted on the internet with impunity, as such a course would alert users to the possible consequences of inappropriate posting. This proposal will therefore educate the public about the value of privacy and this is considered an important part of crafting a regulatory solution that ensures privacy becomes a public good for online users[99].

The criminal law or (virtually) nothing approach that characterises the current state of the law only deals with the extremes of acceptable or very unacceptable. Inserting something into the

[96] McLean, A and Mackey, C, 'Case Comment : Mosley v News Group Newspapers Ltd: how sadomasochism changed the face of privacy law: a consideration of the Max Mosley case and other recent developments in privacy law in England and Wales' (2010) 32(2) *European Intellectual Property Review* 77, 87.

[97] Whilst it may seem that the Information Commissioner would be an appropriate enforcer, given the adjudicatory functions exercised by him, there would be a potential conflict of interests.

[98] A similar outcome attaches to certain road traffic offences whereby drivers can avoid penalty points and fines in certain circumstances by attending a safe driving course, by virtue of the Road Safety Act 2006 s. 34. ~~. The police may offer such a course to suitable offenders under the National Driver Offender Retraining Scheme, which has been in place since 1991. See http://www.acpo.police.uk/documents/uniformed/2013/201303-uoba-ndors-guidance.pdf (last accessed 2 April 2015).~~The offences to which it applies include speeding and careless driving offences under the Road Traffic Act 1988 s. 3. We are grateful to Louise Loving for help on this point.

[99] Papacharissi, Z and Gigson, op. cit., n. 14, at p. 86.

middle ground could have beneficial effects, even if only marginally, given the peripheral influence of the law in this area. Nevertheless, we believe it is an avenue worth exploring.

As Lord Justice Leveson has articulated in relation to online communications, "the question for us all [is].. to ensure that the criminal and civil law remain effective"[100]. Essentially, then, a more nuanced approach aimed at raising public and individual awareness may help in the identification and appreciation of what, in the light of evolving social tools and online behaviours, might be regarded as rightly incurring legal responsibility. This, we argue, can be achieved by putting in to effect the practical suggestions detailed above, which, by speaking to the contours, customs and practices of online communications, improve the applicability and usefulness of both criminal and civil law in the context of online communications.

[100] The Rt. Hon. Lord Justice Leveson, "Hold The Front Page: News-Gathering In A Time Of Change", University Of Melbourne, Australia, 12 December 2012, available at http://www.judiciary.gov.uk/wp-content/uploads/JCO/Documents/Speeches/lj-leveson-speech-hold-the-front-page-melbourne-12122012.pdf (accessed 1 July 2015)..