HOUSE OF LORDS

Select Committee on Communications

1st Report of Session 2014–15

Social media and criminal offences

Ordered to be printed 22 July 2014 and published 29 July 2014

Published by the Authority of the House of Lords

London : The Stationery Office Limited
£9.00

HL Paper 37

The Select Committee on Communications

The Select Committee on Communications was appointed by the House of Lords on 12 June 2014 with the orders of reference "to consider the media and the creative industries."

Membership

The Members of the Select Committee on Communications are:

Baroness Bakewell
Lord Best (Chairman)
Lord Clement-Jones
Baroness Deech
Lord Dubs
Baroness Fookes
Baroness Hanham
Baroness Healy of Primrose Hill
Lord Horam
The Bishop of Norwich
Lord Razzall
Baroness Scotland of Asthal
Lord Sherbourne of Didsbury

Declarations of interest

See Appendix 1

A full list of Members' interests can be found in the Register of Lords' Interests:
http://www.parliament.uk/mps-lords-and-offices/standards-and-interests/register-of-lords-interests

Publications

All publications of the Committee are available at:
http://www.parliament.uk/hlcommunications

Parliament Live

Live coverage of debates and public sessions of the Committee's meetings are available at:
http://www.parliamentlive.tv

Further information

Further information about the House of Lords and its Committees, including guidance to witnesses, details of current inquiries and forthcoming meetings is available at:
http://www.parliament.uk/business/lords

Contact details

All correspondence should be addressed to the Select Committee on Communications, Committee Office, House of Lords, London SW1A 0PW. Telephone 020 7219 6076/8662. Email holcommunications@parliament.uk

CONTENTS

Evidence is published online at http://www.parliament.uk/hlcomms and available for inspection at the Parliamentary Archives (020 7219 5314)

References in footnotes to the Report are as follows:
Q refers to a question in oral evidence

Social media and criminal offences

CHAPTER 1: INTRODUCTION

"#filthypikey"

"hope your crying and now you should be why cannot you even produce for your country your just a diver anyway a over hyped prick"

"Crap! Robin Hood airport is closed. You've got a week and a bit to get your shit together otherwise I'm blowing the airport sky high!!"

"Go suck muamba's dead black dick then you aids ridden twat", "you are a silly cunt … your mothers a wog and your dad is a rapist! Bonjour you scruffy northern cunt!"

"UnBonJuif est un juif mort xd kc"

"Fuck off and die you worthless piece of crap", "go kill yourself"; "I will find you", "rape her nice ass"

"swindler"

Background to this inquiry

1. Which of the above statements are criminal and which are merely offensive? Which deserve punishment by the state; which need access only to a private remedy; which require no remedy because we value freedom of expression more than preventing offence?

2. The House appointed this Committee on 12 June, to consider the media and the creative industries. We are interested in how the development of media affects people's behaviour and how the law and public policy need to respond. In that context we set out to explore the social media and criminal offences.

3. We wished to operate at some speed, because this is an issue of current concern, and we were grateful to be able to hear at short notice from:

   (a) The Director of Public Prosecutions;

   (b) The Chief Constable of Essex, the Association of Chief Police Officers' coordinator for the digital intelligence and investigation environment;

   (c) Policy Director, UK, Middle East and Africa, Facebook, an online social networking service;

   (d) Director, Public Policy, EMEA, Twitter, an online social networking and microblogging service (on which users' individual publications, "tweets", are limited to 140 characters each);

   (e) Legal Officer, Article 19, a freedom of expression organisation; and

(f) John Cooper QC of 25 Bedford Row.[1]

We have published the transcript of oral evidence which, in itself, forms a valuable resource for those interested in this subject.

4. Our principal objectives in this report are to offer the House some information about an important area of public policy and to stimulate discussion. We have also offered some opinion, but that opinion is tentative because, in the time available, we have not considered the subject as broadly or in as much depth as it merits. Our inquiry has raised a number of further questions, some relatively specific, others which go to the fundamental dilemmas of the internet.

5. **Our overall conclusion is that the criminal law in this area, almost entirely enacted before the invention of social media, is generally appropriate for the prosecution of offences committed using the social media.**

6. We make this report for the information of the House and we do not expect a formal response from the Government.

1 We explicitly thank the Recorder of Manchester for releasing Mr Cooper from court for the purpose.

CHAPTER 2: SOCIAL MEDIA AND THE LAW

Social media and offences

7. The social media are a recent invention. The two most popular websites, Facebook and Twitter, were founded in 2004 and 2006 respectively. They may be new, but they are big. 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. 500 million "tweets" are made a day.[2] In addition to these well-known providers, there are many other social media forums, based all over the globe, with different focuses of activity (from flower arranging to sadomasochism), all with the purpose of "social networking", of connectivity: enabling people to express themselves and interact using the internet.

8. As we heard from John Cooper QC, "the vast majority of people who use the social media are like society. The vast majority are decent, intelligent, inspiring people. The problem comes with a small minority, as in society, who spoil it for everyone else."[3]

9. Amongst the ways in which people are spoiling it for everyone else are the following behaviours:

   (a) cyber bullying—bullying conducted using the social media or other electronic means;

   (b) revenge porn—usually following the breakup of a couple, the electronic publication or distribution of sexually explicit material (principally images) of one or both of the couple, the material having originally been provided consensually for private use;

   (c) trolling—intentional disruption of an online forum, by causing offence or starting an argument; and

   (d) virtual mobbing—whereby a number of individuals use social media or messaging to make comments to or about another individual, usually because they are opposed to that person's opinions.

   These definitions are our own and imprecise; others use these words to mean different and overlapping things.

10. In addition to these apparently modern offences, most offences which can be committed by using words or images can be committed using the social media, for example threatening violence to the person.

The law: facts

Criminal offences

11. Criminal offences define acts (or omissions) which are so harmful that the wrong is thought to be against the state rather than the individual who has suffered the act; the state prosecutes and, on conviction by a court, the state punishes, by deprivation of liberty, fine or other means.

---

2 Q 25

3 Q 1

12. There are two different ways to think about the harmful acts committed using social media: either they are new acts, or they are acts already prohibited by the criminal law but committed in the new forum of social media as opposed to elsewhere. We have been persuaded that the latter is usually the case. "The social media is simply a platform for human beings to behave or misbehave"[4]; "It is not about the medium, it is about the offence".[5]

13. Harassment, malicious communications, stalking, threatening violence, incitement are all crimes and have been for a long time.

14. The Director of Public Prosecutions has published guidelines for the application of the current statute law to prosecutions involving social media communications. The guidance is clear and accessible. The guidance is structured by conduct, relating different sorts of conduct to different potential offences:

    (a) credible threats of violence to the person or damage to property:

        (i) Offences Against the Person Act 1861, s 16 (threat to kill)

        (ii) Protection From Harassment Act 1997, s 4 (fear of violence)

        (iii) Malicious Communications Act 1988, s 1 (threat)

        (iv) Communications Act 2003, s 127 (of a menacing character)

        (v) together with legislation related to racial, religious, disability, sexual orientation or transgender aggravation

    (b) communications targeting specific individuals:

        (i) Protection from Harassment Act 1997, s 2 (harassment)

        (ii) Protection from Harassment Act 1997, s 2 (stalking)

        (iii) Protection from Harassment Act 1997, s 4 (fear of violence)

        (iv) Protection from Harassment Act 1997, s 4A (stalking involving fear of violence, serious alarm or distress)

    (c) breach of court order, e.g. as to anonymity:

        (i) Contempt of Court Act 1981

        (ii) Sexual Offences Amendment Act 1992, s 5 (identification of a victim of a sexual offence)

        (iii) restraining orders, conditions of bail

    (d) communications which are grossly offensive, indecent, obscene or false:

        (i) Malicious Communications Act 1988, s 1 (electronic communications which are indecent or grossly offensive, convey a

---

4 Q 5

5 Q 37

threat false, provided that there is an intention to cause distress or anxiety to the victim)

(ii) Communications Act 2003, s 127 (electronic communications which are grossly offensive or indecent, obscene or menacing, or false, for the purpose of causing annoyance, inconvenience or needless anxiety to another)

These offences all pre-date the invention of social media. These offences are offences under the law of England and Wales; we have not considered the position in Scotland or Northern Ireland. A table of our own design showing these offences and their relationship to social media is at Appendix 3.

15. The Protection from Harassment Act 1997 also provides for civil remedies in the form of injunctions and damages, on application to the High Court, to protect a person from harassment.

16. **As this report sets out, there are aspects of the current statute law which might appropriately be adjusted and certain gaps which might be filled. We are not however persuaded that it is necessary to create a new set of offences specifically for acts committed using the social media and other information technology.**

17. **Despite calls in oral evidence to the contrary, we have not been persuaded that it is always desirable to remove overlaps: we understand that overlaps commonly occur in the criminal law[6] and are usually necessary to provide for different circumstances.**

18. **Similarly, we see no special need to codify or consolidate all offences which can be committed using social media: it is no more desirable to do so for these offences than for any other part of the criminal law.**

19. The Director of Public Prosecutions publishes statistics which show by year the number of offences charged and reaching a first hearing, by reference to the statutory provision creating the offence. There are at present no statistics which indicate the balance of offences committed online and by traditional means, nor of the number of offences reported. We have anecdotal evidence as to the scale of the problem, but few facts. **It would be useful for such statistics to be compiled.**

Defamation

20. Social media can just as readily be used to defame (bringing ill fame or dishonour upon) someone as can any other media. Defamation has not been an offence since commencement of section 73 of the Coroners and Justice Act 2009. Defamation remains privately actionable in the High Court (i.e. civil courts), with no limit to the damages available as a remedy. There is no longer any distinction between slander (oral defamation) and libel (defamation through other media). This report is not about defamation.

---

[6] Q 16: "Alison Saunders: … Assault is a sort of classic where you might have overlap, whether it is a common assault or a section 47—actual bodily harm. That is what the guidance that we have issued is around…

Lord Razzall: But you do agree that currently there is a bit of an overlap?

Alison Saunders: There is, as with a number of different parts of the legislation that we operate under."

Freedom of expression

21. The United Kingdom is a signatory to various international obligations which secure freedom of expression. Article 10 of the European Convention on Human Rights maintains that "everyone has the right to freedom of expression" and that that right may only be qualified in narrowly limited circumstances. Those circumstances include national security, public safety, the protection of morals, and the protection of the reputation or rights of others".

Box 1: ECHR Article 10—Freedom of expression

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

22. The Human Rights Act 1998 requires judges to interpret legislation in a way which is compatible with the Convention rights so far as it is possible to do so. This means that all of the offences described at paragraph 14 must be interpreted still to give effect to Article 10. The restrictions this places on the offences and on freedom of expression is explored by the courts case-by-case. It is most relevant to considering prosecution of communications which are grossly offensive, indecent, obscene or false. The courts have said:

> "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, shock or disturb …" (*Sunday Times v UK (No 2) [1992] 14 EHRR 123*)

> "Satirical, or iconoclastic, or rude comment, the expression of unpopular of 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 [section 127 of the Communications Act 2003]" (*Chambers v DPP [2012] EWHC 2157(Admin), LCJ*)

> "There can be no yardstick of gross offensiveness otherwise than by the application of reasonably enlightened, but not perfectionist, contemporary standards to the particular message sent in its particular context. The test is whether a message is couched in terms liable to cause gross offence to those to whom it relates." (*DPP v Collins [2006] UKHL 40, Lord Bingham of Cornhill*)

23. Article 19, a freedom of expression organisation, argued that, due to this international obligation, it was not legitimate to prosecute offences of sending a grossly offensive communication unless the communication had threatened violence.[7] John Cooper QC qualified this by saying that psychological violence was violence, at least for some offences.[8]

24. In addition to the requirement for compatibility with the ECHR, the Director of Public Prosecutions' guidance requires prosecutors to take into account context:

> "prosecutors should have regard to the fact that the context in which interactive social media dialogue takes place is quite different to the context in which other communications take place. Access is ubiquitous and instantaneous. Banter, jokes and offensive comments are commonplace and often spontaneous. Communications intended for a few may reach millions."

25. It quotes Mr Justice Eady in the High Court giving his opinion as to the nature of comments on an internet bulletin board as being:

> "contributions to a casual conversation (the analogy sometimes being drawn with people chatting in a bar) which people simply note before moving on; they are often uninhibited, casual and ill thought out; those who participate know this and expect a certain amount of repartee or 'give and take'." (*Smith v ADVFN [2008] 1797(QB)*)

26. The Director's guidance says that, in consequence:

> "prosecutors should only proceed with cases under section 1 of the Malicious Communications Act 1988 and section 127 of the Communications Act 2003 where they are satisfied that there is sufficient evidence that the communication in question is more than:
>
> - offensive, shocking or disturbing;
> - satirical, iconoclastic or rude; or
> - the expression of unpopular or unfashionable opinion about serious or trivial matters, or banter or humour, even if distasteful to some or painful to those subjected to it."

27. In contrast, the Chief Constable of Essex observed to us that social media commentary has a permanence, whereas the same comments in "a playground, coffee shop or pub" are transient and forgotten within moments.[9]

28. We consider that today's users of social media and other information technology should be well aware that, in certain forums, they are capable of having a huge audience, invited and uninvited; known and strangers; anonymous and identified.

---

[7] Q 2

[8] Q 3

[9] Q 21

29. Similarly, today's users should also be aware that the major website operators enable their users to protect themselves if they wish to do so, principally by adjusting their "privacy settings", for example to make their profile visible only to people they have explicitly approved.

30. Although we accept that social media are not entirely analogous to a public bar (because the comments endure unless removed by the website operator), **we consider that the Director's guidance appropriately takes account of freedom of expression.**

The law: opinion

31. In this section, we offer our opinion on the adequacy of the statute book in relation to criminal offences and social media.

"Cyber bullying" and "trolling"

32. **Our starting point is that what is not an offence off-line should not be an offence online. There is no specific criminal offence of bullying.**[10] **We consider that the current range of offences, notably those found in the Protection from Harassment Act 1997, is sufficient to prosecute bullying conducted using social media. Similarly, sending a communication which is grossly offensive and has the purpose of causing distress or anxiety is an offence under section 1 of the Malicious Communications Act 1988. Although we understand that "trolling" causes offence, we do not see a need to create a specific and more severely punished offence for this behaviour.**

"Virtual mobbing"

33. John Cooper QC considered that the current form of the Protection from Harassment Act 1997 was sufficient for the prosecution of virtual mobbing.[11] Section 4A of the Public Order Act 1986 might also be relevant. For the 1997 Act, a "course of conduct" is however a necessary ingredient of the offence. A course of conduct "must involve conduct on at least two occasions". If 100 people send a single abusive tweet each to one person, it is not clear whether any offence has been committed under the 1997 Act.

34. There is a long-standing common law concept in criminal law of "joint enterprise", whereby all members of a group acting with common purpose and common intention may be held liable for the consequences of their actions. **We do not see why the common law principle of joint enterprise should not apply to offences committed under the Protection from Harassment Act 1997 and similar legislation, so enabling the prosecution of members of a group acting with common purpose and intention. The courts will determine whether joint enterprise catches instances in which the people involved did not know each other and acted at different times and in different places.**

Revenge porn

35. The treatment of incidents of "revenge pornography" (defined at paragraph 9(b)) deserves further consideration.

---

[10] Q 10

[11] Q 8

36. The first question that arises in our mind is whether the behaviour (i.e. revenge porn) is already caught by one of the existing offences and, if not, whether it ought to be criminalised.

37. In a recent debate on the question, the Minister said that offences created by section 127 of the Communications Act 2003, the Protection from Harassment Act 1997 and the Malicious Communications Act 1988 were all relevant. [12] Section 127 of the 2003 Act provides that is an offence to send:

> by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character

Section 1 of the 1988 Act provides that it is an offence to send:

> a [communication] which is indecent or grossly offensive; a threat; or information which is false and known or believed to be false by the sender; [if his purpose is that] it should cause distress or anxiety to the recipient or to any other person to whom he intends that it or its contents or nature should be communicated

38. The offences are triable in the magistrates' court and a person found guilty of such an offence is liable to up to 6 months' imprisonment, a level 5 fine (up to £5,000) or both.

39. Clause 27 of the Criminal Justice and Courts Bill, currently before the House, proposes to i) make the offence and the 1988 Act triable in either the magistrates' court or the Crown Court; and ii) increase the available sentence on conviction by a magistrates' court to 12 months' imprisonment, a fine or both; and by the Crown Court to 2 years' imprisonment, a fine or both. Notwithstanding our observation at paragraph 49, we consider this new flexibility to be desirable.

40. Revenge pornography is not directly considered in the Director of Public Prosecutions' guidance for prosecutions involving social media communications. The Director's separate guidance on the prosecution of offences relating to obscene publications sets out a general reluctance to prosecute (especially where the subjects consent to the behaviour) other than where a publication portrays illegal or extreme sexual acts. Ordinary images of consensual sexual acts are not considered obscene. **We would welcome clarification from the Director of Public Prosecutions as to the circumstances in which an indecent communication could and should be subject to prosecution under section 127 of the Communications Act 2003 or section 1 of the Malicious Communications Act 1988.**

41. Irrespective of the commission and prosecution of a criminal offence, a private remedy is already available to the victim. Images of people are covered by the Data Protection Act 1988 (as "personal data"), and so is information about people which is derived from images. [13] Images of a person count as "sensitive personal data" under the Act if they relate to "sexual life". Under the Act, a data subject may require a data controller not to process the data in a manner that is "causing or is likely to cause substantial damage

---

12 HL Deb, 21 July 2014, col 978

13 Available at: http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv

or substantial distress to him or to another". The Information Commissioner may award compensation to a person so affected. Personal data "processed by an individual only for the purposes of that individual's personal, family or household affairs (including recreational purposes)" are exempt from this provision but the European Court of Justice has determined that posting material on the internet is not part of one's "personal, family or household affairs"[14].

42. In addition, since the judgment of the European Court of Justice in the Google Spain case, data subjects have the right to ask search engines to remove links to certain data relating to the data subject:

> "… it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question"[15]

This is a useful, if after the event, protection in cases where the website operator refuses to remove the information.

43. An individual may also apply to the High Court for a privacy injunction to prevent or stop the publication of material relating to a person's sexual life. This was successfully done in the case of *Contostavlos v Mendahun* ([2012] EWHC 850 (QB)): the court granted the claimant an injunction to prevent the publication by the defendants of a video showing the claimant and defendant having sexual intercourse, which one of the defendants proposed to publish in the circumstances common to revenge porn. The case was set to involve consideration of damages but settled before the court had to determine the question.

44. We are concerned that the latter remedy is available only to those who can afford access to the High Court. It would be desirable to provide a proportionately more accessible route to judicial intervention.

---

[14] ECJ Case C-101/01

[15] ECJ case C-131/12; *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*.

Time for authorities to investigate before prosecution

45. For most of the offences with which we are here concerned, the prosecution must start (usually the laying of an information in a magistrates' court) no later than six months after the offence took place. That period is set by section 127 of the Magistrates' Court Act 1980. The Chief Constable of Essex asked for website operators to respond faster to requests for evidence.[16] The Director of Public Prosecutions asked for longer because it could take longer than that to obtain information from website operators abroad.[17] **We sympathise with this perspective and suggest that 12 months would be proportionate.**

46. **There is little point in extending this time limit unless the data exist. It would obviously facilitate the detection and prosecution of crime if operators of social media websites were required to capture and retain evidence of the traffic on their sites. This though raises the much broader and exceptionally contentious issues around communications data.**

Other

47. **A number of statutes passed before the invention of the internet refer to publications in terms only of print media. For example, section 39 of the Children and Young Persons Act 1933 restricts reporting by newspapers in relation to children involved in criminal proceedings: electronic communications and social media are not caught; we believe they should be.**

48. **The offences with which we are concerned involve both the act and the nature of the intention on the part of the person committing the act (the "*mens rea*"). This latter aspect varies between offences and might benefit from a degree of consistency.**

49. **There are often calls to increase the severity of sentence available for the punishment of these sorts of offences. We favour increasing the courts' discretion in this area but we would be reluctant for Parliament to require more cases to be tried in the Crown Court (i.e. judge and jury as opposed to magistrates), due to the implications for workload. Any increase in flexibility should be carefully monitored and the proportionality of the consequences considered.**

Anonymity

50. The internet readily facilitates its users doing so anonymously. Although it is possible to identify (including retrospectively) which computer in the world was used to post a statement (because each computer has a unique "internet protocol address"), it is not necessarily possible to identify who used that computer to do so.

51. This is in part because many website operators facilitate the anonymous use of their service. There is no consistent attitude taken by website operators: some require the use of real names (Facebook, although they do not actively confirm users' identities); some allow anonymity but challenge

---

16 Q 20

17 *Ibid*

impersonation (Twitter)[18]; others allow absolute anonymity. Google+ abandoned its real name policy and apologised for having tried to introduce one. [19]

52. Twitter drew to our attention the value of anonymity for human rights workers, dissidents and journalists working in conflict areas: it enables them to publish information and opinion without placing themselves at risk.[20]

53. There is a less positive side to this disinhibiting effect of anonymity, with its lack of apparent accountability and immediate confrontation: it facilitates offensiveness, notably in the forms of cyber bullying and trolling. ask.fm is a Latvian-based social networking site where users can ask each other questions with the (popular) option of anonymity. The site is popular with British teenagers and is sadly infamous for the bullying conducted using it and for the consequences of that bullying. In 2012, Erin Gallagher committed suicide at the age of 13. Her mother said that Erin had named ask.fm in her suicide note and that she could not cope with the bullying.[21] Anthony Stubbs committed suicide in 2013; his girlfriend received abuse on ask.fm.[22] There are further similar incidents relating to the same and other websites. As a result of these incidents and the adverse publicity which they attracted, ask.fm has introduced a number of privacy options.

54. Section 5 of the Defamation Act 2013 incentivises website operators to know the identities of their users (see paragraph 89). It is a fraught question whether to require the operators of websites (which enable their users to post opinion) to establish the identity of people opening accounts to use their services, whether or not the website subsequently allows those people to use their service anonymously. Would this be an undesirably chilling step towards tyranny, or merely a necessary administrative step to ensure that law enforcement agencies can properly investigate crime? **From our perspective in the United Kingdom, if the behaviour which is currently criminal is to remain criminal and also capable of prosecution, we consider that it would be proportionate to require the operators of websites first to establish the identity of people opening accounts but that it is also proportionate to allow people thereafter to use websites using pseudonyms or anonymously. There is little point in criminalising certain behaviour and at the same time legitimately making that same behaviour impossible to detect. We recognise that this is a difficult question, especially as it relates to jurisdiction and enforcement.**

Provision of evidence

55. There are means by which both public authorities and private individuals may try to obtain information about the identity of a person who has made a statement anonymously, with a view to court proceedings.

---

18 QQ 30, 35

19 Available at: http://www.theguardian.com/technology/2014/jul/16/youtube-trolls-google-real-name-commenter-policy

20 Q 35

21 Available at: http://www.independent.ie/irish-news/tragic-erin-named-askfm-in-suicide-note-claims-mother-29497140.html

22 Available at: http://www.lep.co.uk/news/local/family-call-for-ask-fm-to-be-shut-down-1-5629088

56. A private individual may ask the court to make a "Norwich Pharmacal order", a well-established procedure which requires the respondent to disclose information to the claimant. The respondent must be either involved or mixed up in a wrongdoing, whether innocently or not, and is unlikely to be a party to the potential proceedings.

57. A relevant public authority for the purposes of the Regulation of Investigatory Powers Act 2000, including the police, may use Chapter II of that Act to obtain communications data for the purpose of detecting crime. The Joint Committee on the draft Communications Data Bill observed: [23]

> **Communications data held overseas**
>
> 33. RIPA is drafted so as to attempt to give United Kingdom public authorities a legal basis for requesting communications data from CSPs [communications service providers] based overseas if they operate a service in the United Kingdom. However, many overseas CSPs refuse to acknowledge the extra-territorial application of RIPA. The procedure can of course be used to request access to data, and many CSPs will comply but emphasise that they are doing so on a voluntary basis; others will refuse to respond to RIPA requests at all. At that stage the only way in which United Kingdom law enforcement authorities can access the data is through the arrangements for international mutual legal assistance which allow the judicial and prosecuting authorities of one state to seek from the authorities of another state help in the prevention, detection and prosecution of crime.

58. We see the same issue. John Cooper QC said that the law was not yet certain as to where the cause of action arose. This created a problem with proving the offence.[24] Twitter said that they would cooperate and work with the police in any territory where an offence had been alleged to have been committed.[25] We notice however that the authorities in France have only very recently, and at the end of a lengthy court process, persuaded Twitter to cooperate with them in relation to the investigation of the posting of anti-Semitic tweets.[26] Twitter's position remains that they are cooperating voluntarily. **We encourage website operators to expedite requests for identity data made by our recognised law enforcement agencies using powers granted by Parliament.**

---

[23] Joint Committee on the draft Communications Data Bill, *Draft Communications Data Bill* (Report of Session 2012–13, HL Paper 79, HC479) paragraph 33.

[24] Q 7

[25] Q 28

[26] Available at: http://www.theguardian.com/technology/2013/jul/12/twitter-data-french-antisemitic-tweets

CHAPTER 3: GUIDANCE ON PROSECUTIONS

Guidance on prosecutions

59. It might not always be at the forefront of people's minds that, just because an offence appears to have been committed and has been reported to the police, it will not always be investigated or prosecuted by the state.

60. The Prosecution of Offences Act 1985 requires the Director of Public Prosecutions to issue guidance on the principles to be applied when prosecutors consider whether to institute proceedings for any offence. All of the guidance is published. There is a core document supplemented by specific guidance on particular ranges of offences. The two basic principles are: i) is there enough evidence against the defendant; ii) is it in the public interest for the CPS to bring the case to court.

Evidence

61. In terms of evidence, Crown Prosecutors must consider whether evidence can be used in court and is reliable and credible. Crown Prosecutors must be satisfied there is enough evidence to provide a "realistic prospect of conviction" against each defendant.

Public interest

62. In terms of public interest, a prosecution will usually take place unless the prosecutor is sure that the public interest factors tending against prosecution outweigh those tending in favour. Public interest considerations include the likely sentence, the delay if there has been a delay, the position of trust that the alleged offender may be in, the position of the victim and whether they are a particularly vulnerable victim.[27]

63. The Director necessarily has significant discretion to determine when it is in the public interest to bring a prosecution and when it is not. It is always open to Parliament to qualify that discretion.

64. The Director has published guidelines for prosecutions involving communications sent using social media. As we set out at paragraph 14, the guidance is structured by four types of conduct:

    (a) communications which may constitute credible threats of violence to the person or damage to property

    (b) communications which specifically target an individual and which may constitute harassment or stalking

    (c) communications which may amount to a breach of a court order

    (d) communications which may be considered grossly offensive, indecent, obscene or false.

65. The guidance says that cases falling within (a), (b) or (c) should be prosecuted robustly, whereas cases which fall within (d) face a high threshold and in many cases a prosecution is unlikely to be in the public interest.

---

[27] Q 11

Grossly offensive

66. There is a long-standing and unresolved debate about the extent to which "grossly offensive" statements should be criminalised: we discussed the question at paragraphs 21 to 30. There is a similar debate about when such offences should be prosecuted.

67. In relation to these offences, the Director's guidance says:

> "a prosecution is unlikely to be both necessary and proportionate where:
>
> the suspect has expressed genuine remorse;
>
> swift and effective action has been taken by the suspect and/or others for example, service providers, to remove the communication in question or otherwise block access to it;
>
> the communication was not intended for a wide audience, nor was that the obvious consequence of sending the communication; particularly where the intended audience did not include the victim or target of the communication in question; or
>
> the content of the communication did not obviously go beyond what could conceivably be tolerable or acceptable in an open and diverse society which upholds and respects freedom of expression.
> …
>
> In particular, where a specific victim is targeted and there is clear evidence of an intention to cause distress or anxiety, prosecutor should carefully weigh the effect on the victim, particularly where there is a hate crime element to the communication(s). A prosecution … may be in the public interest in such circumstances"

68. The Director told us that the threshold for prosecution in the majority of cases involving social media was the same as for making the same comment orally in a public place.[28]

69. **For the reasons set out at paragraphs 21 to 30, we think that the Director's guidance on the prosecution of "grossly offensive" communications is proportionate and appropriate. It does however have the effect that few offences committed under section 1 of the Malicious Communications Act 1988 and section 127 of the Communications Act 2003 will be prosecuted. There may be a case for Parliament itself determining the circumstances in which such offences should be prosecuted. On the other hand, the advantage of this remaining in guidance is that the guidance can be adjusted with greater agility than can a statute.**

70. It is also appropriate because the volume of alleged offences is so high. As John Cooper QC put it: "the police are being inundated with spurious complaints … They cannot investigate every transgression on the social media".[29] In due course, we hope that better statistics will be available as to allegations, investigations and prosecutions: they would inform the debate as to the appropriateness of the law.

---

[28] Q 21

[29] Q 7

CHAPTER 4: OTHER ISSUES

Children

71. Society grants a leniency to children for some behaviour which would be prosecuted as criminal if done by an adult. In England and Wales, children below the age of 10 are not generally held to be capable of committing a crime. Special guidance from the Director of Public Prosecutions applies to considering whether to prosecute a child between the ages of 10 and 18. This is not because society considers that children between the ages of 10 and 18 may behave with impunity; instead it considers that it is usually proportionate for parents and schools to take proportionate remedial action and to educate the child as to appropriate behaviour.

72. The Code for Crown Prosecutors says that prosecutors must have particular regard to:

> "was the suspect under the age of 18 at the time of the offence? … The best interests and welfare of the child or young person must be considered including whether a prosecution is likely to have an adverse impact on his or her future prospects that is disproportionate to the seriousness of the offending … As a starting point, the younger the suspect, the less likely it is that a prosecution is required …
>
> However, there may be circumstances which mean that notwithstanding the fact that the suspect is under 18, a prosecution is in the public interest. These include where the offence committed is serious, where the suspect's past record suggests that there are no suitable alternatives to prosecution, or where the absence of an admission means that out-of-court disposals which might have addressed the offending behaviour are not available"

73. This is generally thought to be proportionate and appropriate: the criminal justice system can intervene when it needs to do so.

74. Our inquiry is limited to consideration of the law. It strikes us though that parents and schools have a responsibility generally to educate children: children need to be taught that being horrid online is just as wrong and hurtful as being horrid face to face. Similarly, parents have an essential responsibility to protect their children from harm on the internet as they do when children are in any other public space. Schools have an opportunity to draw to parents' attention when they detect that parents might need to intervene. How most appropriately and effectively to approach this is a matter we have not considered. It strikes us as unlikely that simply banning access would be effective.

Balances: law v policy interventions

75. We have limited this inquiry to an investigation of the law, but the law is rarely the most effective tool for changing behaviour: effective law tends to reinforce, rather than in itself change, social attitudes.

76. At present, the law prohibits people from sending grossly offensive messages but people send them nonetheless, and in great number, in part due to the ease with which the internet and social media facilitate communications. The

threshold for prosecution is rightly high. This prevents the courts from being overwhelmed with inappropriate cases, but it does not reduce (let alone prevent) inappropriate complaints to the police. As John Cooper QC put it: "the police are being inundated with spurious complaints … They cannot investigate every transgression on the social media".[30] The consequence is that there is every chance that offences which deserve to be prosecuted will not be, due simply to the volume of complaints.

77. A victim has to be confident that an offence has been committed; the police constable to whom the offence is reported needs to understand what offence has been committed and whether it is initially proportionate to consider the matter criminal or whether some other course of action should be taken. Other than gradual, general social education, there is no efficient way to address this. The advertisement of the law and of rules on websites is desirable, but not very effective. The widespread publicity given by the traditional media to the conviction of people prosecuted for committing offences using social media does more to educate than any advertisement. We welcome the efforts of the police to educate themselves about the relationship between social media and criminal offences and hope that this will extend to the officers with whom the public are most likely first to come into contact.

78. In the light of the volume of offences, society has four options: i) do nothing and accept the status quo; ii) add resources so that more allegations can be investigated and prosecuted; iii) change the law so that the behaviour is no longer criminal; iv) retain the law and approach to prosecutions, but seek to change behaviour through policy interventions.

Website operators

Attitude

79. Both Facebook and Twitter presented themselves to us less as corporations responsible as legal persons under the law, and more as communities who operate according to their own rules.[31]

80. Those rules can be admirable: Facebook has a real name culture, a set of community standards (e.g. regarding nudity), enables people to control their own privacy, and enables the reporting of abuse;[32] Twitter have rules against threats of violence, targeted harassment and similar issues. Other operators are less responsible. Irrespective of the responsibility of the website operators, the behaviour with which we are concerned is criminal.

Monitoring

81. The number of staff employed to consider reports of content or conduct is inevitably inadequate to the scale of use of the website. Globally, Facebook employ "hundreds" of people in this area; Twitter "in excess of 100".

82. Facebook has developed technology to prevent or quickly stop the posting of certain material, for example child sexual exploitation.[33] Similarly, systems

---

30 Q 7

31 QQ 25, 26; cf paragraph 63

32 Q 26

33 Q 26

urgently flag for human intervention the most serious types of report, such as suicide or self-harm[34] but the systems are not perfect because the traffic on the site is varied and can irrationally spike. We received no evidence about the speed or proportionality with which less serious types of report were processed.

83. These actions in our opinion have been driven by the companies' own values and by the market, not by law. Many website operators are significantly less responsible.

84. **We encourage website operators further to develop their ability to monitor the use made of their services. In particular, it would be desirable for website operators to explore developing systems capable of preventing harassment, for example by the more effective real-time monitoring of traffic.**

Self-help

85. Every user of Facebook can control the extent to which other users may interact with them: privacy settings. Facebook has introduced a tool to report abuse; and also a tool whereby user A may ask user B to remove a post (usually a photograph) in which the user A is portrayed. Facebook told us that in 85% of cases, user B complies.[35]

86. **Self-help, as in the ability to block sight of abuse, is valuable but its value is limited when the abuse remains in the public domain. We encourage website operators further to develop the effectiveness of measures to enable individuals to protect themselves when using social media services.**

87. **It would be desirable for website operators to publish statistics on monitoring and self-help.**

Liability at law

88. A European Union directive[36] has harmonised provision on electronic commerce, including the liability of websites which host content originated by others. That directive is implemented in United Kingdom law in the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013). Those regulations give immunity to websites from damages or criminal sanctions where they act merely as a conduit, cache or host, so long as they operate an expeditious "take down on notice" service. This acts as an incentive to website operators to remove illegal or actionable material. It is for the website itself to determine whether the material which they have been asked to remove is genuinely illegal or actionable.

89. The Defamation Act 2013 goes one step further. Section 5 creates a defence to an action for defamation for the operator of a website to show that it was not the operator who posted the statement on the website. The defence is defeated if the claimant shows that it was not possible for the claimant to identify the person who posted the statement, the claimant gave the operator a notice of complaint in relation to the statement, and the operator failed to

---

34 QQ 27, 30

35 Q 26

36 Directive 2000/31/EC on electronic commerce, articles 12 to 15.

respond to the notice of complaint in accordance with regulations made by the Secretary of State.[37] The act thus incentivises website operators not only to operate an expeditious and proportionate "take down on notice" service but also to be capable of identifying people who post statements using their websites.

90. Parliament has thus accepted the view that the liability of website operators should be limited in respect of content they host but which they have not originated. It is however significant in being the first statute in this country to link immunity from liability to disclosure of the identity of the person who made the statement. **It might well prove desirable to extend this approach to criminal offences capable of being committed using social media. It is however premature to decide until society has useful experience of its operation.**

91. Website operators are not necessarily accessories in liability to crimes. The law could be changed to clarify this.

92. Another approach might be the establishment by law of an ombudsman, funded by website operators, to set policy and consider complaints in this area. Although not a solution to every problem, it is desirable to have a well-developed system of self-policing and self-regulation.

Jurisdiction

93. It is trite but necessary to say that the global nature of the internet raises difficult questions as to jurisdiction. Facebook and Twitter offer their services across the globe, as do most social media website operators. A fundamental benefit of the internet is the way in which it has interconnected the whole of the world. Facebook and Twitter are both publicly listed companies incorporated in the United States of America which operate data centres in a number of countries but not the United Kingdom.[38] They are by no means unusual in operating in this way. When a website operator develops a technology automatically to prevent something bad, it inevitably needs to do so to some common international standard: it is not feasible that it should consider the drafting of section 1 of the Malicious Communications Act 1988. It is though feasible that every democratic state should expect automatic cooperation from website operators in relation to the detection and prosecution of crime. Similarly, there is at present inevitable uncertainty as to the ability of our courts to try offences when the person committing the offence, the host or publisher and the victim might each be based in a different country. **The only way as we see it to resolve questions of jurisdiction and access to communications data would be by international treaty.[39] The question is though relevant to many more areas of the law and public protection than criminal offences committed using social media and is politically contentious in most countries. This raises issues beyond the scope of this inquiry.**

---

[37] Defamation (Operators of Websites) Regulations 2013 (SI 2013/3028)

[38] When we asked both Facebook and Twitter to give us specific data about an element of their operations, they were unwilling to do so. We found both companies obliging witnesses but, if we had wished to press them for the data, we would have had no power to compel its release because neither company operates formally in the United Kingdom.

[39] The Data Retention and Investigatory Powers Act 2014 has sought to extend the extraterritorial effect of the Regulation of Investigatory Powers Act 2000.

CHAPTER 5: SUMMARY OF PRINCIPAL CONCLUSIONS

94. Our principal conclusions have been:

(a) **the criminal law in this area, almost entirely enacted before the invention of social media, is generally appropriate for the prosecution of offences committed using the social media**;

(b) **there are aspects of the current statute law which might appropriately be adjusted and certain gaps which might be filled. We are not however persuaded that it is necessary to create a new set of offences specifically for acts committed using the social media and other information technology**;

(c) **the Director of Public Prosecutions' guidance for prosecutions involving communications sent using social media appropriately takes account of freedom of expression**;

(d) **what is not an offence off-line should not be an offence online. There is no specific criminal offence of bullying. We consider that the current range of offences, notably those found in the Protection from Harassment Act 1997, is sufficient to prosecute bullying conducted using social media. Similarly, sending a communication which is grossly offensive and has the purpose of causing distress or anxiety is an offence under section 1 of the Malicious Communications Act 1988. Although we understand that "trolling" causes offence, we do not see a need to create a specific and more severely punished offence for this behaviour**;

(e) **we would welcome clarification from the Director of Public Prosecutions as to the circumstances in which an indecent communication could and should be subject to prosecution under section 127 of the Communications act 2003 or section 1 of the Malicious Communications Act 1988**;

(f) **due to the frequent need to obtain evidence from abroad, it would be proportionate to extend the period for the investigation of offences committed using social media to be tried in a magistrates' court to be extended from 6 to 12 months**;

(g) **a number of statutes passed before the invention of the internet refer to publications in terms only of print media. For example, section 39 of the Children and Young Persons Act 1933 restricts reporting by newspapers in relation to children involved in criminal proceedings: electronic communications and social media are not caught; we believe they should be**;

(h) **there are often calls to increase the severity of sentence available for the punishment of these sorts of offences. We favour increasing the courts' discretion in this area but we would be reluctant for Parliament to require more cases to be tried in the Crown Court (i.e. judge and jury as opposed to magistrates), due to the implications for workload. Any increase in flexibility should be carefully monitored and the proportionality of the consequences considered**;

(i) **from our perspective in the United Kingdom, if the behaviour which is currently criminal is to remain criminal and capable of prosecution, we consider that it would be proportionate to require the operators of websites first to establish the identity of people opening accounts but that it is also proportionate to allow people thereafter to use websites using pseudonyms or anonymously. There is little point in criminalising certain behaviour and at the same time legitimately making that same behaviour impossible to detect. We recognise that this is a difficult question, especially as it relates to jurisdiction and enforcement**;

(j) **from our perspective, the only way to resolve questions of jurisdiction and access to communications data would be by international treaty. The question is relevant to many more areas of the law and public protection than criminal offences committed using social media and is politically contentious in most countries. This raises issues beyond the scope of this inquiry**.

95. For those interested in our introductory quotations, they are:

(a) a "hashtag" used for linking messages on Twitter. It is in use;

(b) an example of a tweet sent to Mr Tom Daley, a diver who failed to win a medal in the 2012 Olympic Games and in 2013 announced that he was gay. Investigated but not prosecuted on the basis that it was not grossly offensive;

(c) the sender of this tweet was prosecuted for sending a message of a menacing character contrary to section 127 of the Communications Act 2003. He was initially prosecuted, convicted by a magistrates' court and fined £385 and £600 costs but, after three appeals, his conviction was quashed by the High Court (including the Lord Chief Justice) on the basis that "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 [of the 2003 Act]".[40] Accordingly, the appeal against conviction was "allowed on the basis that [the tweet] did not constitute or include a message of a menacing character";

(d) examples of a series of tweets sent by a person in response to others about a black footballer who had collapsed on-pitch with a cardiac arrest. Investigated and prosecuted as a racially aggravated offence under section 4A of the Public Order Act 1986; offence admitted; sentence of imprisonment for 8 weeks;

(e) an example of a French anti-Semitic tweet, one of many text and image tweets currently being investigated by the French prosecution authorities (cf paragraph 58);

(f) examples of a series of tweets sent by two individuals (amongst others) to a person campaigning for a woman's face to appear on a banknote. Investigated and prosecuted as an offence under section 127 of the

[40] See: http://en.wikipedia.org/wiki/Twitter_Joke_Trial - cite_note-High_Court_Judgment-27

Communications Act 2003; offence admitted; sentences of imprisonment for 12 and 8 weeks; and

(g) just to show that nothing is ever really new, a man was convicted by magistrates in 1913 under section 4(1)(c) of the Post Office (Protection) Act 1884 for sending "grossly offensive" postcards to officials in Leeds in which he described an Alderman as an "insurance swindler".

APPENDIX 1: LIST OF MEMBERS AND DECLARATIONS OF INTEREST

Members

Baroness Bakewell
Lord Best (Chairman)
Lord Clement-Jones
Baroness Deech
Lord Dubs
Baroness Fookes
Baroness Hanham
Baroness Healy of Primrose Hill
Lord Horam
Bishop of Norwich
Lord Razzall
Baroness Scotland of Asthal
Lord Sherbourne of Didsbury

Declarations of Interest

Baroness Bakewell
No relevant interests declared

Lord Best (Chairman)
No relevant interests declared

Lord Clement-Jones
No relevant interests declared

Baroness Deech
No relevant interests declared

Lord Dubs
No relevant interests declared

Baroness Fookes
No relevant interests declared

Baroness Hanham
No relevant interests declared

Baroness Healy of Primrose Hill
No relevant interests declared

Lord Horam
No relevant interests declared

Bishop of Norwich
No relevant interests declared

Lord Razzall
No relevant interests declared

Baroness Scotland of Asthal
No relevant interests declared

Lord Sherbourne of Didsbury
Non-executive Director, Trufflenet (monitors and analyses social media)

A full list of Members' interests can be found in the Register of Lords' Interests: http://www.parliament.uk/mps-lords-and-offices/standards-and-interests/register-of-lords-interests

Specialist Adviser

Lilian Edwards, Professor of Internet Law at Strathclyde University, acted as Specialist Adviser for this Inquiry.

From 2006 to present, Professor Edwards has been an Advisory Board member of both the Foundation for Information Policy Research and the Open Rights Group.

APPENDIX 2: LIST OF WITNESSES

Evidence is published online at www.parliament.uk/hlcommunications and available for inspection at the Parliamentary Archives (020 7219 5314).

Evidence received by the Committee is listed below in chronological order of oral evidence session and in alphabetical order. Those witnesses marked with * gave both oral evidence and written evidence. Those marked with ** gave oral evidence and did not submit any written evidence.

Oral evidence in chronological order

**	Gabrielle Guillemin, Legal Officer, ARTICLE 19	QQ 1–10
	John Cooper QC	
**	Chief Constable Stephen Kavanagh, Association of Chief Police Officers	QQ 11–24
*	Alison Saunders, Director of Public Prosecutions, Tim Thompson, Legal Adviser to Director of Public Prosecutions, Crown Prosecution Service	
**	Simon Milner, Policy Director-UK, Middle East and Africa, Facebook	QQ25–37
**	Sinéad McSweeney, Director of Public Policy-EMEA, Twitter International Company	

Alphabetical list of all witnesses

** ARTICLE 19

** Association of Chief Police Officers

** John Cooper QC

* Director of Public Prosecutions, Crown Prosecution Service

** Facebook

** Twitter International Company

APPENDIX 3: SOCIAL MEDIA AND CRIMINAL OFFENCES

Behaviour	Offence	DPP guidance	Time limit, if any, for investigation before prosecution	Court	Maximum penalty
Breach of court orders	Contempt of Court Act 1981	(3) Breach of court orders			
Breach of court orders (e.g. naming a person)	Sexual Offences Amendment Act 1992, s 5 (identification of a victim of a sexual offence)	(3) Breach of court orders	6 months	Magistrates' Court	Level 5 fine (up to £5,000)
Cyber bullying	Offences Against the Person Act 1861, s 16 (threat to kill)	(1) Credible threats		Crown Court	10 years
Cyber bullying	Protection From Harassment Act 1997, s 4 (fear of violence)	(1) Credible threats		Magistrates' or Crown Court	Magistrates: 6 months, up to maximum fine or both Crown: 5 years, fine or both
Cyber bullying	Protection from Harassment Act 1997, s 2 (harassment)	(2) Communications targeting specific individuals	6 months	Magistrates' Court	6 months or level 5 fine (up to £5,000) or both
Cyber bullying	Protection from Harassment Act 1997, s 2A (stalking)	(2) Communications targeting specific individuals	6 months	Magistrates' Court	6 months or level 5 fine (up to £5,000) or both
Revenge pornography	Communications Act 2003, s 127 Malicious Communications Act 1988, s 1	(4) Communications which are grossly offensive, indecent, obscene or false	6 months	Magistrates' Court	6 months or level 5 fine (up to £5,000) or both

Behaviour	Offence	DPP guidance	Time limit, if any, for investigation before prosecution	Court	Maximum penalty
Stalking	Protection from Harassment Act 1997, s 4A (stalking involving fear of violence, serious alarm or distress)	(2) Communications targeting specific individuals		Magistrates' Court or Crown Court	Magistrates: 12 months, up to maximum fine or both Crown: 5 years, fine or both
Threats	Malicious Communications Act 1988, s 1	(1)Credible threats (4) Communications which are grossly offensive, indecent, obscene or false	6 months	Magistrates' Court	6 months or level 5 fine (up to £5,000) or both
Virtual mobbing	Communications Act 2003, s 127	(1) Credible threats (4) Communications which are grossly offensive, indecent, obscene or false	6 months	Magistrates' Court	6 months or level 5 fine (up to £5,000) or both
Racial or religious aggravation	Crime and Disorder Act 1998 s 28	(2) Communications targeting specific individuals			
Disability, sexual orientation or transgender identity aggravation	Criminal Justice Act 2003 s 146	(2) Communications targeting specific individuals			