HOUSE OF LORDS

Select Committee on Communications

SOCIAL MEDIA AND CRIMINAL OFFENCES INQUIRY

Oral and supplementary written evidence

Contents

John Cooper QC and ARTICLE 19 – oral evidence (QQ 1-10)

Evidence Session No. 1 *Heard in Public* *Questions 1 - 10*

TUESDAY 1 JULY 2014

Members present

Lord Best (Chairman)
Baroness Bakewell
Baroness Deech
Baroness Fookes
Baroness Hanham
Baroness Healy of Primrose Hill
Lord Horam
Lord Razzall
Lord Sherbourne of Didsbury

_____

Examination of Witnesses

John Cooper QC, and **Gabrielle Guillemin**, Legal Officer, ARTICLE 19

Q1 The Chairman: Thank you both very much for joining us, and I apologise that we have summoned you here at very short notice. This is because we are trying to get our little inquiry done before we all go off for our very long summer recess—known to the courts as well at this part of the year—so thank you both very much. Also, John Cooper, we thank your judge for releasing you from court. We are grateful to him for allowing you time off.

John Cooper: I, too, am grateful to him. The Recorder of Manchester was most accommodating.

The Chairman: Thank you both very much for being here. I just warn you that this is all broadcast online. A transcript will be taken and then we will check the content of that with you. Can I begin by asking each of you in turn to tell us your particular background and interest in this subject and possibly push us in the direction that you would like us to go? One or other may go first, but perhaps Gabrielle Guillemin could lead off.

Gabrielle Guillemin: Thank you very much, Lord Chairman. My name is Gabrielle Guillemin. I am a legal officer at ARTICLE 19, which is an international free-speech organisation based in London. We have regional offices in places such as Brazil, Mexico, Senegal, Kenya and Bangladesh, so we work very much around the world. I have been leading the work of ARTICLE 19 on internet policy since 2011. In particular I was responsible for the third-party intervention on behalf of ARTICLE 19 in the Twitter joke trial case, following which we were closely involved in the DPP consultation on his guidelines on social media prosecutions.

As part of my work, I regularly meet with representatives of Facebook, YouTube and Google to discuss their internal policies on how to deal with hate speech online. We have also intervened in several cases before the European Court of Human Rights on issues such as

intermediary liability and freedom of expression online. We very much welcome this very timely inquiry into social media prosecutions, as we have been very worried by the increasing number of social media prosecutions in the UK. I very much look forward to discussing these matters with you further this afternoon. Thank you.

The Chairman: Thank you very much. John Cooper?

John Cooper: Thank you, my Lord Chairman. Again, I am happy to be here to assist in whatever way I can with this timely inquiry, and thank you for that invitation. I practice from 25 Bedford Row in London and have an extensive practice, both nationally and internationally, in social media related offences, accusations and, indeed, civil actions as well. As you will have seen from my biography, I have represented a range of individuals and organisations. Most recently, I have been particularly known for defending Paul Chambers in the so-called Twitter joke trial—which we may discuss as we go along in these proceedings—but also in wider aspects of the criminal law and the civil law as it impacts with social media, including the impact on jurors and the guidance that, in my view, needs to be given to jurors, which is not clear at the moment. That resulted in another case that I was defending, the case of Joseph Beard, which was the first trial in front of the High Court of a juror who had accessed the internet to obtain material he should not have had, which he communicated to his jury, causing a very expensive trial to collapse.

I have also represented a number of high-profile celebrities and sportspeople—whatever the word "celebrity" may mean nowadays. I am presently representing a number of politicians—you will be relieved to know they are international politicians rather than national ones—in relation to transgressions that may have occurred against them and their family. Attacks on people on social media also have an impact on others, such as children, and I am involved with a case where a child was brought into the issue as well. So the wider aspects of attack may be of interest to this Committee. I was previously a co-editor of the *Encyclopaedia of Data Protection and Privacy* so I may be able to assist where that interacts with our discussion.

Very briefly, in the one minute I probably have left, I would like to emphasise that the social media is still a very young media. The criticism that is sometimes given that the law does not react properly to it is, I think, at times not aimed fairly. Let us remind ourselves that Facebook was invented only in 2004 and Twitter a few years later. So, although we are a little behind the step, I do not think we should be castigating ourselves too much. The law often needs to catch up. That said, in conclusion, the law should catch up. I am of the view that there are too many disparate statutes in existence at the moment, which can be amalgamated. Whether they can be technologically neutral is another matter. Perhaps the answer is to amalgamate statutes that generally deal with harassment, stalking and threats, and conclude that that confusion needs addressing rather than focusing particularly upon a social media statute.

Finally, on a note of positivity, 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. I would perhaps like to make that plea when we discuss issues: social media is a power for good but, like all society, sometimes people abuse it.

The Chairman: Thank you both very much for those important introductions.

Q2 Lord Horam: Let me start at a very basic level by asking you: what sort of offences are there? Is there an acknowledged classification of offences, and how would you define them?

John Cooper: My goodness me, I am conscious of the time that your Lordships have to deal with this—

The Chairman: Briefly.

John Cooper: Absolutely, but I do put a rider to that, that it will be the stuff not of a lecture but of a course. Let me try to give your Lordships an idea of where we lie here. The Protection from Harassment Act 1997 is an important statute that deals with stalking and intimidation. That Act deals with patterns of behaviour. For there to be a successful prosecution under that statute, the prosecution will have to satisfy the court that there are specified acts that have occurred on at least two occasions. The harassment Act deals with courses of conduct. They can be courses of conduct directed at victims or, indeed, as I touched upon a moment ago, include actions directed at people connected to victims. The harassment Act can encompass family relationships as well.

The 1997 Act now encompasses social media behaviour. Again, I think it is interesting to note that it comes from 1997. Every single Act that I think we will discuss today pre-dates the social media—every single one, and some significantly so—and the harassment Act is one of them. The harassment Act is constantly being updated. By an Act of Parliament in 2012, which was only recently enacted, two new sections were added to the harassment Act—sections 2A and 4A—which increase potential prosecutions in relation to stalking and add a more serious offence of stalking involving fear of violence, and serious alarm and distress. That is the harassment Act.

Of course we have something that is very much in my mind now after the Chambers trial, which is the Communications Act 2003. The Communications Act 2003, section 127, deals with an individual who will be guilty of an offence if they send by means of—and, again, listen to the terminology—"electronic communication". Even in 2003, this was pre-social media and did not even have social media terminology. It deals with "menacing" messages or communications that are "grossly offensive or of an indecent, obscene or menacing character". Let me put that Act in context, so that you can understand the level of that Act. Consider for a moment the Paul Chambers case, because it does help to understand how far that Act goes or does not go. You may remember that in the so-called Twitter joke trial Paul Chambers was prosecuted for the following expression: "Robin Hood Airport is closed. You've got a week and a bit to get your"—and I will leave the expletive out—"together, otherwise I'm blowing the airport sky high!" Finally, after seven court hearings and a lot of public money being expended, the case was thrown out by the Lord Chief Justice, Lord Judge, as he then was, because it was considered by this court that what Chambers said was not of a menacing character. As I put it to the court at the time, had that been of a menacing character, John Betjeman would be turning in his grave when he wrote, "Come, friendly bombs, and fall on Slough!" That really brings home the limits and the parameters of some of these statutes.

I will rush on, because I do not want to take up too much more time. There is also the Public Order Act, for instance, which we should consider. You may be surprised to hear that all the other statutes that I have mentioned so far do not have an element of racially aggravated offences or religiously aggravated offences. The harassment Act, the Malicious

Communications Act—which is another statute that I have yet to mention—and the Communications Act do not have racially or religiously aggravated sections in them.

As you may remember, there was the Fabrice Muamba matter, in which tragically—thank goodness he lived—a black footballer collapsed on the football field with a heart attack and the appalling element in social media came to the fore and the poor man was racially abused on the social media. As I recall, it was section 4A of the Public Order Act 1986 that was used to prosecute that culprit. Again, that is an example of old statutes—1986 in that case—being used. It is a little bit like what happens to airplanes in time of war, when suddenly you get a civilian aircraft that you need to build up into a fighting craft in a panic situation and make effective, or when a cruise liner all of a sudden needs to become a troop-carrying ship. That is a good analogy, if I can use it, for some of the statutes that we are using for social media.

I will stop there, but for the avoidance of doubt—because I know we are being recorded and I do not want people screaming at me on the social media, "He did not mention the Malicious Communications Act"—there are other Acts as well and I could go on. So for anyone that might say later that I did not mention them, I know they are there.

Lord Horam: Thank you, Mr Cooper. Is there anything you would like to add to that, Ms Guillemin?

Gabrielle Guillemin: Yes, thank you, my Lord. I agree with John's analysis of the UK law on social media offences, but I thought it would also be helpful to give you a brief outline of the position in international law.

International law clearly provides for restrictions on freedom of expression, in order to protect people from threats of violence as well as from hate speech where it involves incitement to discrimination, hostility or violence. International law also requires the state to take measures to protect people from harassment. These are all areas in which the state can legitimately impose proportionate restrictions on freedom of expression. What international law also says very clearly is that merely being offensive, without the threat of violence, is not a legitimate basis for restricting freedom of expression. I think this is something that is very important to bear in mind, which was highlighted in the DPP's guidelines on social media prosecutions. He made several references to the standards elaborated by the Strasbourg court in this respect—namely, that freedom of expression also protects expressions that offend, shock or disturb.

The Chairman: Thank you very much. You draw the important distinction that the threat of violence, if added in, changes everything.

Gabrielle Guillemin: Yes.

The Chairman: That is really helpful.

Q3 Baroness Hanham: On the subject of violence, can that be a threat of psychological violence as well, or does it have to refer to physical violence?

John Cooper: Psychological violence is part and parcel of the consideration. It is particularly part and parcel of the consideration when it comes to section 4A, stalking, under the new provisions under the harassment Act, but what is marked is that that is only very recent. Thank goodness that has been brought in because—you make this absolutely valid point—a lot of social media attacks are psychological. That is one of the problems we have in terms of bringing the law up to date and it is relevant to your question.

The Anti-Social Behaviour, Crime and Policing Act 2014 describes anti-social behaviour as, "conduct that has caused, or is likely to cause, harassment, alarm or distress to any person". It does not have a definition for anti-social behaviour on the social media. In my opinion, the public's definition of anti-social behaviour relates to noisy neighbours or "hoodies" in supermarkets and precincts. The definition of anti-social behaviour, as presently before us in legislation, does not deal and grapple with anti-social behaviour on the social media. In my opinion, we need to provide clearer definitions of social media relevant anti-social behaviour, which we do not have at the moment.

Q4 Baroness Hanham: Thank you very much. That was not my question but a short intervention. Let me just flick the coin over and go from the other side. We have been talking about legislation, where clearly a lot of it is not related to what is happening now, but is there anything within it that—and you may have touched on this—if there were changes, you would not want to lose because it works?

Gabrielle Guillemin: First of all, I am not aware of any significant problems in the operation of the Offences Against the Person Act 1861 or the Protection from Harassment Act 1997 in terms of freedom of expression. Obviously, the law should continue to protect people from harassment, threats of violence and hate speech, by which we mean incitement to violence, discrimination or hostility. In relation to psychological violence, I would urge caution because, when the Act refers to anxiety and these very subjective feelings, that is actually the problem. With psychological violence, it is eminently subjective to each person and how they feel about the attack.

Going back to how the law works and what works well, one positive feature of the current legal framework is the DPP guidelines on social media prosecutions, which were very much welcomed at the time. That said, we hesitate to say that this is an area where the law is working well because, as we have seen, there have been a large number of prosecutions where the guidelines are still not working as effectively as they should. The main problem is the fundamental lack of clarity on the tests to be applied for what the DPP described as the "fourth category" of cases; namely, those to do with grossly offensive comments. By and large, we thought the intention behind the guidelines was a good one; they were generally sensible and we would certainly encourage the spirit of the guidelines to be taken forward if there was reform forthcoming in this area.

John Cooper: I have to disagree.

Baroness Hanham: Oh good, the first conflict.

John Cooper: I have never found—and I have written and spoken in public arenas—that the guidelines are anything other than, as I refer to it, the longest definition of common sense that I have ever read. There are 25 pages. It is no secret that I say this, as Keir Starmer and I have debated this on a number of occasions with a varying degree of heat—that is good, as that is what debate is about.

One of the problems in the Twitter joke trial—and it is not just the Twitter joke trial but generally—was the understanding of the prosecutors as to what the present law is. The social media community, I emphasise again, is a young community. I do not necessarily mean young in age, although it is sometimes, but it is a new community and it is getting to grips with what it should and should not do. There are always transgressors, but people are getting to grips with what they should and should not do, and there is a high degree of self-

policing among leading commentators, such as David Allen Green—#CarefulNow—on certain issues that were of pressing legal interest to the courts at the time. That is an example of internal policing, if I may put it that way.

In my view, one of the problems is the understanding of the law by the Crown Prosecution Service. Without doubt, there are people there who are extremely specialised and competent. On the other hand, there are those who simply do not understand the social media. With the Twitter joke trial, the fact is that the police, the airport security services and all those sections thought it was a poor, crass joke but not a criminal offence. It was only prosecuted when it got to the Crown Prosecution Service with an utterly misconceived interpretation of what the law was. The DPP guidelines perhaps make people feel good about things and common sense is being articulated, but it should not have to be articulated. It worries me that the level of understanding of the law at the Crown Prosecution Service level certainly was not what it should have been two years ago. Perhaps it has improved—I do not know. You may be hearing from people from that section, so I had better leave that to one side.

Q5 Baroness Healy of Primrose Hill: How do you think this problem can be resolved? I can see what you are saying that the prosecutors do not understand what laws to use, but what do you think would be the best way as opposed to 25 pages of guidelines? Are there any other solutions?

John Cooper: Reading a few law books? I do not mean to be flippant, but it happens to us all—lawyers, doctors or whatever profession you are in—that we read a lot of books when we are training and then, sometimes, when you get into the cut and thrust of practice, you tend not to continue professional education as significantly as you should do. I do believe that there should be professional development training in these areas. No doubt there is, but there should be more of it. It is all down to training and understanding, but it is all down—and I use the words advisedly—to common sense. Let us forget that it is social media. When I am advising clients and they say to me, "Can I say this on the social media?", I say, "Well, would you say it to an assembled number of 10 or 20 people in public or perhaps to even less? And if you would not, then do not say it on the social media". The social media is simply a platform for human beings to behave or misbehave.

Baroness Healy of Primrose Hill: You talk about training, but they should all be using the social media.

John Cooper: Yes, and more and more people are. It is amazing. Speaking from my experience at the Bar—Baroness Deech may have a similar experience—when we first started using social media as barristers, I recall that many of us were thought to be reliving our own youth in a rather unseemly way. That was about a year or so ago. Now the tweeting at the Bar is so loud it is like an aviary, and I speak only for the Bar. In answer to your question, I think there is more of an awareness now that it is done by all people—perhaps I may encourage your Lordships, if you do not already tweet, to do so. As I said at the top of my opening statement, it is an important, positive and inspiring arena, and I would like to keep that atmosphere going here if I can. It is only like society and it is a medium that, for instance, drove the Hillsborough initiatives and drove a number of other public profile initiatives to put them in the public eye, so that we do have inquiries, some of which your Lordships sit on. The social media has been responsible for that as well.

Q6 Lord Sherbourne of Didsbury: So that I am clear, can I ask Mr Cooper and Ms Guillemin: are we saying that the laws that are not technically specific, in terms of technology specific, are sufficient without having to have legislation that particularly identifies the social media technology? That is question one. Question two is: given the mass of communication now on the social media, do people who themselves feel victims in some way—they will not be lawyers but they may well feel victimised—have sufficient means to understand what recourse they have to law to protect themselves?

Gabrielle Guillemin: First of all, on the question about the nature of the law and whether that should be technology neutral, I would like to go back to section 127 of the Communications Act 2003 and section 1 of the Malicious Communications Act, which both refer to the "communications network". I do not think that the main problem here is that they are not technologically specific; the real problem is that the meaning of "the public electronic communications network" and "electronic communications" has changed over time. For example, 100 years ago we could have said that an electronic communication might have been the telegraph; 50 years ago that would have been the telephone; 20 years ago we had pagers and now there are e-mails, Twitter and Facebook posts.

The point is that all these involve electronic communications, but the underlying context of the medium has changed. People go on to social media and have very casual conversations on Twitter in the same way that they would down the pub. Some of the analogies that these rules were designed for no longer hold up, such as, for example, nuisance phone calls. On the whole, we tend to think that it is better for the law to focus on the harmful nature of the action itself and not the misuse of a communications network. Generally speaking, when looking at how to deal with the problems that arise from internet communications, I think it is always very important to bear in mind that specific approaches might have to be tailored to the internet. This is something that we are seeing a lot of in different areas of the law, for example defamation or copyright. We see where copyright authorisation was necessary in the offline world but now it is potentially applicable to all sorts of acts online. It is very important to remember how we would also behave in the offline world.

Secondly, as far as victims are concerned, obviously this is a very serious issue but one thing I would like to remind the Committee—and something that I think should be emphasised with internet users in general and those who use social media, in particular—is the tools that are available to them on these platforms. There is a range of technological tools that are available. It may well be that they are not sufficient and, if matters escalate, it might be necessary to bring in the criminal law for, what we have been talking about, threats of violence or harassment. But these tools are available, such as privacy settings on Facebook or having a private Twitter account.

John Cooper: It is important to make clear that there are no new offences committed on the social media. The social media has not invented new offences. Harassment is an old offence. Stalking is an old offence. Defamation is an age-old offence. Threats, be it to kill or otherwise, are all old offences so I cannot think—and I would be interested to debate with anyone that possibly can posit something—of any new offence that has been created by the social media. So where does that—

Q7 Lord Sherbourne of Didsbury: Just on that point, take the example of porn revenge. Let us suppose that one particular male sends to one friend what would be a very private photograph or video of a personal, intimate nature with his former girlfriend, which is sent

to one friend only. If after that it goes viral, because of the friend rather than the person who originally sent the e-mail, where does the culpability lie there?

John Cooper: Again, all cases are fact specific, but if you send something out that is limited to the one individual that you send it to, and you are not involved with the dissemination of it, then there is no culpability there as far as you are concerned. But there are so many myriad ways of sending things on the social media—for instance, you could send it on Twitter in such a way that it could be picked up by your followers.

Lord Sherbourne of Didsbury: It is not an offence anyway to send some very intimate photographs that might be how an innocent person—

John Cooper: Yes, it is. It is indeed an offence to send any form of obscene picture and broadcast it, if it is in such a way so obscene in accordance with the legislation to breach that legislation. Again that is an age-old offence. In fact, it is an interesting exercise—which I probably will go through when I finish giving evidence here—to try to work out whether there is a new offence created by the social media. There are new problems created with the dissemination of that offence by the social media.

One other thing I would just want to touch upon here is the issue of jurisdiction. One of the problems the social media does create is sometimes where a case can be prosecuted or, alternatively, if it is a civil action, where an action can be brought. Where does the action begin? For instance, if something is sent from America and it libels someone over the social media in this country, there is a debate at the moment still going on in the law courts about where the cause of action will arise. One of the real problems within social media and criminal or civil enforcement is jurisdiction or jurisdictional points—there are extra jurisdictional issues. That is new or, if it is not new, it is becoming more and more of an issue. However, that is not a new offence. That is a new problem with proving the offence. That I think is the real problem we have to grapple with.

As far as victims are concerned and how to deal with matters, in my opinion the problem here is an issue of policing. On the whole, the police do an amazing job with social media issues. They have become inundated in the past with problems relating to social media, and it comes back to the point I made to your Lordships a moment ago about anti-social behaviour. The public do not understand what anti-social behaviour is in relation to social media, and the police are being inundated with spurious complaints that they should not be bothered with. There is a funding issue with the police as well, because they cannot investigate every transgression on the social media. In my opinion, there needs to be education, particularly of the general public, as to what amounts to a transgression of anti-social behaviour on the social media, so that the police are not inundated by these complaints that cannot be proceeded with under police investigation.

When there are more serious allegations being made, the police do step in. In fact, only last week a senior police officer issued some guidance and directives as to how officers should deal with these matters and, I think, over 6,000 officers are now being trained to recognise serious social media offences. In answer to the question a moment ago relating to victims, the public do need to be educated, as far as social media is concerned, as to what is an offence and what is an unpleasant freedom of speech—that might be an issue you want to take up in a moment. The police also need to be assisted by the general public and probably provided with more training themselves and—an age-old plea—they would say for more funding as well, but in the present day and age that may not be possible.

The Chairman: We are seeing them next week.

John Cooper: That will be interesting.

Q8 Baroness Bakewell: Picking up on what you said about what is possible within the laws as they exist, are there any conspicuous gaps where action does need to be taken? For example, does there need to be a new means of dealing with something like a Twitter storm that simply assails one person with millions of tweets and presents what is in fact a new kind of offence, is it not, by sheer abundance?

John Cooper: In my opinion, if properly employed, the present legislation is able to deal with the Twitter storm example that you gave a moment ago. The harassment Act 1997—with the new amendments that I mentioned, section 4A in particular, which only came into force about a year ago—deals with stalking involving fear of violence, serious alarm and distress. It deals with a series of events and it deals with issues that relate to continual harassment of the nature that you raised. In my opinion, the present legislation, which protects people generally in society—with perhaps the amendments that have been made and Parliament has enacted in sections 2A and 4A—is equipped to deal with the real problems that you have raised.

Baroness Bakewell: There are two things going on here, are there not? All those things that you have mentioned—stalking and so on—that are covered by the Act are seen as a one-to-one offence, but something else is happening if there are millions of people assaulting one individual. Is that not a different kind of offence?

John Cooper: It is an escalation of the same offence.

Baroness Bakewell: Into a different drama almost?

John Cooper: Into more seriousness and more culpability, but the legislation—particularly the legislation I have spoken of—is equipped to deal with that as well. If I may put it this way, what the social media has done is it has increased the velocity of a crime and perhaps made it more available to more people to commit, but in my opinion that does not mean that the legislation is not there to deal with it.

Baroness Bakewell: But the person who threatened Robin Hood Airport—

John Cooper: Robin Hood Airport, yes.

Baroness Bakewell: —was one individual and could be found and prosecuted. How do you deal with 5,000 people attacking one person?

John Cooper: If that is the case, they are identifiable. If they are identifiable, then they are available for investigation. You do raise an issue of where people are not identifiable, where they employ anonymity and where they go under pseudonyms. Until very recently, there have been problems with that. There is a procedure called the Norwich Pharmacal procedure, which is now being deployed with more alacrity by lawyers. That is a procedure—without going into too much technicality—that can force third parties, such as Twitter, Facebook and others that provide platforms, to provide the names and details of people who skulk, if I may use that expression, under anonymity. I am not trying to say that what you raise is not a real issue, but what I am suggesting is that we have a panoply of law that is able to deal with it. The issue that I would raise is whether there are too many Acts of Parliament and whether they should all be amalgamated into a general Act of Parliament

dealing with all aspects of harassment, stalking and threats such as this—not in relation to social media but in relation to a general amalgamation of remedies and charges under one statute. When you look at the range of statutes that a lawyer, or more particularly a victim, needs to look at when they get a threat, you are looking at a range of statutes in the Public Order Act 1986 and the Malicious Communications Act and so on.

Baroness Bakewell: Can I put this to Gabrielle? What is the international or global situation for a Twitter storm involving prosecuting people across national boundaries?

Gabrielle Guillemin: Here generally I think we would go back to national legislation. We would think that as the law currently stands, with the Protection from Harassment Act, there is enough to go on under this particular Act. We would caution against expanding the definition of "a course of conduct" under the Act to cover those situations where a person who receives a lot of abusive messages, in circumstances where each individual sends only one message. Even though there may be one person at the end receiving thousands of messages, we are still looking at a number of people involved. We do not think it would be a good use of public resources if we were to suddenly change the law to say that every time there is an abusive message that does not amount to a course of conduct potentially all these different people should be prosecuted. Of course, there would be other issues related to anonymous speech, but this is the reason why we think the law should not be amended to expand "a course of conduct".

The second point we would make here goes back to what I was saying earlier about user settings and how people can also learn how to defend themselves online using those tools. Equally, I think it is important to bear in mind that, ultimately, one of the features of social media is that they are fairly addictive. People tend to go on to them to see what happened and how people reacted to what someone has said. The reality is that nobody is forced to go on to Twitter. Of course, there is a lot of abuse that may be very unpleasant, but that does not mean that all of it is illegal. We have to be very careful to distinguish between what is legal and what crosses the line, such as threats of violence, harassment or hate speech.

I would just like to go back to the conversation we were having earlier about revenge porn. One thing that we would say in relation to that is that we are seeing a lot of legislation—for example, in the United States—to address this particular issue, but we would question whether it is for the criminal law to get involved in what is very often the fallout of failed relationships and whether civil remedies are not more appropriate to deal with these kinds of issues.

The other point I wanted to go back to is the DPP guidelines. It was a good point of departure, but clearly it has not quite worked because the police and the public are still trying to understand what it means. I think the real difficulty, and what we have heard recently from Chief Constable Marshall, is that what they are trying to figure out is when an insult becomes a criminal offence. For us, the real issue has to do with this fourth category of grossly offensive messages because the standard itself is not clear. That is the real problem because it is eminently subjective and, therefore, unclear. What we believe is that individuals should not be prosecuted for saying things that may be grossly offensive.

John Cooper: I cannot overestimate the need, in my opinion, for there to be a bringing together of the legislation. Let me give you another example. Sexual harassment is not covered by the harassment Act. It is covered, of course, but it comes under human rights legislation and under the Employment Relations Act 2000. That is another example. I

touched on another example earlier on in our discussions: racially aggravated and religiously aggravated threats and harassment are covered only under the Public Order Acts. In my opinion—and this is not looking quite into the minutiae of the work that you are doing—it is critical to emphasise that there is a mishmash of very important, enabling legislation. I am not as critical as Gabrielle, but I respect her views and very much respect Gabrielle and her organisation. The issue for me is not so much the faulty nature of the existing law but the fact that it is coming at us from all angles.

If we go back to the initial problem, in my view that is the public understanding and the understanding of the police and the Crown Prosecution Service of what powers they have and what transgressions may occur. There needs to be a root and branch reorganising and re-legislating of the harassment and stalking legislation, not to change it but to bring it together in the same basket. That may be out of the ambit of your Lordships' inquiry but none the less I touch upon it.

Q9 Baroness Deech: You have virtually answered my question 7, but having listened to the two of you I am beginning to change my mind and have other thoughts. Given the amount of time that it takes to change the law—if we imagine that this Committee recommended a consolidation and a clarification—it could take five years or more. Then you look back and you say, "Ten years ago the laws that we passed did not foresee the situation now". I fear that we might be wasting our time if we work away on consolidating the law now and that, by the time we change it, there will be something else brand new that we have not thought of and do not see now. So I am not sure about that. You yourself said that the social media is very young and is still developing. So I am not sure about that anymore, although an hour ago I might have said, "Yes, we need to consolidate the law".

The other thing that worries me very much is we have been bandying around the phrase "freedom of speech", and I am beginning to think there is not much of that left in this country—I do not know how it compares with others—given the number of laws that we have, many of which are broken. I am not so sure anymore that we should go further in this respect. I wonder if there is a link with press regulation. Everyone is rushing to say, "Oh, the press must be regulated", and that could lead us to more constraints on freedom of speech. Some of the same people said, "There should be more freedom on Twitter", and people who back, for example, Snowden and Assange do not like hacking. I think there is a confusion—but perhaps it is just in my mind—between what is permissible and what is not. I hope that this Committee might get to grips with the very big topic of what exactly freedom of speech is.

I am going off target a bit, but I saw this film not long ago that is now more than 50 years' old, which I think was called "Beyond the Fringe", with Dudley Moore. Jokes were being made—and I dare not use the words now, as we are being broadcast—about ethnic minorities, the disabled and racial minorities that we would never, never permit or contemplate today, and I am not sure whether we have moved in the right direction or not.

John Cooper: It is interesting, and I know Gabrielle will have very strong views on the freedom of speech issue. I was talking to Gabrielle outside this Committee. I am a living, breathing example of the conflict between social media and freedom of speech. On the one hand, as I indicated at the start, I represent individuals. You may or may not know that I also represented the occupiers outside St Paul's Cathedral arguing for their right of freedom of

speech. So I see the arguments and the debates from both sides. Freedom of speech is important, but of course it is not an absolute right and, therefore, it has to be balanced—and human rights jurisprudence bears this out—with other important rights and issues as well.

Going back to some of the arguments we had during the Chambers appeal, I would say that freedom of speech is not just freedom to be nice or freedom to be unobjectionable; freedom of speech is the right to be objectionable, and it is right that people have the right to be objectionable. In my view, one has to draw the line and the balance that we draw in society, so it is not a social media problem. The balance needs to be struck of when one goes over the limit.

Carrying on with Baroness Deech's train of thought, I think that what social media adds on freedom of speech is the fact that it goes further, wider, quicker and faster. In that respect, that is when we have to come back to the law to control it.

Baroness Deech: I am not even sure of that. Lady Bakewell raised the issue of lots of people or thousands of people being offensive to one person. On a slightly smaller scale, I know of instances where an entire lecture hall or an entire theatre can howl down one speaker. There is apparently no legal remedy for that. Of course, an offensive statement in a newspaper will very quickly reach all over the world, so I am not sure it is anything different.

John Cooper: The Malicious Communications Act 1988, for instance, was an Act that was used during the Tom Daley incident. You may recall that appalling series of events where Mr Daley, trying his best, did not achieve a medal in the Olympics. As a result of that, he received a torrent of abuse, particularly from one individual, including threats to drown him.

Baroness Deech: Gabrielle, I may have cut you off, I am sorry. Were you about to say something?

Gabrielle Guillemin: No. I would like to respond to the question in general, but I—

John Cooper: I will limit myself to saying: there was an example of statute used against one individual who attacked one individual, but Gabrielle has something to add.

Gabrielle Guillemin: Thank you very much. First, going back to the question about consolidation, we understand that it would be desirable and it would be welcome. At the same time, we recognise that it is difficult to find parliamentary time to do this. In our view, a simple and important way of fixing this would be to remove "grossly offensive" as a means of criminalising what people say online, which may be extremely unpleasant but does not amount to a threat of violence or harassment or hate speech in the sense of incitement to violence, hostility or discrimination. In a way, that would be a simple fix.

To go back to how freedom of expression is exercised on social media, I think we find very interesting parallels in relation to defamation. For instance, a case that we are intervening in, in Strasbourg, which is called Delfi AS v Estonia, concerns comments that were made below a newspaper article on a matter of public interest in Estonia that had to do with ferries and roads to get access to various islands. These comments were offensive, but many leading lawyers in this country, looking at this case, were surprised because they thought these comments would be thought too trivial to amount to defamation in this country. However, what happened in the Estonian court was that the news portal was asked to remove the offensive messages. They were removed immediately, but the news portal was still found liable for the comments. The point here is that very often on social media, for example, in relation to these comments, they may be abusive but the way in which the law

could address this is by treating it in the case of defamation as too trivial to warrant the case going before the courts. In many ways, this is now a possibility because there are various technological tools available to internet users.

Also, I think there was a very important remark made by Mr Justice Eady in the Smith case about the nature of these communications online. What he said was that they were "rather like contributions to a casual conversation … which people simply note before moving on"; "they are often uninhibited, casual and ill thought out"; and "those who participate know this and expect a certain amount of repartee or 'give and take'". So, again, it is very important to bear in mind the context of online communications here.

Secondly, I would like to go back to a comment that was made earlier regarding what sort of advice should be given to someone who wants to go on Twitter. It is true that someone with legal training would probably advise them to be careful in what they say because they might get caught by the law, but for us here that becomes a problem. We operate in many different countries and so it becomes very difficult, especially with authoritarian, non-democratic Governments because, when you are talking about something that is offensive, that could be many different things and involve a criticism of politicians, for instance. One of our concerns with legislation—for example, with section 127 of the Communications Act in particular—is that, when we are having conversations with internet or pro-democracy activists around the world in countries such as the Gambia or Azerbaijan or even Tunisia, they tell us it is very difficult for them to push for reform because their Governments immediately say, "Look at what they are doing in the United Kingdom", so that makes our work somewhat harder, too.

The other thing I want to record very briefly is that under international law, of course, freedom of expression is not absolute. But because it is such an important right, and the foundation of democracy, any restriction on this freedom should be very narrowly drawn. We think this is a very important thing to bear in mind, especially in the context of social media. Of course there is a lot of abuse and a lot of bad things that happen there, and it is perfectly legitimate to have legislation to address some of these problems, but at the same time social media has allowed public debate to take place. For example, it is not just confined to news articles. People can really engage. So we should be careful when thinking about enacting legislation not to diminish what has been a great gain, in terms of our democracies and being able to engage in matters of public debate.

The Chairman: That is really helpful. We only have a minute left of our time and I do want to hear a final question from Baroness Fookes.

Q10 Baroness Fookes: There has been a suggestion in the Commons, in the current Criminal Justice Bill, that the penalties should be made harsher. Is that something that either of you would favour?

John Cooper: The penalties generally range across the statutes. If one leaves out threats to kill, for instance, under the Offences Against the Person Act 1861, and just deals with the other offences, the average maximum is about six months' imprisonment. I think the suggestion in the House of Commons is to increase it to two years or so.

Baroness Fookes: Particularly, I think, in the case of cyberbullying.

John Cooper: Indeed. I have no concern that the parameters of sentencing be increased. It will enable the courts and the judge, upon conviction or upon a plea of guilty, to have a

wider range of expression to take into account serious transgressions on the social media in particular in relation to cyberbullying. I would also say this: define cyberbullying. There is no criminal offence of bullying presently on the statute book. For instance, I do not think bullying should necessarily be criminalised. If it was, I think a lot of barristers might be making complaints every time they go into certain courtrooms. The fact of the matter is "bullying" should not be the expression used in any event for this increase in sentencing.

Baroness Fookes: But you can find something that would do the trick in one of these many Acts?

John Cooper: Yes. That is why I am treating your question by taking out the expression "cyberbullying" because that would end the debate for me. I do not think sentences should be increased for cyberbullying—I do not even recognise that offence. But I do think that the penalties could be increased. Some of them are effectively low level fines anyway, and the variation of transgressions across the social media does demand an answer, to give a judge flexibility in doing so, whether or not it is prosecuted.

Can I be cheeky and just for 10 seconds link into this just on the "grossly offensive" point? I disagree. In my view "grossly offensive" can remain, but I would adopt what the DPP said, "If in the public interest to pursue". In his assessment of what could be prosecuted, the DPP did include "grossly offensive" but added "If in the public interest". I would like to leave the courts with the powers that they have. I would agree that the sentencing parameters should be increased to give the flexibility to judges. But the key here is providing the courts, the police and society with the tools but—goodness me—not forgetting common sense and discretion as to how to use them.

The Chairman: Thank you very much. I think, Gabrielle, we might be able to end on a note of disagreement, might we not? Would you feel as supportive of Angie Bray MP's suggested upping of penalties?

Gabrielle Guillemin: We would most certainly favour more education and restorative justice measures, especially bearing in mind that in a lot of these cases we are talking about young teenagers who are still learning and still making mistakes. We believe that in those cases it would be preferable to have education over longer imprisonment, essentially.

I would like to go back very briefly, if I may. I think we are going to have some disagreement about "grossly offensive". Of course there are always going to be cases where everybody agrees that something is grossly offensive. For example, I would certainly agree that someone applauding the horrendous death of a teacher completely gratuitously is grossly offensive. But our concern is that in most cases "grossly offensive" is not a standard that would be sufficiently certain to provide the necessary degree of legal certainty for people to be able to regulate that conduct online, which is why we believe that the standard itself should be removed from the statute.

The Chairman: Thank you. We did end on a little bit of controversy there. Thank you both very much indeed, and for coming at short notice as we said. Thank you.

ARTICLE 19 and John Cooper QC – oral evidence (QQ 1-10)

Transcript to be found under John Cooper QC

Association of Chief Police Officers and Crown Prosecution Service – oral evidence (QQ 11-24)

Evidence Session No. 2 *Heard in Public* *Questions 11 - 37*

WEDNESDAY 9 JULY 2014

Members present

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

_____

Examination of Witnesses

Alison Saunders, Director of Public Prosecutions (DPP), **Tim Thompson**, Legal Adviser to the DPP, Crown Prosecution Service, and **Chief Constable Stephen Kavanagh**, Essex Police on behalf of the Association of Chief Police Officers

Q11 The Chairman: Welcome. Sit yourselves down and let in any guests that are joining us. Before we get into our session, I need to ask my colleagues to place on record any interests that they feel they should declare, so would any of my colleagues like to?

Lord Sherbourne of Didsbury: If I can declare my interest. I am an unpaid non-executive director of a company called Trufflenet, which monitors and analyses the social media and the traffic on them.

The Chairman: Thank you very much. Welcome to the three of you. Thank you very much indeed for coming. We have arranged this at very short notice and you have been incredibly obliging so we are extremely grateful. It is not easy, I know, in people's busy, busy diaries. We are going to be televised on the new media, I suspect, rather than broadcast to the nation, but you need to bear that in mind. Each of my colleagues will be asking you questions. Feel free to answer a question put to one of the others on the panel, or not. If you do not feel you have anything to add it is not compulsory for everybody to answer every question. So with those preliminaries could I ask, Alison Saunders, if you would very kindly explain the position from your perspective on social media offences and the CPS—where you are coming from, in the extraordinarily important role that you have, and how you see this big issue that now has gained a lot of publicity even just recently?

Alison Saunders: Yes. Thank you very much for inviting me here, first. It is an important topic for us to consider. I have been Director since November last year, but I have been in the service since 1986. I am well aware of the guidance and the way in which we have dealt with social media cases and, indeed, I have dealt with some myself.

It might be helpful if I just outline how we generally make our decisions before dealing specifically with social media, because we make our decisions—all decisions, whether they involve social media as evidence or not—in accordance with the *Code for Crown Prosecutors*, which is a document that is laid before Parliament. We have a test there that all cases have to comply with, which has two limbs. The first is an evidential test, which means we must be satisfied that we have sufficient, reliable and admissible evidence that provides us with a realistic prospect of conviction. That means that a jury or a Magistrate if properly directed is more likely than not to convict. So, no matter what the case involves, whether it is social media evidence or any other type of evidence, it must, first of all, pass that evidential test. If it does we then go on to consider whether or not it is in the public interest to prosecute, because it has never been the case that just because you have evidence it will always be in the public interest to prosecute.

We set out in the code some examples of public interest considerations that we might take into account. So, for example, 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 if they are a particularly vulnerable victim. So we will consider those sorts of things, and only if the evidence passes the evidential test and we think it is in the public interest will we prosecute cases, and so that will apply to the cases that we might come on to talk about later on today.

As well as looking at the code, what we have done is that we have identified particular categories of cases of offending that we think that prosecutors could do with some extra guidance on, over and above the *Code for Crown Prosecutors*. So we have them for a number of different offences as well as some procedural issues, and that is just used as an aid for prosecutors to point them in the direction of things that they need to take into account, considerations that they need to have or particular legal issues that they need to have at the forefront of their mind.

As you know, we have decided in the service that there was a category of evidence in cases involving social media that cause some particular difficulty, so in December 2012 my predecessor decided that we should have some guidance. I am pleased to say we also consult widely now on guidance that we are about to issue to prosecutors. So in December 2012 he issued some interim guidance to prosecutors and also consulted on it widely, and we had about 59 different responses from various individuals, bodies and organisations that had comments on the guidance. This guidance was then further published in its final form in about June 2013.

The guidance gives prosecutors some practical guidance about the sorts of offences that we might come across involving social media, the issues in gaining evidence, the types of offences and when you would use the types of offences, and in particular when certain categories of cases needed to be referred to either the Chief Crown Prosecutor of CPS Direct, which is the organisation that does most of our charging offences, or to the Director's private office. In the guidance we based it around four different categories of offending where social media might be involved. So it was communications that amount to credible threats of violence, a targeted campaign of harassment against an individual, breaches of

court orders or statutory provisions, and other cases that may vary widely. This is the one that really causes the most concern and that I think you have already dealt with in some of the evidence that has been before you, and this is the one where the contents of communications may be considered to be grossly offensive, indecent, obscene or false, and those are the ones that for prosecutors can quite often be the most challenging cases.

We have issued guidance in relation to that and certainly oversight of that last category of cases is quite strong, and it has been centralised so that we can make sure that there is consistency of the application of both the guidance and the principles, and we prosecute those cases where we really should be prosecuting.

As a matter of interest to the Committee perhaps, we do collect data on offence type. So for the Malicious Communications Act, section 1 or section 127 of the Communications Act, we have routinely collected data about what sort of numbers we have. Since 2012 we have seen the numbers of prosecutions falling in relation to those, which is after the guidance has been issued. We cannot tell if those are social media cases or not because they may be other types of communication that falls within that offending, but it is perhaps worthy of note that the fall in the number of offences prosecuted comes after the guidance has been issued. So concerns that we are prosecuting more of these cases, or too many, may not always be justified.

Q12 The Chairman: That is very helpful. Thank you very much. Tim Thompson, you may want to introduce yourself but possibly not elaborate further on—

Tim Thompson: I know that part of my two minutes has already ceded to the Director—

Alison Saunders: Sorry.

Tim Thompson: —as is right in accordance with my role. I am a lawyer in the CPS. I am currently the Director's legal adviser. Part of that role involves the oversight in the decisions in the category 4 social media cases. I have been in the private office for about two years, which covers the time from the interim guidance coming in, involvement in the cases that were looked at during that, involvement in the discussions about the final guidance and, as I say, ongoing oversight.

The Chairman: Fine. I know you will join in shortly. Chief Constable Stephen Kavanagh, thank you very much for joining us. Would you like to introduce your own perspectives on this?

Chief Constable Kavanagh: Thank you very much, Lord Chairman. I am currently the Chief Constable of Essex and, following some recent discussions and increasing awareness of the rapidly changing issues facing law enforcement, the Home Office, the Association of Chief Police Officers, the College of Policing and the National Crime Agency have asked me to take on a role in leading the co-ordination of how we look at what we are calling the Digital Intelligence and Investigation environment.

The piece of work does reflect a growing consensus of the need for law enforcement to develop an integrated approach nationally, which builds new skills for officers and staff and new ways of working but also supports, where it is felt appropriate, the development of new legislation. Law enforcement certainly welcomes the debate this Committee has started, and I hope that the findings of your inquiries will form my terms of reference, in terms of the piece of work that I am to take forward.

It is important to recognise the scale of the challenge we face. Every day 200 million tweets are sent and 250 million photos are uploaded. Every minute 204 million emails are sent and 570 websites created. There is an excess of 845 million Facebook users. We have new numbers—quintillion bytes of data in the digital environment are growing by 50% every year. Policing cannot, and should not, monitor everything that is happening on line and nor would you want us to, but there is a balance that we feel needs to be struck. The debate has been allowed to polarise and there is a balance between the right of freedom to expression and the right for those suffering abuse, vilification and extreme victimisation. Of course policing must remain proportionate; however, we have a duty to protect those suffering those real harms, especially the most vulnerable who do not know where to turn.

This is an issue that can touch anybody's lives at any time from any background, and there are too many victims out there whose lives have been devastated by online abuse. Of course legislation can be applied to many of the criminal behaviours in the social media, but we believe it is time to consider whether enabling preventative and enforcement legislation will assist in keeping people more safe in the online environment and provide a framework that is equally important that gives oversight and accountability to police where they do venture into this sensitive arena.

The Chairman: Thank you. That is really helpful.

Q13 Lord Clement-Jones: If I can just come back to the DPP: you gave us some very helpful background about the guidelines for prosecutions involving social media communications. I wonder if we could take you a little bit further along that track in terms of background. What were the actual problems that were perceived at the time that the guidelines were meant to tackle, basically? Secondly, you mentioned that you had 59 responses. I wonder who were the cohort of people consulted at the time.

Alison Saunders: The reason why the guidance was thought necessary, or we thought we should have guidance, is because we had had a number of high-profile cases that raised issues—the balance particularly around right to free speech and protecting individuals from harm, ensuring that there was consistency. Because we are an organisation that covers the whole of England and Wales, we have prosecutions up and down the country, and one of the things that is important for us is to make sure we have consistency around prosecutions. So it was thought there was some need because of the queries that we were getting from prosecutors to try to do that and I think—

Lord Clement-Jones: So there was a slight incoherence, was there, in terms of types of prosecution and—

Alison Saunders: I think certainly inconsistency, and we have tightened that up considerably with the guidance. It was around that sort of fourth category where we are looking at perhaps a grossly offensive definition. That is where we put in the extra protection around making sure it was centralised. It had previously come through the principal legal adviser's office. We have slightly changed that now so it can be authorised by the Chief Crown Prosecutor for the CPS charging, who takes the majority of charging decisions in the CPS. Those that do not go through him then have to come up to my private office to be authorised. We slightly loosened it because what we have seen is that the guidance is working and there is a much greater degree of consistency, but again because of the

sometimes sensitive nature of those cases, and to make sure we are protecting free speech and getting that balance right, that is why we have kept it more centralised.

In relation to the consultation, it was a wide-ranging consultation. It was out on our website. Anybody who wanted to basically respond to it could. We had responses from a number of individuals, organisations and campaigning groups, so quite a wide variety. We can let you have the names of those who responded if you like. We can send that later to the Committee.

Lord Clement-Jones: Very useful. You had the social media themselves commenting on it?

Alison Saunders: Yes. I should have said that not only did we put it on the website for consultation but my predecessor also held a number of meetings with a wide-range of people, including some of the social media providers, to come and talk to us directly on where they thought the balance lay, what they thought about the issues, what did they think about the guidance. So it was a big exercise in making sure that we consulted as widely as we could and received as much information as we could to ensure the guidance was as good as it could be.

Q14 Lord Clement-Jones: You made some interesting comments about the impact of the guidelines. I wonder if you and the Chief Constable perhaps as well could elaborate a bit about what you think essentially of the net result because, clearly, an assessment of how those guidelines have worked so far is important.

Alison Saunders: Yes. We looked at them because the interim guidance had been out for six months by the time we then finalised the final guidance, so that gave us an opportunity to review them, and also we have looked at them subsequently. We think that they have worked well, not just for us—and perhaps Stephen will be able to comment on this—but also for the police because a lot of these decisions may be made by police charging, but the guidance is public. It is out on our website so it helps police colleagues know what we would be looking at. It also lets members of the public know the sorts of things that we will be looking at as well in relation to social media cases. Certainly the feedback we get from prosecutors internally is that they find it very helpful. It does inform the way in which they make decisions and has made it easier. Certainly, from the numbers coming through the private office, which Tim will mainly be able to talk about, we are seeing less and more consistency around those that are coming, which again encourages me that they are working as they should be. I do not know if you want to add anything to that.

Tim Thompson: That broadly sums it up. The numbers coming through for approval in the eight months after the guidance was finalised were slightly lower than the numbers in the six months while the interim guidance was in force. There was a higher proportion approved in terms of the proposal to prosecute, so there was more evidence of people applying the guidance consistently. Broadly speaking, we would say that the guidance seems to have bedded in quite well.

Lord Clement-Jones: Although you might see a lot of activity in current times, I daresay, from press reports and so on. Chief Constable, what would you like to say from your perspective?

Chief Constable Kavanagh: Yes. The challenge that policing is facing is that the speed with which social media is moving, and the amount that has now not intruded but the way that people are living their lives within the social media environment, has meant that officers'

knowledge of what was previously a crime scene now has to dramatically change and change quickly. The College of Policing is supporting this, making officers more aware of what core business is in terms of the offences that can take place on social media. The challenge that we face—and we have had good work with the CPS—is that defence counsel or lawyers will try to ask different questions about how the police and the CPS present evidence to Magistrates at different time. So we need to get clear the framework in which we present, in a consistent way, screenshots of social media, levels of abuse or photographs that have been used, and we need not just the CPS and the officers to be aligned but we need the Magistrates and the courts to understand when there are excessive requests being made in relation to that. We do have to take responsibility for attributing the appropriate data or offences to individuals, because we know many Facebook accounts are built on false personas, as are other accounts, so we have to take responsibility to make this much more core business. Police training needs to be changed dramatically, so that everyone from the new beat Bobbies and PCSOs, all the way through to homicide investigators, will be part of it.

We think within policing, the Regional Crime Units that have now been established—the RCUs—the counter-terrorism and the national picture are getting increasingly well covered, but this is core business for us now and we need to make sure we are ready and working alongside the courts and the CPS.

Q15 Baroness Fookes: If we could now look at the current legislation: I might add that I am always reluctant to call for new laws until you have decided whether the existing ones can be made useful in a new situation, such as we have with social media. Could each of you say whether you think the current legislation under which you operate is satisfactory or not?

Alison Saunders: In the guidance we point prosecutors to the types of legislation and offences that they should be looking at, and I think it is quite important in this arena to make sure that we are looking at legislation that helps address the offending, not necessarily the means—that allows us to look at the offending no matter what the means of committing it is. There is quite a different distinction between "Is social media there as just a means to commit the offending?", as it is not the offending itself. For example, when we look at the harassment offences, we can prosecute people for harassment, physically harassing somebody, sending letters or doing something through social media, and we do think it is satisfactory. We think the Communications Act again—it has antiquated language, so the language perhaps around some of it is quite old fashioned; it is not surprising when you look at the date of it—is flexible enough to allow us to use it for the social media cases that we have found. We have not yet seen many where we cannot fit it in. Where we do think the legislation may need to be looked at is around some of the reporting restrictions in relation to anonymity and breach of orders. Certainly some of the breach of orders, particularly when dealing with children, I think—and again Tim will be able to give you more of the detail on this—cannot be committed through social media.

Tim Thompson: Yes. The issue there is that section 39 of the Children and Young Persons Act, which restricts reporting in relation to children involved in criminal proceedings, is breached by publication. But that particular Act has publication defined in a way that does not include deliberately putting things on social media. Whereas, the Sexual Offences Amendment Act, which provides anonymity to the complainants in sexual offences, does apply to people who publish things on social media but does not carry a penalty other than a

financial penalty. That is something that some District Judges have commented on when dealing with particular cases where individual victims of rape have been vilified in campaigns of people deliberately naming and abusing them, and the penalty available has been a financial one. There are issues around particular offences but the other offences, such as under the Offences Against the Person Act and the Protection from Harassment Act, are broadly capable of being adapted to new situations.

Baroness Fookes: Chief Constable?

Chief Constable Kavanagh: Thank you. The police are concerned around not just the social media but the whole digital environment, in that by dealing with just the offences once something has taken place we are almost missing a trick. What I feel, and the Director of the NCA, Keith Bristow, talked about recently, is trying to do neighbourhood policing and not leaving the police station. There are three key areas that I would be interested to explore. One is about enabling law enforcement to go into these environments, in an ethical and appropriate way, to establish where crimes are taking place or being planned. There is also a preventative element in "going equipped to steal"-type legislation, which is now taking place within social media and other environments that we need to properly consider, and of course then there is the enforcement aspect once an offence has already taken place. But I think by just focusing on the enforcement aspect we are at risk of missing an issue.

When we look at the processes that currently go on around denial of service—internet sites, harvesting people's personal data, the development of malware—these are clearly issues that are embedded within some of the social media environment and other digital environments that need to be challenged at an earlier stage if we are going to take back some form of control within this sphere. Currently there is no mandatory reporting requirement once data breaches do take place. In terms of law enforcement, in understanding the national, local and international threats that exist, without any compulsory reporting, confidentiality must be key. If a company is going to report a data breach it can undermine their credibility and their brand. But we still need to understand what is coming into this country on a daily basis, and at the moment we do not have that broader understanding and of course what we do know is that many of the victims do not report some of the offences on social media because of embarrassment, trauma and other issues. So there is a big issue of underreporting, failure to use common language and identifying the strategic threats as well.

Baroness Fookes: Would you suggest some new legislation that was neutral?

Chief Constable Kavanagh: I think the police always have to be careful about suggesting legislation. We would encourage the exploration of some of those new types of offences and how effective and how well known trying to apply existing and dated legislation would be. Some of that includes the Regulation of Investigatory Powers Act. When police do go into the social media environment we are trying to use RIPA to make sure that we can be seen to be accountable and be proportionate in what we are doing. Is that the right piece of legislation to use? We are making the best use of it, as you would expect us to, but I think this Committee and the debate does offer us an opportunity to say: how fit for purpose is legislation in terms of more proactive law enforcement, prevention and then ultimately enforcement once an offence takes place.

Baroness Fookes: Perhaps you would build on current legislation, or if you were doing something newer you would use that as a basis and then increase it in some way that would be helpful.

Chief Constable Kavanagh: Absolutely. I think, Lord Chairman, you heard from Mr Cooper last week. His suggestion about trying to streamline and to look at what already exists is key. What we do not want is additional legislation for things that can already be dealt with.

Q16 Lord Razzall: I think your answer there rather leads into my question because I think we—and I suspect from what you were saying, you—feel that there is a little bit of an overlap if a decision has been taken to charge somebody in a case involving communication sent by social media. Do you agree there is sometimes that overlap and, if so, how do you decide which legislation to use to charge the defendant?

Alison Saunders: We get that in a large number of circumstances. 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. It helps prosecutors to work their way through the circumstances and the context of the offending, because again that is important.

Lord Razzall: So the answer is you would look at the guidance?

Alison Saunders: Yes. That leads them to which offence should be—

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.

The Chairman: Do you have you a supplementary, Baroness Healy?

Baroness Healy of Primrose Hill: Yes. Even with the guidance, do you think there is a lack of clarity for prosecutors deciding under which Act to pursue a particular case and, if so, how should this be resolved? We have heard how much legislation is available but we are confused, so I do not know whether prosecutors need more help.

Alison Saunders: I do not think so. Tim may have some views from the cases that he has seen, but generally what we are seeing is that prosecutors, once they work their way through the guidance, take into account the circumstances of the offence. It is what they do every day with cases not involving social media, looking at the cases and deciding on the charges, and there may well be a number of offences where you get overlaps and you have to choose which legislation best fits. It is around: does it fit the circumstances? Does it give the courts sufficient sentencing powers for the gravity of the offence, which is another issue that we will look at, and does the evidence support the actual charge?

Tim Thompson: Certainly there is an overlap but that does not mean there is a duplication. For example, if someone reports that they have been threatened and reports it is potentially a threat to kill, one of the elements of threats to kill in terms of an offence is an intention to make the other person believe the threat would be carried out. So, if you had a threat that fell short of that it might amount to an offence of making a threat under the Malicious Communications Act. If the threat was repeated it might amount to an offence under the Protection from Harassment Act, but there has to be the repeated course of conduct. Or, if the threat was less explicit and amounted to a menace rather than a threat—and I will

assume for these purposes there is a difference—then it might amount to an offence under section 127 of the Communications Act. So it is a question of working through the actual facts and applying the most appropriate bit of legislation, but, as the Director has said, that is the case in lots of areas of criminal law. It is not confined to social media.

Q17 Lord Sherbourne of Didsbury: If I can explore a little more what we discussed earlier about the legislation under which you are operating, which of course goes back quite a number of years. You have said, and I understand this, that even though the terminology might be slightly old fashioned or distant compared to modern technology, it works. The question I would like to ask is that as social media developed since these Acts were passed and became operative, have you looked at how to enforce these Acts in a new way? Perhaps I can put it more clearly. As the social media has developed so fast, are there things that you first thought would not be covered or may not be applicable, which you have now decided that actually do fall within the provisions of the various Acts? I ask that mainly because I want to know whether or not, as we move forward, in ways that we probably cannot even yet envisage, in social media and the scale of it and the intensity of it, whether or not you will again find you are having to look at these things in a way you had not envisaged?

Alison Saunders: As things like social media develop we have had to think about: how does it fit within the legislation? Sometimes that may mean taking cases where we think we are pushing the boundaries, and exploring with the courts as well, whether or not we do have the right fit. In a lot of the cases since the guidance has been published we think we have found the right fit. It is not necessarily easy. We have had to think about it and think about what legislation we can use because of the methods of committing the offence. I suppose my plea, if you are looking at new legislation or different types of legislation, is it does not get pinned to a particular way of doing the offence, because that in itself, for the very reasons you have just articulated, may very quickly be out of date and cause us more difficulty than something that describes the offending—the actual consequences that we are looking at. So if it is a threat to kill it is a threat to kill. It does not matter how it is administered. That is what we want—the ability to be able to fit it in, no matter whether it is letters, if it is physical, face to face, or if it is over social media. It is a threat to kill and we have the legislation that enables us to prosecute that.

Lord Sherbourne of Didsbury: Given that the opportunity for scale in social media is so different from pre-IT and technology, has that changed your perception of what might be covered by the Acts?

Alison Saunders: Again that is the strong guidance to prosecutors around being very careful, about if it were something that would not have been criminal before, that you do not suddenly make it criminal because it just happens to be over the internet. Also balancing against that, if you said something in a room just with your two friends it would not go out, but if you tweet it to your friends and then it is re-tweeted and then re-tweeted actually it is a completely different scale. You need to be aware of that when you are putting things out on to the internet because that does make it very different, which is why we talk about the context and the harm behind it as well in the guidance.

The Chairman: Perhaps Chief Constable Kavanagh just wants to come in.

Chief Constable Kavanagh: Thank you, Lord Chairman. I totally agree with what Alison has just been setting out. My concern is that we have some very well informed learned

individuals who are deciding how to apply what has been described as a panoply, a mishmash, or a myriad of different pieces of legislation. If you are a member of the public who has been subject to trolling, vitriolic attack or the revenge indecent imagery that we have heard so much about, and you do not know what the problem is—you do not know how to define what the offence is—it is about having the confidence to come to the police, let alone the front counter clerk at Southwark Police Station at 2 o'clock in the morning understanding what those pieces of legislation are. There is a lack of consistency in what the victims and the public are receiving at the moment. I think we need to say: how do we help them to understand what type of offences they are experiencing? There is some potential for new ones within it but, at the same time, we must make sure that we do not add to that myriad that has been set out already.

Q18 Lord Clement-Jones: I want to pursue Lord Sherbourne's question a little bit because I think the guidelines very much were written at a particular time. Not much time has elapsed but nevertheless things have changed since then; a lot of it is about communication to individuals. It does not take into account, or does not appear to take into account, in the way that your answer did, this whole question about scale—at-large communication. For instance, I mean allegations about criminal offences that are made at large on social media, which are not necessarily targeted at the individuals themselves. They may not ever receive them themselves but they are out there in the ether.

Alison Saunders: That is a very difficult question for prosecutors or investigators. If I just sent something to Tim but he chooses to re-tweet it to the whole of Parliament, then that is a very different act but it is my initial tweet that is the offending issue. So for prosecutors that is very difficult. They would have to look around the context, but I think if they were just satisfied that there was no intention to take it any further, I am not sure we would be encouraging that as a prosecution.

Lord Clement-Jones: Do we bring about criminal libel or something? Is there anything that we can get a handle on that might be a useful tool?

Tim Thompson: There is the offence within the Communication Act of saying something that is false for the purpose of causing distress, anxiety or annoyance, I think the words are. So where something is demonstrably false that can be used. Of course we do not necessarily want to start having a huge trial about whether particular criminal allegations are false, but the scale of exposure is one of the factors that prosecutors will consider in terms of whether it is appropriate to prosecute, as is the likely impact on individuals, whether or not it was drawn particularly to their attention. If it is likely to come to their attention because of the scale of the exposure then that is still a factor.

Q19 Baroness Deech: Some people say that we need one more Act to pull everything together and make it all clear and coherent. I think there is perhaps enough—perhaps too much already—and the problem is people do not know about it, both those who have to use it and those who are affected. So do you think—and I bear in mind what the Chief Constable said about preventative action—it is better to have a new Act or would that take too long, or might it be better to try to get out to those who use the social media just how many offences they might be committing? There must be a way of getting this across to people on the very social media that they use.

Alison Saunders: I have some conceptual difficulty over a new Act or even a consolidated Act: what is it going to consolidate or put in there? When we look at the offences that we use, the malicious communication, harassment, threats to kill, they are all incredibly different and they do not necessarily just deal with social media. If you put those all in one Act, do you then have a separate Act just for things that are committed by social media? I am not quite sure how it would work. So I suppose that is a way of saying I think possibly one last Act is maybe not going to solve the issue. I do think that the Chief Constable's point is really important—sometimes victims do not understand what the offences are or what they can be looking at in relation to criminal conduct and, therefore, reporting. So perhaps there is something about more education that would go towards prevention, as well, and education not just for victims but for those people who may inadvertently find themselves committing offences because they think somehow it is okay to do it on social media and actually it is not.

Lord Razzall: Some of the newspaper editors do not seem to think that phone hacking is a crime.

Alison Saunders: Absolutely.

Tim Thompson: Anecdotally, there is some evidence that the prosecution of some high-profile cases has raised awareness. I say that because we have seen cases where people have posted messages and then their friends or contacts have commented back saying, "You are going to get in trouble for this" and it is often the people who then say, "I do not care. I am carrying on" who end up being prosecuted. So there is clearly a growing level of awareness.

Q20 Baroness Hanham: I can just follow on from this because I can see that consolidated legislation becomes a nightmare and takes time. If I offered you a magic wand and said, "Sort this out", where would your magic wand take you? That is question one, and then question two is—there were loads of things I was going to ask but I just want to ask this—it must be quite difficult to persuade or to get people to understand that the evidence has to be held by them, presumably. Otherwise, you cannot prosecute because you have to be able to get home with it. Can you get it from any source other than the person complaining so that you actually have access to it? This may come from a profound lack of Twitter knowledge, but I can see that to prosecute you cannot take nothing to court and if it is just a message, you have to be able to have some access to be able to take that to court. So, magic wand: how do you get the evidence into court?

Alison Saunders: Can I take the second one first, because that is easier, while I think about the magic wand? There are lots of issues about how we get the evidence and particularly for the police around how they get the evidence. Some of it we may have to get from abroad, so we need to go to internet providers to get evidence from them, and that can take time. One of the things—going back to, as I am thinking about it, your magic wand—is we know that there are already plans to look at the six months' statutory time limit, and that would be extremely useful because certainly when we get evidence from abroad it can quite often take longer than that. Even if it is investigations into who was it who sent that tweet or email or whatever, it can take some time to attribute it to the individual.

You do not necessarily have to have the victim who produces it. If it is there it is there and it is the best evidence, but obviously for some offences we would be looking to have the

individual it was directed at, if it was something that then had an impact on them, but, wherever we could, we would try to avoid bringing in that individual themselves.

Chief Constable Kavanagh: I think with a magic wand I would definitely speed up the response of some of the social media providers to letters of request for evidence. There needs to be a far greater sense of responsibility taken. The only way that we will take control of some of these issues is by that sense of community; very much in the way that we deal with other crime types, we have to have that sense. The overwhelming majority of people engaged in social media are upstanding decent people and there is an enormous amount of good, but we need that sense of community to start mobilising behind this because much of this can be dealt with without the weight of the CPS and the police.

The jurisdiction issues need to be clarified as well and I do think we need enabling and oversight legislation that supports the police in getting into this environment—understanding it. Prevention needs to be highlighted as well.

Q21 Lord Dubs: Do you think there is anything in the argument that people are using social media and it is the first time in their lives they have, actually—other than conversation with friends—put themselves on the wrong side of the law? They may be putting things on social media that normally they would use in conversation with people they do not like, in pubs and so on, and that never gets into this domain. Do you think that people are sufficiently aware of what they are up to when they start communicating on social media?

Chief Constable Kavanagh: If I may, I think it is an enormously important point. There are some young people who are making foolish, unpleasant, sometimes deeply offensive comments that they would pass in a playground or a coffee shop or a pub that would be forgotten within moments, and the naivety that those things will be held and they will be judged upon them in the future have been lost upon them. So the foolish errors of my generation, and possibly the people sitting here, have been lost and forgotten. But they are not being lost and forgotten. There needs to be education. There needs to be an awareness piece for people to understand the impact of what they are saying and doing, absolutely.

Alison Saunders: Most of the cases that we prosecute are cases that you would prosecute if somebody was saying them out loud physically in a playground or a pub or in the street, because they are just as offensive there. So there are a lot of cases we would prosecute if they were done orally as well as over social media.

Lord Dubs: But in practice you would not, would you, if they were shouting in a pub?

Alison Saunders: You may because, if they were shouting racist comments or they were being directed towards an individual, then you may find that they are committing an act under a Public Order Act offence. So there are offences that will cover that in the physical environment and we will look at prosecuting those or cautions. Indeed, people have been cautioned for social media offences as well. So it is not so different sometimes and I think we forget that this may be offending that you would ordinarily prosecute anyway; it is just the way in which it is conducted.

Lord Dubs: It may not be different but do people understand that what they are doing can amount to a criminal offence?

Alison Saunders: They may not, and what they also do not understand, of course, is that it gives us a really good evidential chain because, as the Chief Constable said, the evidence is there and it remains there.

Tim Thompson: Can I add that these are issues that are dealt with in the guidelines, though, so if it is clear that someone has fired something off without thought and genuinely regrets it, that is a factor that is taken into account? Most of the cases that are prosecuted involve people who have set out to be really hurtful. For example, deliberately posting something on to a memorial site for a child who has been murdered, that is not a throwaway comment. It is those sorts of cases that are prosecuted, not the cases where people make a single ill-judged remark.

Lord Dubs: Thank you. Would you like to comment on the sort of sentencing that there is for people who do what we are talking about? In other words, are the sentences too harsh? Are they too lenient? How ought we to be looking at this?

Alison Saunders: I would not comment on that. Sentencing is very much a matter for the court rather than for the prosecution. What we do make sure is that we provide the court with the fullest information so that they can consider the sentence in accordance with the Sentencing Guidelines, so really that is not a matter for me to comment on.

Lord Dubs: If I can put it another way: I understand why you have said what you have said. What would victims like to see happening? In other words, it is not just the sentence that society imposes. Does the victim feel that meets their concerns or not? Is that still beyond your remit?

Chief Constable Kavanagh: Whether or not there is opportunity in due course to get Victim Support along to talk about some of these issues, I think the scale of the humiliation, the embarrassment and the impact, not just on those targeted but those around them, is often not captured by us in an effective way to give to the court. So we have to make sure that the sheer impact that this can have on individuals and their families is better captured for the future.

Tim Thompson: We have taken account of the views of victims. Obviously we still have to make the decision but in borderline cases we have consulted about the possibility of, for example, a conditional caution with a letter of apology being written, and we have taken decisions in light of the victim's views.

The Chairman: Can I ask the Chief Constable whether ACPO has a line on this amendment to the Criminal Justice Bill that would allow more severe sentences to be passed and extend the period of time available to people to build a difficult case against offenders? Does ACPO have a line on this rather fast moving debate?

Chief Constable Kavanagh: In a fast moving environment I will give you the position. I think anything that helps us to investigate thoroughly and put the matters before the CPS has to be to the benefit of victims and society more broadly, and anything that allows judges to use the full range of penalties that they might need to consider has to be helpful.

Tim Thompson: There is, though, a law of unintended consequences. While it would increase the penalty, that would mean that all offences in that category, regardless of what type they were in particular, could be tried in the Crown Court and, therefore, could end up adding to the weight of the Crown Court cases. I am not sure that there is evidence that District Judges or Magistrates feel particularly constrained in sentencing under these offences. The proposal

for an extended time limit is a very practical one. There was an extended time limit in the Telecommunications Act until that was replaced with the Communications Act provision. So that is something that has some direct and obvious benefit without having wider consequences.

The Chairman: That is really helpful to us.

Q22 Lord Horam: Can I ask the Chief Constable a question about workload? I am told that half the cases being forwarded to frontline officers are complaints concerning the social media. Is that the case? That seems a fantastic statistic.

Chief Constable Kavanagh: The anecdotal evidence is that half of anti-social behaviour or harassment is now linked. There are a variety of other offences that take place. I suspect that if you look at fraud there may be a higher proportion. That is something I think would be worthy of the Committee just recognising; it is where the College of Policing and ACPO have come to. If you look at social media in isolation to other forms of digital communication, including email and other digital opportunities, we feel that you have to look at it in its broadest sense.

Lord Horam: Are you saying that ordinary non-digital anti-social behaviour and social behaviour on social media are linked, and that is what is producing this large proportion of work?

Chief Constable Kavanagh: We think that the level of underreporting and the volume of work will be significant for us to undertake. That is something that we have to work through, the expectations of people about what is viable for us to take on, because at a time of austerity policing already there have been some big decisions around labour and other areas.

Lord Horam: Absolutely. This is a whole extra burden, is it not?

Chief Constable Kavanagh: It is an enormous requirement for us to keep people safe, and the training that we are talking about across core policing business will be a massive undertaking for the College of Policing and local policing colleges to undertake.

Lord Horam: What do you do by way of training?

Chief Constable Kavanagh: At the moment there is a variety of training from digital investigations and open source, which looks at social media and other sites that will allow us to see what else is going on in the digital environment, all the way through to senior investigators and covert internet investigators, which is the equivalent of undercover officers who operate with very specific requirements and very tight oversight. So there is a whole range of training that currently goes on. The concern that the college has and ACPO has, together with the Home Office, is that we now need to get the Bobby on the beat confident that, when somebody comes up to them in the street and makes an allegation of harassment or trolling or other forms of abuse on social media, they have the tools and the confidence to deal with it.

Lord Horam: How do you do that? Do you take them off to an education establishment for a period of time and instruct them in all this or tranche by tranche? How do you do it?

Chief Constable Kavanagh: There is variety of ways. Certainly I have been responsible for the Open Source Intelligence working group within the ACPO arrangements. We have a

range of training, from computer based, sitting at the desk and raising awareness of what the opportunities are, all the way through to two-week courses embedded at the College of Policing or local colleges. So there is a whole range, and to make the core business aspect of policing more effective in this arena the majority would have to be computer based within police stations and locally. It is only when it gets more sophisticated—

Lord Horam: So they are doing it in situ in their local police stations?

Chief Constable Kavanagh: Yes.

Lord Horam: Most of the time.

Chief Constable Kavanagh: Yes.

Lord Horam: Thank you.

The Chairman: Are you really, though, thinking this is going to become an overwhelming problem if the social media gathers momentum, at the speed that it is—that you might be drawn into stuff that would not have in the past been part of proper police work? Is the prospect of the future daunting for ACPO members?

Chief Constable Kavanagh: It is not daunting. It will require us, just as we are already in other areas of policing, to make some clear decisions. What does help is we are not in the policing of morals or good taste. What we have to do is make clear to members of the public where those boundaries are, and if they step over those boundaries that we will intervene quickly and decisively with the support of the CPS. I was surprised that Mr Cooper was suggesting that the Obscene Publications Act could be used in relation to revenge indecent images. It is an aged piece of legislation that clearly does not fit the bill for people who are hugely traumatised by what has taken place. So what is acceptable is changing the whole time, and what the police need to do is make sure we reflect what society wants of us, not what we think is appropriate.

The Chairman: That does lead it on to Lord Sherbourne.

Q23 Lord Sherbourne of Didsbury: Yes indeed, very much to the question I want to ask, on the particular question of revenge porn. There has been a lot of chat and I think the Secretary of State for Justice has said that there may be a need to look at changes in the law to deal with this. I am not totally clear, and I raised this last week in the hearing: what exactly might be the current weakness in the law with regard to revenge porn? If somebody posts on their Facebook a very intimate private photograph, at what point does that become something that might well be an offence?

Alison Saunders: For us—and I have mentioned this before—it is about looking at the context. So if it is just a case of posting something up that is not indecent or obscene then I am not sure that there would be an offence committed. Some of the revenge porn that we have seen and prosecuted has been not like that. It is not images sent between consenting adults, it is where relationships have either ended and there is some acrimony and they are posted because it is, "I am going to send it to all your employers because I want to humiliate you" or "I am going to distress your family by sending this picture to you". Those are the ones where we do look at the context and do prosecute now, and we may prosecute under malicious communications. It may be under harassment or it may be, if the victim is under 18, under the Protection of Children Act. There are offences that we use now and we do

prosecute but if it is just a case of an image that is not obscene, indecent or not doing it for some harmful purpose—

Lord Sherbourne of Didsbury: Let me take a particular example, again, where I am not totally clear, which is something that is done in a vengeful way. It is made clear it is done in a vengeful way by some comment relating to the picture, which is of a very intimate sexual kind, for example, and it may be an invitation for dissemination but it is not necessarily. Does it require it to be passed around or not or if you just post it and make it clear that there is an intent, but you are not doing anything more than just posting it on your own Facebook?

Tim Thompson: It is important to distinguish between the guidelines that are to do with how we approach social media offences and the offences themselves, which are not related to social media—they are related to electronic communications. So if you communicate a message to someone and your purpose is one of the things specified in the Act, and the thing that you communicate can be described as grossly offensive, indecent or obscene, you commit an offence, even if you send it to one person. So in your example of one person sending to one other person an image that could be described in that category, and which is done for the purpose of causing distress or for any other unlawful purpose, then an offence is committed and we would prosecute.

Lord Sherbourne of Didsbury: Do I take it from what you have said that you feel at the moment you are able to deal with these sorts of cases under the prevailing law?

Alison Saunders: We are dealing with them and we have prosecuted some of these. There is an issue, a slightly different issue that is not so much about the legislation to prosecute but around anonymity because some people may be extremely embarrassed about coming forward and revealing this because the prosecutions will be in public and may be reported. So there may be something around anonymity for those who might make allegations, which is a slightly different issue.

Q24 The Chairman: Are there any final comments? Chief Constable, you first perhaps just to wind up?

Chief Constable Kavanagh: I would just build on that last point. We were discussing outside that in some of these chatrooms that take place, often a young woman will do something that is intensely embarrassing and then be persuaded and controlled into doing something more and more. Again, that is just drawing these young people into increasingly embarrassing and difficult situations, and to clarify how we can intercede in some of these situations—real-time interception, support for people who are finding themselves in these difficult places—is increasingly important because it is having an enormous impact.

The Chairman: Yes, thank you.

Alison Saunders: I want to pick up two things that Mr Cooper talked about last week, just to make sure that I correct any factual inaccuracies there. One was around the training for prosecutors and whether or not they read any law, and I can assure the Committee that they do and that they have been trained. That is part of the guidance and of course the case that Mr Cooper was talking about was before the guidance. It was one of the cases that made us think about the guidance.

The Chairman: Robin Hood Airport.

Alison Saunders: Exactly. That is one of the cases where we looked at it. That case led in part to the guidance, which now informs prosecutors and, again, we have e-learning training for prosecutors[1] and they are talked to about this. The second thing was in relation to racially aggravated. I think the Committee had some concern about whether any of these offences might be racially aggravated, and there are specific offences of racially and religiously aggravated harassment contained in the Crime and Disorder Act, and that has existed for 15 years or so, so there are provisions that we can use for that. Perhaps that gives some comfort to the Committee.

The Chairman: That is more than helpful.

Tim Thompson: Nothing from me. Thank you.

The Chairman: Thank you, all three of you, very much indeed for giving up your time. You have given us tremendous food for thought. That is extraordinarily helpful.

[1] An e-learning course that complements the CPS Guidelines on Prosecuting Cases Involving Communications Sent Via Social Media has been developed. This course is part of a wider e-learning package on online crime. A release date for this package has not yet been determined. This is in addition to an existing e-learning course covering cyber stalking, which was released in September 2012.

Crown Prosecution Service and Association of Chief Police Officers – oral evidence (QQ 11-24)

Transcript to be found under Association of Chief Police Officers

Crown Prosecution Service - supplementary evidence

OFFENCES CHARGED AND REACHING A FIRST HEARING IN MAGISTRATES' COURTS

		2009	2010	2011	2012	2013	2014
Communications Act 2003 { 127(1)(a) and (3) }	Send by public communication network an offensive / indecent / obscene / menacing message / matter	1,182	1,652	1,547	1,724	1,156	477
Communications Act 2003 { 127(1)(b) and (3) }	Cause to be sent by public communication network an offensive / indecent / obscene / menacing message / matter	87	171	306	298	150	103
Communications Act 2003 { 127(2)(a) and (3) }	Send false message by public electronic communication network to cause annoyance, inconvenience or anxiety	326	294	307	278	233	85
Communications Act 2003 { 127(2)(b) and (3) }	Cause to be sent by public communication network a false message to cause annoyance / inconvenience / anxiety	51	167	149	128	125	48
Communications Act 2003 { 127(2)(c) and (3) }	Persistently make use of public communication network to cause annoyance / inconvenience / anxiety	488	528	648	680	558	252
Malicious Communications Act 1988 { 1(1)(a) and (4) }	Send letter / communication / article conveying indecent / offensive message	207	282	301	346	326	130
Malicious Communications Act 1988 { 1(1)(a) and (4) }	Send letter / communication / article conveying a threatening message	478	624	728	728	609	322
Malicious Communications Act 1988 { 1(1)(a) and (4) }	Send letter / communication / article conveying false information	49	48	49	58	75	37
Malicious Communications Act 1988 { 1(1)(b) and (4) }	Send communication / article of an indecent / offensive nature	158	210	194	189	131	87
	Total	**3,026**	**3,976**	**4,229**	**4,429**	**3,363**	**1,541**

2014 data covers Jan to May 2014 inclusive

1. Data relates to the number of offences recorded in magistrates' courts on the CMS system.

2. Offences data are not held by defendant or outcome.

3. Offences recorded in the Offences Universe are those which reached a hearing. There is no indication of final outcome or if the charged offence was the substa

4. Offences recorded in the Offences Universe of the MIS are those which were charged at any time and reached at least one hearing. This offence will remain recorded whether or
with and there is no indication of final outcome or if the offence charged was the substantive offence at finalisation.

5. CPS data are available through its Case Management System (CMS) and associated Management Information System (MIS). The CPS collects data to assist in the effective management of its prosecution functions. The CPS does not collect data which constitutes official statistics as defined in the Statistics and Registration Service Act 2007. These data have been drawn from the CPS's administrative IT system, which, as with any large scale recording system, is subject to possible errors with data entry and processing. The figures are provisional and subject to change as more information is recorded by the CPS.

Facebook and Twitter International Company – oral evidence (QQ 25-37)

Examination of Witnesses

Simon Milner, Policy Director, UK, Middle East and Africa, Facebook, and **Sinéad McSweeney**, Director, Public Policy, EMEA, Twitter International Company

Q25 The Chairman: Our next two witnesses, welcome: Simon Milner from Facebook and Sinéad McSweeney from Twitter. Thank you both very much indeed for joining us, again at short notice. We are really glad to have you with us. You sat in on the previous session, so you have heard me say that we are being televised on the internet. Would you begin—Simon, let us start with you—by perhaps telling us a bit about your own background and how you are viewing these big issues of social media offences?

Simon Milner: Thank you very much, Lord Best. My name is Simon Milner. I am Facebook's Policy Director for the UK, Middle East and Africa and it is a pleasure to be invited back to give evidence to this Committee. Facebook—I hope you know what it is. It is a service that has been running for about 10 years now and we have over 1.2 billion people regularly using Facebook and some 34 million people using Facebook in the UK, many of them via a mobile phone.

We take the safety of the community of people on Facebook extremely seriously and there are a number of things that we do in order to keep people safe. These things have grown over time, so they were not things that were at the start of the Facebook. We have learnt a lot over our period of operation in order to ensure we can provide the best possible tools and resources and expertise to help people keep themselves safe, and then in extreme circumstances for us to help them and for us to work with law enforcement wherever we need to in the world in order to do that. I am very happy to explain more about those as we get into questions and I look forward to those.

The Chairman: Thank you very much. Sinéad.

Sinéad McSweeney: Thank you. I am Sinéad McSweeney, Director of Public Policy for Twitter in Europe, Middle East and Africa, based in our headquarters in Dublin. My background: I am with Twitter two years today, in fact, and prior to that had spent between eight and nine years working in policing on the island of Ireland, both north and south, so I see a few familiar faces from the Northern Ireland context around this table today.

I guess in my day-to-day work, I engage with Governments, regulators and others on safety, as well as the many, many other policy issues that impact on the department, so I am representing the company in that capacity today, but more specifically, I am representing my colleagues, including our Head of Global Safety Outreach, Patricia Cartes, and our trust and safety teams, our user services teams, our legal teams and indeed the engineers and product managers who work on safety for the company day in, day out.

Twitter, the platform itself, is an open and public platform. We constantly emphasise to our users that they are speaking in a public space. It provides people an opportunity to share information or talk about issues, whether they are global, national or local issues, and reach many, many people with that message. We have 255 million monthly active users on the platform, 15 million of those in the UK. The platform sees 500 million tweets a day, so that

is 1 billion tweets every two days, and in fact, it took just a little over three years for us to reach that 1 billion tweet mark; that will give an idea of the scale of growth, that we now see that volume every two days.

The platform itself, as I say, is very much an open public platform for sharing information. It is guided by and underpinned by the fundamental principle of freedom of expression. Our bias is towards sharing as much information and content as possible. That said, there are rules as to how people can share information on the platform and use the platform and, where people violate those rules and users report those violations to us, they are reviewed and actioned by our team. Similar to Simon, as we get into the detail of questions, I can talk about the different actions that we take for different issues that arise.

The Chairman: Thank you very much. Lord Clement-Jones.

Q26 Lord Clement-Jones: Perhaps we could take that on, in that case. Simon, you talked about the best possible tools and, Sinéad, you talked about rules. Perhaps you could just take us through what your companies already do to prevent exposure to harassing, threatening or grossly offensive material online—in particular what you provide to users to report abuse and the kind of work you do to monitor material posted on your sites.

Simon Milner: Very happy to do that, thank you very much. I think there are three main features of Facebook that it is worth you understanding in this context. First, Facebook has a real name culture, so we have a rule that says you have to be yourself on Facebook, and that means that everybody's action on Facebook is tied back to their real identity. This is something that was from the very foundation of Facebook and we think it is one of the reasons why Facebook has grown as much as it has—that people are much more willing to connect to people they know in the real world and to engage with them on our platform. We also feel it creates an environment in which people are accountable.

We also have a set of community standards, so this is not a free for all. There are rules about what is allowed and what is not allowed on Facebook and one of the very clear rules that people can see in our community standards is you cannot use Facebook to harass or bully individuals.

Then what we do is enable people to control that. There are some things that people can do in order to control their privacy on Facebook. Unlike Twitter, Facebook is not a completely public space, it is a series of communities, if you like, and each individual on Facebook determines how broad they want their community to be, both in terms of who they are friends with, but also every single thing they do they can decide who can sees it. You may have a small circle of friends, but want to post something publicly, or you may only want to post something to a small group.

Then you can also decide whether or not you want to interact with people who are being abusive, in the same way as most of us in our everyday lives, if we think that somebody is going to be confrontational, we will go out of our way to avoid them; it is very straightforward to do that on Facebook. You can block someone, such that they cannot interact with you, nor can they see any of your content on the platform, and that is a very powerful tool to deal with someone who wants to have a go at you to prevent them having any kind of contact with you.

Absolutely people can report to us. We have a very extensive system of reporting, so virtually any piece of content on Facebook can be reported to us, for instance, in terms of being abusive or constituting harassment, whether it is a photo, a comment, a link, a

message: whatever it is, it can be reported to us. We have a team of experts who will look at those reports and make a judgment.

I can also tell you we have introduced some other features that enable people to resolve problems without necessarily reporting them to Facebook. Sometimes quite low-level disputes between people—we all know we do not always get along all the time—instead of them escalating into fully-fledged harassment, we now have tools that we have built within our reporting process that enable people to ask someone, for instance, to take down a photo about them they do not like and to do it in a way that is quite empathetic, and in most situations people do so. Some 85% of cases where people ask someone to take a photo down using our tool for this, people take the photo down and both parties feel better about each other, there is more trust between them. That is an example of how we have moved on from just, "Report and we will look at it" to, "Report or resolve" and that is something that we have had a lot of interest from other companies in how that works and wanting to understand how they could incorporate it into their reporting systems.

Sinéad McSweeney: As I mentioned, Twitter is an open and public platform, and I think it is sometimes useful to draw parallels with a public space. I was interested even to hear the Chief Constable in the previous session talk about anti-social behaviour and draw maybe some parallels with that. In that context, at its highest level, I think about activity like this on Twitter at three levels. You have the individual social responsibility, as a citizen in a public space, as to how you behave and the appropriate social norms as to how people should behave.

You then have the sense of community and peer impact on how individuals behave, so if you think of families having a picnic in Hyde Park and somebody comes along and they are shouting at the children or whatever, you will find citizens nearby in other families who will say, "Come on, this is not the place for that. Move on". Again, somebody in the last session mentioned somebody posting information and somebody saying, "You will get in trouble for that" and people almost correcting each other. Then at the next level, I guess to take the family picnic situation, you also have park rangers.

Within the Twitter context, we take a number of steps to mirror that activity in the public space. First, we make it clear to our individuals what their responsibilities are: there are rules against direct threats of violence, targeted harassment and a range of issues like that, so they know when they come into that public space the rules by which they need to comply.

There is an extent to which by working through our help centre and the advice that we give for people how to behave online—again, reiterating the public nature of the space—and more particularly through the work we do in education initiatives, working in partnership with the Safer Internet Centre, with schools, with Cybersmile and various other safety organisations, we are helping to inform the community and those peers as to the behaviour they should expect of others in this public space and how they can call out that behaviour when they see it.

Then, as I say, I see the park ranger analogy as being our trust and safety teams, those trained, expert people who receive reports when they come in from users and action them as and when they arise. In the last 12 months in particular, taking feedback that we have received from people here in the UK and elsewhere, we have tried to simplify our reporting procedures. We have introduced in-tweet reporting to make it easier for people to get to the place where they can file a ticket. We are working on our media settings, our filtering capability for users so that they can control their experience. Then the element beyond, I

think, the three sides is when activity tips over into actual criminal activity and therefore we then have a whole separate process for dealing with police.

You mentioned about proactively monitoring and moderating content. You will appreciate the level and volume of content means that that in essence is not practical in a real sense. However, we do have certain measures like, for example, photo DNA to detect illegal child sexual exploitation content, so that is one aspect of proactive content moderation. Then we have also noticed that there are certain abusive behaviours that mirror spam-type behaviour. So, in actual fact, in improving the technology around our spam detection, we are also finding that we are getting results around abusive behaviour and that is something else from which we are currently learning.

Lord Clement-Jones: What I seem to be getting from both of you is that this is not a static situation. You are both evolving your tools and your systems and there has been quite a lot of evolution even over the last year in both respects.

Simon Milner: In fact, since I last gave evidence at this Committee, the new reporting features I mentioned where we enable people to resolve problems have been introduced right across the service all across the world. Yes, we are always looking for feedback, we are always trying to use evidence around how people are behaving on the site. When people have a bad experience, how can we help them resolve the problem? If we are not doing it in a good way, let us see how we can make that better. Absolutely innovation is at the heart of our company, and I am sure the same with Twitter, and that includes innovating in how we keep people safe on our platforms.

Q27 The Chairman: Do you have any statistics on how many people request that content be taken down from websites and how often you accede to that request?

Simon Milner: I am happy to go first. We do not have any public data on that, no, Lord Best, but it is a question I often get asked: "How many reports do you get and how many do you act on?" It is fair to say two things: first, there is a lot of noise in the reporting system. If somebody says they like Rihanna, the pop star, there will be many people who think it is bullying or harassment or they will report it as pornographic. There is a lot of noise in the system.

Also, my contention would be that the key thing here is expertise, so not how many decisions we make but how many do we get right, and that is why we focus very much on investing in expertise in our centres and ensuring that we get the very best people, the best expertise looking at those reports. That is the best judge and we are always very open for policy-makers, safety organisations and parliamentarians to come and visit our Dublin headquarters and to meet with the team that review these reports and see firsthand the expertise that lies within.

Sinéad McSweeney: Yes, I would have a similar take on it in terms of looking at statistics on numbers of reports or numbers of requests. It is not necessarily informative as to the true nature of the issue that you are trying to address as a Committee. The number of reports we receive is definitely a tiny fraction of the overall volume of content on the platform, but that said, the figures themselves are not necessarily meaningful or informative.

Simon mentioned Rihanna: I was going to talk about One Direction fans, who report Bieber fans. You could literally have a spike in reports one day, and when you dig down into them, you just find that somebody took a notion somewhere that Harry Styles was better than Justin Bieber and everybody complained about Bieber fans. That adds nothing to the substance of what you are trying to look at today, so it is important therefore to look at the

substance of reports rather than the quantity. What we focus on rather than volume is on making sure that those reports that are likely to be flagging something that is very serious or potentially grave are attended to as a matter of priority, so that is the focus rather than the overall volume.

Simon Milner: If you would not mind me adding: one of the things that we do, and I am sure Twitter are the same, is we try to also use systems, so it is not just about people looking at reports. It is also about using systems to flag the most serious types of report, so looking out for reports from particularly vulnerable users. Somebody who is under 18 reporting that they are feeling harassed or bullied, and particularly telling us how it is making them feel, we are going to get that report more quickly than an older person reporting spam on their service. Also, using systems to ensure that when we get something like a spike in reports around a particular issue—that once we have looked at a piece of content and we judge that it is fine, it does not breach our terms—then we can use systems to make sure that we do not have to look at all the many thousands of reports potentially that might come again about a particular piece of content. If it has not changed, then our decision remains the same.

Q28 Lord Horam: You are saying that statistics can be easily misleading in this area, just looking at the overall picture. It is very much the nature of the offence that may be more difficult to extract from all this. How many people do you employ in dealing with potential abuse of this kind?

Simon Milner: Shall I go first? That seems to be the way we are handling it. We do not have a public figure, Lord Horam, on how many people we employ in that specific team.

Lord Horam: Do you have a private figure?

Simon Milner: Of course. We know how many people we employ.

Lord Horam: How many is it?

Simon Milner: We have hundreds of people who are safety experts working for Facebook.

Lord Horam: Is that in Ireland or is it—

Simon Milner: That is across four centres, so Ireland, which is a centre that will handle reports from all across the world, with more than 20 languages spoken there; also Austin, Texas; our Californian headquarters in Mendel Park; and Hyderabad, India.

Lord Horam: So you will have hundreds of people in those four centres—

Simon Milner: Hundreds of people.

Lord Horam: —dealing with potential abuse?

Simon Milner: Dealing with reports of content or conduct on Facebook that people on Facebook believe should not be happening, that are breaches of our terms, but some of those could be—

Lord Horam: Is that a high proportion of your total staff?

Simon Milner: Facebook has a total staff of around 7,000.

Lord Horam: So this is 1,000 maybe?

Simon Milner: I cannot give you the specific number, I am afraid.

Lord Horam: But it is something of that kind. How about Twitter? Is that similar?

Sinéad McSweeney: Obviously we are a smaller company. We have 3,000 employees worldwide and we do not have the same number of users, so we would have in excess of 100 people working across a range—

Lord Horam: In excess of 100 people?

Sinéad McSweeney: Yes, working across a number of timezones in order to provide cover 24/7 and that is covering—

Lord Horam: Is this internationally? This is not just the UK unit, is it?

Sinéad McSweeney: No. I think the key point is we ensure we have timezone and language cover, but rather than focusing geographically, the teams look at distinct issues. For example, we have a minors and content team.

Lord Horam: They look at an issue internationally rather than just looking at—

Sinéad McSweeney: They have the expertise in that area, so the minors and content team is headed up by John Starr, who is ex-FBI, ex-National Centre for Missing and Exploited Children, so his team will look at the complaints that relate to that issue. Then you have the user safety team or identity team, the law enforcement team, rather than splitting it geographically, but yet it is such that you have timezone cover also.

Lord Horam: Yes, I understand. But you have to operate internationally, I fully appreciate that, but there are different laws in different countries. Does that cause you problems?

Sinéad McSweeney: No. The vast majority of what we are discussing can fall within the platform's own rules and therefore is dealt by these teams in the context of whether or not it is a violation of our rules. Should police in any individual jurisdiction come to us and say, "An offence has been committed on your platform. It is an offence in this jurisdiction"—for example, there may be hate speech offences in France or Germany, which would not be criminal offences here—we would co-operate and work with the police in France, because it is a criminal offence in France. Similarly, there may be offences here that are not offences in other places, but we would work with the police in the context of what their requirements are to investigate that offence. We navigate it that way.

Simon Milner: It is a similar picture for Facebook, so bullying and harassment is not allowed on Facebook wherever you are on the globe, irrespective of whether there is a local law around bullying and harassment; that does not matter to us. It is what is allowed in our community. Then the main way we will take account of local law is when we are dealing with law enforcement.

Lord Horam: Thanks very much.

Q29 Lord Dubs: May I just ask: perhaps I am misunderstanding something and maybe the answer is obvious, but the complaints that you get, they either come from people or they come from the police, is that right?

Simon Milner: The police do not tend to make complaints. Certainly the police do not use our reporting process. I can explain how the police ask us for information if you would like, but it is not via our reporting process.

Lord Dubs: No, I will come on to that later, if I may. But is it possible that people who feel aggrieved do not know how to put a complaint to you or is it so widely known does everybody know automatically where to go to say—

Sinéad McSweeney: It is never beyond the bounds of possibility that no matter how many times you tell somebody something that they do not know it. Even drawing on my old days in police communications with basic crime prevention advice, six out of 10 burglaries take place through open doors and windows, and people still leave their doors and windows open.

We are never done in terms of highlighting the resources. As companies it is an area on which we work together in the context of Safer Internet Day and working with resources that are put together by central, respected organisations in this space—so different organisations who put together documentation for schools or parents with all the ways in which to report content or issues on the different platforms and put it all in one place.

Simon Milner: I would say I spend a lot of time travelling around the UK talking often to groups of teachers about how Facebook reporting works. It is much more likely a child is going to ask their teacher, "I have this problem on Facebook. I do not know what to do about it" and I want those professionals who are working with young people to know what to do, because it is those situations in which the young person—or an older person—is suffering harassment and does not act. If they do not tell us, we will not know.

Having said that, there are mechanisms for people to tell us about someone else they are worried about on Facebook, so it is not always about, "I am feeling vulnerable". People can use our reporting process to let us know about someone else they think is depressed, maybe even suicidal, because of what they are experiencing in the real world or on Facebook. But you are absolutely right, Lord Dubs, that the onus is on all of us and it is a shared responsibility here to ensure that people know that they can do something. They do not have to suffer in silence.

Q30 Lord Razzall: That leads neatly into my question, which is: perhaps each of you could explain to us—just talk us through—when your organisation receives a report of potential abuse, what happens when that report has been received? It may be impossible to say how long it takes you to respond because it may differ, but give us some indication. It would be useful if you could give us some indication as to what potential actions you might or might not take, having received the report.

Simon Milner: When we get a report, we will review the report. We have a community operations team; they will review the report. If they conclude that the piece of content or the action that has been taken that has been reported does not comply with our community standards, it will be removed from Facebook, so it will be deleted.

Lord Razzall: So you remove it?

Simon Milner: We remove it. The person who we are taking action against, we do not let them know who has reported it, so the reporter remains anonymous. We will also let the person who reported it to us know what happened to their report. We introduced something in April 2012 called the support dashboard, so any time you make a report to Facebook, we will let you know we have received your report, we will give a sense of how long we think it is going to take to respond to it and then once we have decided on our action, we will tell you what action we have taken and you will get a notification from us explaining that. Then we can and will take action against individuals, depending on the severity of their breach, and often people have done this innocently: they did not realise, for instance, that Facebook has a rule about, say, nudity. It may be a perfectly innocent photo of someone they love, but we do not allow nudity and if that is reported to us, we will remove it and we will let that person know, "Hey, you cannot do this".

When people start to become repeat offenders, then we are much more likely to take more stringent action. We may restrict what they can do on Facebook. We can limit people's ability to upload photos, for instance, if that is the way that they have been abusing our service. Of course, we can and will take action to remove people from Facebook who are breaching our terms. Particularly, for instance, I mentioned earlier about our real name policy. If somebody is reported to us as being a fake name or an imposter, then we will remove that account, irrespective of whether the content of the account is breaching, but the very fact that that person is not authentic will mean their account is removed.

Lord Razzall: How long does this process normally take?

Simon Milner: It depends. It depends on the issue. Where we get reports that someone is, for instance, suicidal or self-harming, we are going to get those reports very quickly, potentially within minutes. When we get reports of illegal images, of child sexual abuse on the service—thankfully they are extremely rare because of the technology we use to keep them off the service—we are going to act very quickly, within minutes, to remove those.

It will also depend on what is going on in the world. For instance, during the Syrian conflict we can often get enormous volumes of reports relating to both sides in the Syrian conflict trying to report each other's content and that can mean that the team in Dublin is consumed by that. That is why we cannot be definitive about how long it takes, but believe me, when it is something really serious, when somebody is at risk of real harm, we will move quickly.

Lord Razzall: What about Twitter?

Sinéad McSweeney: I think the answer is echoed in your question, in that it depends on the nature of the abuse or the issue being reported and it depends on additional steps that may be required. For example, if somebody is reporting an impersonation, we may require them to provide identification, because obviously we do not want to close somebody's account inadvertently. That will impact on the timescale. In terms of the actions that are taken, the tickets are reviewed by the relevant team. As I said, we have different ones looking at different issues and the action can range on the actions taken at the account level, so the action is against the user of the account that has breached our rules, and that can range from no action, obviously if there is no real breach, to a warning, to a temporary suspension, to a permanent suspension.

Our overall objective, similar to Facebook and many platforms who are operating in this space, is that clearly issues like self-harm, suicide and illegal content will be at the top of the list in our triaging to action quickly, but the overall objective at all times, whether it is from our safety engineers or our product managers, is to make sure that we are getting smarter and more efficient all the time in how we deal with the diverse range of reports that can come in.

Q31 Lord Sherbourne of Didsbury: Can I explore two areas with both of you, if I may, and drill down a little bit deeper, just so I understand? It may be a very elementary question, so forgive me. In the alleged or potential abuses that you are looking at, do they all come from humans or do you have any systems? You used the word "system". Do you have systems as well for monitoring? Obviously people who are on Facebook or Twitter, they may well report what they think is an abuse; that comes from a human being, but do you as an internal system have any process by which you monitor by humans or by electronic systems?

Sinéad McSweeney: We touched on it when we were talking about the volume of content: with 500 million tweets a day, the basic answer is no, it is not possible to moderate or

monitor content. However, we have photo DNA, so that is, as you say, a technology as opposed to a human being, which is there to detect illegal content, illegal child sexual exploitation content, and then to the extent that there are mechanisms to detect spam, they can also have a positive impact in terms of detecting and dealing with abusive behaviour, but the vast majority of rule breaches require a human review, because context is important.

Lord Sherbourne of Didsbury: Predominantly, almost all the abuses that you have to deal with have come from people reporting and you of course have no idea therefore what people have not reported?

Sinéad McSweeney: That is true, yes.

Simon Milner: It is similar for Facebook, but I would classify it as a form of proactive reporting. The way that we tend to think about it is effectively we have had this community of almost 1.3 billion people. They very much act to protect their community. It is almost like a neighbourhood watch scheme at scale in that they can and do look out for each other. When they see things that are happening on their friends' timeline or in a newsfeed where they think, "There is something wrong here", they can and will take action. Sometimes they will be able to resolve it themselves and we provide tools for them to do that.

There is a very extensive help centre where people can put in any query and we will provide information about how to deal with this, but sometimes they need us to help. That is exactly the same as with neighbourhood watch—you do not always have to call the police, but sometimes you do. That is the same thing for us. We find that is the most efficient way of keeping Facebook as safe as we can. It cannot be 100% safe though.

Lord Sherbourne of Didsbury: You do depend on your users to report that. That is the main area from which you understand what possible abuses might be taking place?

Simon Milner: Yes, and the reason that works well is because most people's experience of Facebook is in their newsfeed—it is in that scrolling series of stories from their friends, from organisations, from politicians, from brands that they are connected with. It is when they see something in that newsfeed that it is going to be much more likely that other people are also seeing that piece of content and that it is something we ought to deal with. There may be something in the darkest recesses of Facebook, but if nobody is there, does it matter as much as what people are seeing in the mainstream on Facebook? That is why the scheme works so well.

Lord Sherbourne of Didsbury: Before I come to my second point, the mirror of that is in dealing with those abuses and resolving them: is that done by humans or by systems?

Sinéad McSweeney: All reports are dealt with by human members of the team.

Lord Sherbourne of Didsbury: There is no electronic system that deals with it at all?

Simon Milner: There is in respect of spam, for instance.

Sinéad McSweeney: Yes, with spam, but for the kind of abuses that you are talking about, they are dealt with by the team.

Lord Sherbourne of Didsbury: Exactly, for those abuses, they will be resolved by a human being?

Simon Milner: Yes.

Sinéad McSweeney: Yes.

Q32 Lord Sherbourne of Didsbury: My second question is very simply this. You have explained to us how you deal with abuses: you decide whether or not to limit people's capability on your sites or whether you decide you are going to close them down. To whom do you account so we know that you are doing it well? To whom do you feel accountable to explain, "We are doing this and we are doing this well, in the right way with the right degree of success"?

Simon Milner: Do you want to go first? I am jumping in, I apologise. I think, frankly, Committee hearings like this are very powerful and important. I undertook a similar hearing with an Oireachtas committee in Ireland with Patricia Cartes from Twitter when she was working for Facebook, and being accountable to policy-makers about how we handle these issues is extremely important. We are very open for anybody that wants to know more to come and visit our Dublin headquarters to meet the team, to see the systems in action.

Lord Sherbourne of Didsbury: Do you volunteer the information or do you have to be asked?

Simon Milner: I suppose people have to ask to come and visit. We have an open door.

Lord Sherbourne of Didsbury: No, I mean in terms of being able to say to the world, "We are doing a good job" do you wait to be asked or do you volunteer the information in some public place?

Simon Milner: There is a Facebook page called Facebook Safety that provides lots of information and well over 1 million people have liked that page. It is run by Facebook. There is lots of information there about the things we are doing to keep people safe, so using our platform to help people understand new features, for instance, like the support dashboard. There is also a Facebook security page, which provides lots of resources for people about both how to keep their account safe; you can download software there; we provide advice; there is lots of information for people on how we are doing this. That is how we account to the general public. We all handle media inquiries every single day about particular issues and we are certainly accountable to law enforcement, so we have a team that works closely with law enforcement on these issues. There certainly is not a single regulator, if you like, that has a view on us in respect of the issues. What we have is almost 360 degrees of accountability to the people on Facebook and these different stakeholders who rightly care about whether we are doing a good job.

Lord Sherbourne of Didsbury: The only reason I asked the question is because I have no idea how effective you are at dealing with abuses. You say you are and I have never been able to doubt it, but I have no evidence on which I am able to judge all the good things you say you are doing in handling abuse and dealing with it.

Simon Milner: Are you on Facebook?

Lord Sherbourne of Didsbury: I am on Twitter, not on Facebook.

Simon Milner: Okay. If you joined Facebook, then I would very much encourage people to do this: report a piece of content and see how the process works. Hopefully you will be reporting a piece of content that does not breach our terms and you are not seeing content you should not be seeing or that should not be on Facebook or people are not behaving to you in a way that is abusive or offensive, but report it and see how that process works closely.

Lord Sherbourne of Didsbury: I am not talking about the process, I am talking about how we are able to judge that you have dealt with the abuses, that you have a good system and the figures, the evidence, the statistics and so on, if they are available at all.

The Chairman: I am going to call on Baroness Hanham.

Lord Sherbourne of Didsbury: I am so sorry.

Q33 Baroness Hanham: I just want to follow up a little bit on this, but it is a question on enforcement. We have been discussing it; I do not know whether you were here when the DPP and the police were here. Can I just take you to the most extreme effect, where something has happened on Facebook or Twitter that is deeply offensive to somebody. They do not go to you; they go to the police and report. What access do you then give to the police to get evidence or support for that allegation, because that brings us more into the territory we are in at the moment, which is: is there anything more that we need to be recommending or that from your point of view you would see in terms of criminality and legislation as an area we ought to be concentrating on?

Sinéad McSweeney: I think there are a couple of elements to that. Our preference would be where people see content that they believe violates the rules on our platform that they report it to us and we can action it.

Baroness Hanham: Yes, that is your preference, but they have not done that, they have gone to the police.

Sinéad McSweeney: But the first step is to weed out the people who are going to the police when they do not need to go the police, when it is not a criminal offence and when it is something that can be dealt with. The Chief Constable mentioned it, and I remember it again from my old days: the role of the police is not just the detection of crime, it is also the prevention of crime, and I think that is somewhere industry can help in terms of preventing these issues becoming police matters, so that is that side. Where it is a criminal offence, we have policies in place and we have guidelines that are public that inform police as to how they can make requests of us for user information that may assist them in their investigation.

In addition to that, however, again going back to, "You can never tell somebody something often enough", we have worked with the Home Office, with the police college doing in-service training seminars and so on, to make sure that frontline police officers are aware that there are single points of contact and units within each UK police service who know how to make contact with the various companies to get information. When we provide that training, we also do add on the bit about, "Please also advise members of the public that some of these issues can be resolved outside of the criminal justice system" and point them to our help centre, point them to our forums and let us try to deal with issues that way.

Simon Milner: The same applies to Facebook.

The Chairman: We are beginning to run out of time, so can you be brief in this response?

Simon Milner: The same applies with Facebook. Law enforcement can make requests of us when they deem that there is a criminal offence. Of course, they have the evidence because somebody has come to them with their screenshots, their Twitter feed and their Facebook messages. They can make requests of us through these single points of contact. We have an online process for law enforcement to do that and the guidelines about how that works are fully public. We also disclose how many requests we get from law enforcement in the UK and on how many of those requests we provide information. I am happy to provide that information now or in writing to the Committee.

The Chairman: That might well be very helpful.

Q34 Lord Dubs: Just picking up on the last point, when you say "a request from law enforcement" are you talking about both from the police and from the courts? In other words, my question is how many such requests do you get—I think they are called Norwich Pharmacal orders—for the disclosure of the ID of users who have posted harassing, threatening or offensive material?

Simon Milner: This, Lord Dubs, is in respect of individuals who want to find this information out rather than the police, because the police do not have to use a Norwich Pharmacal order—they can use RIPA and our online process for requesting this data. In terms of individuals trying to get identifying information, we have only seen a handful of cases in the UK in the last three years where Norwich Pharmacal orders have been used to get that information from Facebook.

Lord Dubs: Let me put it another way: my concern here is how many requests from the UK police or from the courts have you had for the disclosure of ID?

Simon Milner: They are two different things. From the UK police, we have had roughly 3,800 requests last year and we provided information in respect of roughly 70% of those requests. From the court, it is a handful. It is very, very small number, so roughly 3,800 from the police, but as I say, I can give you the exact data, if you would like, on a handful of Norwich Pharmacal orders and I am very happy to write to the Committee to provide that number.

Sinéad McSweeney: Similarly, the vast majority of information requests that we get come from the police using RIPA and in civil matters, yes, the option of the Norwich Pharmacal is there. We have had very, very rare instances—in fact, I do not even know if there was one in the UK. I will have to check.

Lord Dubs: But from the police, do you have any numbers for them?

Sinéad McSweeney: I had, but I cannot find them right at this minute, so I will follow up.

Lord Dubs: If you would, that would be very helpful.

Q35 Baroness Fookes: Could you just clarify for me a point that is puzzling me a little? I thought you both said that the identity of the people using Facebook or Twitter is known and you do not like people hiding behind pseudonyms and so forth. Presumably therefore if you have an alleged abuser, they too will be known.

Simon Milner: On Facebook, yes, we do have that policy. Not everybody abides by our policy, so there are some people who will set up a fake account in order to abuse someone, and in those situations, that name will be meaningless. But also even in a situation where somebody is their authentic self, they may not be providing enough information on their Facebook account in order for the police to identify which Lord Clement-Jones it is—there may be three or four Clement-Joneses, and they need to try to find which one it is. That is why they might come to us for the type of information that enables them to narrow it down.

Baroness Fookes: You would be able to give them that supplementary information to identify correctly?

Simon Milner: Correct.

Baroness Fookes: Thank you. Twitter?

Sinéad McSweeney: We allow people to use our platform under a pseudonym or anonymously, but this is something that we are quite proud of because of the value that it has brought to human rights workers, dissidents, journalists working in conflict areas and so on, and it has allowed them to do a very effective job to get information out without finding themselves at risk in those areas. There are undoubtedly a small number of people who abuse that privilege, and in those circumstances, to the extent that we have information that may assist police and police request that with valid legal process, we can share that with them.

Baroness Fookes: Would you give that information to another individual who might feel affronted or upset or would it be given to the authorities—the police, for example?

Sinéad McSweeney: It has to be pursuant to valid legal process, and generally speaking that is a police request under RIPA.

Simon Milner: It is the same for Facebook. We are subject to data protection laws and that means we cannot just provide somebody's personal information to a third party without a due legal process, so we need a court to require us to do that under something like a Norwich Pharmacal order in the UK.

Baroness Fookes: Thank you.

Q36 Baroness Healy of Primrose Hill: I understand that you obviously make great efforts to ensure that people using your systems understand there are some principles they have to adhere to, but what steps do you take to ensure that your users understand that communications over social media can amount to a criminal offence? At the moment, the push for legislative reform seems currently to focus on sentencing powers, but do you think they should be looking at alternative approaches such as restorative justice or education?

Sinéad McSweeney: It is going back to some of the principles I discussed earlier around encouraging the same kinds of individual responsibility from users in the public space that is Twitter that we would expect of them in a public space that is the local park or the street or the local shopping centre. The written words and resources that we have on the help centre are the work with those whom we know are reaching young people—and indeed older people—on a daily basis, safer internet centres and so on. I think that we need to keep reinforcing the message that the same standards of basic human decency, etiquette and human behaviour that we expect of each other, and as parents that we expect of our children, in the offline world, we expect those in the online world.

Going back to the issues around preventing crime or preventing anti-social behaviour as opposed to just remedying it and enforcing laws and sentencing for it afterwards, I think that is where we would prefer to put our focus.

In terms of alternatives to sentencing, I am aware of very interesting work that has happened in Ireland—and no doubt there are local UK police officers doing exactly the same thing, but nobody hears about it—where they are going into schools and dealing with these issues as juvenile liaison officers, just putting people in rooms, whether it is online or offline bullying, and getting them to talk to each other and using kind of restorative justice models and so on. These are unsung heroes; they are individual police officers who have just taken that upon themselves to take an interesting approach to these issues. They are getting places and they are achieving results.

Simon Milner: Facebook is an open platform; anybody can create an account providing they are over 13 and anybody can create a page on Facebook. Some of the best examples we see

of this type of communication is by police authorities. The Staffordshire Police have a very active social media manager and their page is tremendously informative about what is going on in Staffordshire, whether that is about traffic things, about missing people, about criminals on the run, whatever the issue is, but they can also—and do—use that page to communicate to their many hundreds of thousands of fans about things; the police service in Northern Ireland is also extremely active on Facebook.

I think there is a real scope for, as part of this partnership, authorities that are much more able to be really clear with people about what is allowed and what is not allowed in this country under the law of the land, to have them communicate via our platform. When it comes to Facebook, we should focus on what is allowed in our community and making sure that people understand that if they breach our terms, we will take action, that they understand why we have taken the action we have to remove the piece of content they posted, for instance, and use that as an educative mechanism for people.

It is also worth saying—and I sure this is true for Twitter as well—the vast, vast majority of what people are doing on Facebook is neither breaching our terms nor goes anywhere near issues of criminality.

Q37 The Chairman: A final one from me to wrap up. As you have gathered, we are looking at whether legislative change would be a good idea—whether changes to the law here in the UK would be helpful in dealing social media offences. Would you feel that there are changes to the law that you would support and, if not, is there anything else that you would do, because you obviously do have the best interests of all your many clients in mind. What could we constructively and positively do as a Committee in our recommendations and as a society outside?

Simon Milner: Shall I go first? I would echo what the Director of Public Prosecutions, Alison Saunders, said, which is that we do not see a need for a change in the law or new law. There are various pieces of legislation that can be used to prosecute offences on our service and on other services, because it is not about the medium, it is about the offence. Therefore we do not see a case for any specific regulation or legislation relating to social media. Any attempt to do so would inevitably become out of date very quickly, especially if it was specific to a particular type of social media. Therefore we think it is much more about education, about using the examples of people who have overstepped the mark and how they have engaged in public debate around a particular issue—and we certainly have seen that in recent months—and what happens to them. They are not immune from the law; they will end up in court; their names will become public; they will be in the media; they will be extremely embarrassed, and we should use those examples to help particularly young people, who are often the ones who will escalate things, understand there are consequences if you overstep the mark. We all have a responsibility to do that.

Sinéad McSweeney: I would echo those. We have seen some high-profile prosecutions under existing legislation in the last 12 months and, as I think was discussed in the last panel, there is an educative process in those steps.

In terms of the magic wand wishes, I think it would also be on the education side, the awareness-raising side. I guess you are always going to have a core of people, whether it is online in terms of trolling or offline in terms of antisocial behaviour or public order, who are intent on wrongdoing and criminality, but it is the next circle of people around them that we have to protect and save almost. Criminalising those people potentially at an early time in their career is not necessarily the best step, which is why we would prefer to see a lot more

emphasis and focus on the concept that citizenship and good behaviour is something that exists both online and offline.

The Chairman: Very well put, both of you. Thank you both very much indeed, that was a terrific session. Thank you.

Twitter International Company and Facebook – oral evidence (QQ 25-37)

Transcript to be found under Facebook