



Communications Committee

Corrected oral evidence:

The internet: to regulate or not to regulate?

Tuesday 19 June 2018

3.30 pm

[Watch the meeting](#)

Members present: Lord Gilbert of Panteg (Chairman); Lord Allen of Kensington; Baroness Bertin; Baroness Bonham-Carter of Yarnbury; The Lord Bishop of Chelmsford; Viscount Colville of Culross; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin.

Evidence Session No. 8

Heard in Public

Questions 58 - 70

Witnesses

I: Jenny Afia, Partner, Schillings; Mark Stephens CBE, Partner, Howard Kennedy LLP.

USE OF THE TRANSCRIPT

This is a corrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.

Examination of Witnesses

Jenny Afia and Mark Stephens.

Q58 The Chairman: Can I welcome our witnesses to this session of our inquiry into the regulation of the internet? I will ask our witnesses to introduce themselves in a moment. Just so they are aware, the session today is being broadcast online and a transcript will be taken. I am very grateful to our witnesses for coming along and giving us evidence.

Could I ask Jenny Afia and Mark Stephens briefly to introduce themselves and tell us a bit about their background, and in so doing, just so we know where they come from on this very broad subject, tell us whether there is a need to introduce a new regulatory framework for the internet and the wider digital economy? If so, what form should it take? Should it be largely imposed regulation, self-regulation or co-regulation? Is there a need for a new body to establish that regulation or to co-ordinate the work of existing regulators in the field?

Jenny Afia: Good afternoon. I am a partner at the law firm Schillings, where we specialise in safeguarding privacy. Our clients include some of the world's most successful people. Even for them, with all their resources, trying to have information removed from the internet can be very distressing and very difficult. I really worry what the experience is like for people with fewer resources, most particularly children. I have worked with the Children's Commissioner on her digital task force and I have provided support to the 5Rights Foundation led by Lady Kidron. Most recently, we co-authored a report entitled *Disrupted Childhood*, which looked at the impact of persuasive design strategies on children's mental and physical health.

The first project I did for the 5Rights Foundation, which is relevant to your question, entailed a review of the existing legislation at the time to see what support there was for the 5Rights framework. This was in 2014 and 2015. My conclusion then was that we did not need new laws; we needed better application of the laws and better awareness of what the laws were. If you ask me now whether we need a new regulatory framework, I still think we probably do not need new laws, although had you asked me about a year ago, in between the two questions, I would have said yes. Since then we have had the GDPR, with its emphasis on privacy by design; we have had the Data Protection Act with the age-appropriate design code. I know there are several reviews going on, looking into the issues of artificial intelligence, and there is the Law Commission review.

I have also seen how industry has improved its standards. For example, there is the new operating software coming out by Apple in the autumn. Some of the changes Instagram has made, for instance its attempts to tackle bullying, have been really impressive. At the moment, we have sufficient regulation. The problem is that it is all a little reactive and piecemeal, and I do not know what lies ahead because I do not have sufficient technical expertise, and neither do my clients, to see what is

coming down the line. If we are happy with this reactive model that does not seem to encompass a root-and-branch approach to the internet, at the moment we do not need a new regulatory framework.

Mark Stephens: Thank you for inviting me here today. My name is Mark Stephens. I am a partner in the London law firm of Howard Kennedy. Perhaps also relevantly, I was the founding chair of the Internet Watch Foundation back in 1996—almost before the internet was born and certainly before Facebook, Google, Twitter and all the others—with its avowed intent to remove paedophile material from the internet. I have been working as an adviser with the UN counter-terrorism executive directorate, and we hold meetings on extremist content around the world. I work with ICT4Peace and, last but not least, I am the independent chair of the Global Network Initiative, which is also a multi-stakeholder initiative that brings together academics; ethical investors such as the Church of Sweden and their ethical investment funds; corporates and NGOs that are informed in this space; and people from the ICT sector.

You asked about the need for a regulatory framework. The best place to start with this is that there is a need to look at that word “regulation”, because it can mean a wide spectrum of arrangements between the relevant actors. At one end of the scale it can include voluntary commitments by companies, and at the other end it can mean binding laws with government enforcement. Between those poles lies a range of possible arrangements which exhibit various degrees of flexibility, transparency and accountability. I would draw attention to the fact that the Internet Watch Foundation was founded specifically to deal with one of the most pernicious problems at the time, namely paedophile material. I think it can be said to have been a success in that space.

In relation to the *Internet Safety Strategy* Green Paper that Karen Bradley published, there were some interesting things. There were three things that she really focused on. First, what is unacceptable offline should also be unacceptable online. That gets a tick; we all agree with that. All users should be empowered to manage their online risks and stay safe. That gets a tick; we all agree with that. Technology companies have a responsibility to their users. That gets a tick; we would all agree with that, although the real question there is to what extent they have that obligation, how they show they are doing it and how they empower people. I would, though, add a fourth: if there is to be legislation, it should be clear and unambiguous so that people and companies may properly identify and regulate their behaviours.

Yesterday, I was in Germany, where we were looking at the NetzDG legislation, and I will perhaps come back to that in a minute. But what is interesting is that technology companies have already acknowledged that they have a responsibility in this space to their users. They are using transparency reports; they are taking on hash sharing; and they are policing their own community standards, which invariably stand well within the bounds of the law. Therefore, the principled approach is to identify a lacuna in the existing law or some pressing social need, and

then, if there is a pressing social need, to find a way in which we ought to proportionately fill it.

A note of caution here is that legislation can often be slow and cumbersome; Jenny was adverting to that a moment ago. In this fast space, private responses may well be more potent than government ones because they can respond more swiftly and in a targeted way. One of the questions we have to ask ourselves is this: is there a way of encouraging those companies to perform in that middle space without formal regulation but perhaps within a framework? One framework I was looking at, and have been looking at for some time, is that of the Ruggie principles, the UN guiding principles on business and human rights, which apply to companies, alongside their obligations to report and ensure compliance with human rights and the law more generally.

At this point I have concluded that, certainly looking at the NetzDG legislation, it is not working very well and it is not a lesson we would be wise to follow. It is interesting that you have David Kaye, the UN special rapporteur on free speech, and the German data protection officer—their version of the Information Commissioner—criticising the law. You have seven out of 10 German law experts in the Bundestag criticising the law, as well as really top legal German academics concluding that the law does not achieve its objective, promotes overbroad blocking and has passed the responsibility to prosecute criminal offences from the Government to the private sector, of course with a chilling effect on private speech.

I am concluding, Chairman. This is all against the backdrop that two FDP parliamentarians—those are the liberals to us here; I am sure you all knew that but I did not—last week in Cologne applied to have the law struck down. It does not even look like it will last a whole year. That would not be a good place to be in. It is interesting that the renowned German legal scholar Professor Gerald Spindler has noted that NetzDG is likely to breach EU data legislation, particularly the e-commerce directive, the GDPR, the e-privacy directive and other legislation. We have to think about how those intertwine at the moment.

The Chairman: Thank you both for very helpful opening contributions.

Q59 **Lord Gordon of Strathblane:** This is a question, perhaps first of all, for Mark Stephens, as you were the founding chair of the Internet Watch Foundation. The present CEO gave evidence a few weeks back and made a fairly passionate plea: “Our plea is that our self-regulatory approach is acknowledged as working”; it “is not broken and does not need fixing”. Is that self-regulatory approach unique to that particular segment of the problem or could it be expanded?

Mark Stephens: First, IWF is not self-regulatory. It is paid for by the industry, but it is actually a multi-stakeholder environment. That would be a more appropriate response. It has child protection people involved in it—they are very important, and I mean people at Childline and other organisations—as well as the industry. It recognised that there needed to

be a partnership between the people who were seeking an outcome, which in fact was everybody. Everybody is looking for the same outcome. They all want to remove paedophile material, and they want to work together and draw on the expertise around the table to achieve that in the most efficacious way.

If you look at the Global Network Initiative, it does the same thing: it brings together different kinds of expertise. The challenge is that the problems are disparate. Therefore, I am not convinced that having one umbrella organisation actually produces the outcome you want. The GNI is about as close as it gets, because it is multinational. It has all the major ICT companies from Europe, from BT and Vodafone right the way through to Telia, and it then has the big American platforms such as Google, Microsoft and Facebook, along with those other independent experts who hold them to account. It is important; it works on its own terms. But I am not sure there is a broader role at this particular point in time.

Jenny Afia: I do not believe that, on several issues, self-regulation has worked with the internet to date. My biggest concern is that children's best interests have been ignored probably because of the utopian vision that all internet users would be treated equally and, de facto, if everyone is treated the same, children are treated in the same way as adults. That has led to very significant issues, but I hope those issues are going to be addressed by the age-appropriate design code. I do not believe self-regulation has worked at all. Children's best interests have been sacrificed for commercial gain. But I am optimistic that the situation is being addressed, on a piecemeal basis.

Lord Gordon of Strathblane: Would you agree that it has worked in the case of the Internet Watch Foundation? I accept the caveat that it is not entirely self-regulatory.

Jenny Afia: People who know more about it than I do hold it up as the industry standard. I really do not have any more to add.

Mark Stephens: That is very kind of you.

Lord Gordon of Strathblane: I was wondering whether there might be a way forward through protecting the individual citizen rather than looking at the regulation of internet companies. Is the idea of an internet Bill of Rights a feasible option?

Mark Stephens: You have to go at it with this principled approach. The way I have looked at it is to ask, "What are the basic rights we have as citizens?" I am not sure an internet Bill of Rights gives us anything more than we already have. Again, I come back to the UN guiding principles on business and human rights, which are grossly overlooked by many companies that have voluntarily taken them on. They impose an international law obligation on companies, particularly transnational companies, to behave ethically and appropriately in accordance with the law. That is where the problems lie.

One challenge in much of what Jenny was referring to, particularly around children, with which we would all agree, is that the publishers are often the problem and not the people who are conveying the information. We see that whether we are dealing with extremist content or vulnerable groups within society.

Jenny Afia: I am not keen on the idea of an internet Bill of Rights, because rights should apply irrespective of the environment. This is not how children understand their worlds. The distinction between the offline and online world will fairly soon become antiquated, so the emphasis should be on universal and fundamental human rights.

Q60 **Viscount Colville of Culross:** Good afternoon. We have heard from a number of witnesses that internet intermediaries should be much more liable legally for the content they have on them. The ICO, for instance, has said they “produce content, filter what individuals view and in some cases micro-target individuals with advertising”. Should the safe harbour protections in the EU e-commerce directive be amended or abolished altogether? In that case, is there something else that could replace it to try to increase that liability? Mark, you talked about the German NetzDG law going far too far. Is there something in between that would allow us to give more liability to the internet intermediaries?

Mark Stephens: One of the flaws of the NetzDG law, to be completely candid about it, is that it covers 22 different offences under the German criminal code, and that just lends itself to a lack of clarity and a clash with other areas of the law.

Going back to your question, it helps. The safe harbour has been quite helpful in this space. I have been working with the UN counter-terrorism executive directorate, and we have had some security briefings. There are obviously some things I cannot say in open session, but there are some quite important things I can share. One is that jihadi extremists who create original content are numbered at about 70. We know where they are located by reference to the cell towers through which they upload material. That original content is amplified by about 200 to 250 further individuals, and then it spreads its disease from there. The interesting thing is that the jihadis could migrate to smaller platforms and perhaps areas where regulation was less thorough, but they do not do that. Intercepts tell us that they want to be on the larger platforms, because they feel they have a greater reach and, as a consequence, they complain internally about how quickly their accounts are being taken down. It is not just the individual posts and the videos, but the whole account is being taken down. A game of whack-a-mole is being played.

For that reason, we are seeing the platforms taking urgent action, and we need to encourage them to do that. As a consequence of that, giving intermediary liability is not very helpful. I go back to the days of paedophilia on the internet. The Internet Watch Foundation was born of the fact that the police wanted to prosecute internet companies for “hosting” material they did not even know they had. It was recognised and conceived, I think very wisely, that a much broader partnership in

the public good was to not prosecute, to give them that immunity and to allow them to co-operate with law enforcement and report all the material they find, so those people who share that kind of disgraceful material can be found.

We have decided, for good and decent reasons, not to turn the cell towers off for the individuals where we know where they are located, partly because we are going to get good intelligence from them, and we do. It would be wrong to burden the platforms with the obligation of not only playing whack-a-mole, which they are doing as best they can, but also with some measure of liability. That is the opening concern I have in relation to starting to down that route.

Jenny Afia: I like the concept in principle. From my sense of justice, it makes sense to me. My experience on the ground is that content is not removed quickly enough. I am also told by social media companies that efforts are being made to change that, and I very much hope that is the case. Day to day, our experience is that it takes a long time and a lot of banging on doors or knocking on algorithms to have content removed.

Viscount Colville of Culross: Should we have a duty of care established by statute to stop online harm? If so, how might that code work?

Jenny Afia: I am interested in the idea on the basis that, if we draw an analogy with the physical world, we have the concept of a duty of care. There is a duty of care to take steps to avoid harm in the workplace, in public spaces, in parks and when you build homes. To the point I made earlier about there no longer being a distinction between the online and offline worlds, it would make sense to extend that duty of care in principle. It would still be worth, particularly given Mark's point about unintended consequences, identifying the harms that are not currently being addressed. If we are satisfied that there is a lacuna, in principle the idea is quite appealing.

Mark Stephens: One of the challenges around a duty of care is that it requires you to be aware of the problem you have. Let us take hate speech for a moment. The platforms are all aware that they have the problem, in line with their obligations under the Ruggie principles, the UN guiding principles on business and human rights. They are taking actions. We can argue about whether it is enough, but they are taking actions. As a consequence, I wonder what we get from ratcheting up the obligations on them. They have a view internally, and it is quite clear to me that they do not want this material on their platforms, because it falls in breach of their own community standards. We had a rather bizarre situation of a case in Berlin a few months ago, in which it was determined that Facebook had taken down something under the NetzDG law that was lawful, but Facebook still kept it down on the grounds that it was in breach of its own community standards. We are likely to get into problems with this.

Q61 **The Lord Bishop of Chelmsford:** I wonder if we can keep going with the topic we have just come on to, the moderation of content. Jenny,

certainly in your written submission, this is something you were particularly writing about. I have two questions, really. Are the processes used by the online platforms to moderate online content fair, effective and transparent? Particularly, what processes should be implemented for individuals or organisations that wish to reverse decisions? Who should be responsible for that? I want to hear from both of you but, Jenny, given what you have been saying, it would be great to hear what you think could or should be done.

Jenny Afia: The processes used to moderate content are not that fair currently, because they do not even seem to comply with their own terms of use. We have seen a few examples of this. Recently, we had a female client, and somebody on Twitter and then posting on YouTube was calling for her to be genitally mutilated. Both YouTube and Twitter said that did not contravene their terms. We have had photos identifying the home of a client, a high-profile businessman, with frightening accuracy. Those photos were published on YouTube, and we were told they did not violate privacy policies. We have various examples where content is not removed that, on the face of their own community guidelines, would seem to contravene them, which does not feel fair.

Are the processes effective? They are effective sometimes or often, but not often enough. It is concerning. It is horrid. I hate getting internet cases, and there are loads of them, because you do not have a degree of confidence that you can help a client even though the law is on the client's side. The processes are not that effective and they are definitely not transparent. You do not know if a human has made a decision on your complaint or it has just been determined by an algorithm. It feels like there should be a process for internet users who want to reverse decisions to moderate content, short of having to bring litigation.

I know Australia has the e-safety commissioner model, which is a form of ombudsman that you can take complaints to. I asked some Australian practitioners about their experience of it, and it has been fairly limited so far, so I do not feel that qualified to say how effective it has been. But it feels like it would better protect both the right to privacy and the right to freedom of expression if there was another body in place that could help determine complaints.

The Lord Bishop of Chelmsford: I have a supplementary, but I would like to hear what Mark has to say first.

Mark Stephens: I will try to keep it as brief as I can. Content moderation across platforms varies quite considerably. That is more so because companies are at different stages of evolution. I would exhort the Committee to think that the most profitable way forward is perhaps to focus on methods of reporting. How do you get to the page to report it? How do you know it is being responded to? If you were going to a regulator, whether it was self-regulation or statutory regulation, you would expect a certain degree of outcomes; you would expect progress reports. You would expect all those things that could helpfully be expected of them.

It is interesting to note, from my experience, that European ICT companies have more experience in transparency reporting than those in the US. They are rushing to catch up, but a good example is that Google will allow anyone in the company, or indeed outside, to put forward suggestions as to how reporting can be improved. For example, to Jenny's point about not knowing whether it is an algorithm or a human, in fact everything is reviewed by a human. The problem is that humans are fallible, as are algorithms, I suspect.

This is the challenge here: how do you direct the travel towards a greater amount of takedown? The best work I could refer to you that I have seen is the Berkman Klein Center's report *Account Deactivation and Content Removal*, from 2011. I have not seen anything subsequent to that, but it was pretty comprehensive and it was well done. The gap in this part is that each company has its own transparency reporting; you cannot read across from one to the other. We should be able to make that read-across, to determine who the best actors are, where the industry's gold standard is and where the suboptimal players are.

The Lord Bishop of Chelmsford: Human fallibility is my specialist subject. This may be the naive question to end all naive questions. There seems to be this debate going on about the need for freedom of expression and how we moderate and regulate content. But part of me—we have heard this from other witnesses—wondered whether it could work the other way. The algorithms could be geared not to wait until the content comes up and then ask, "Could you take it down?" Could the algorithms work much harder to stop the content going up in the first place? Then you appeal to have it put up if a mistake has clearly been made. Is that a completely ridiculous thing to suggest?

Jenny Afia: No, it is not. People at Instagram, for example, are working on that at the moment. They have introduced what they call bullying filters. They have identified certain words that are so obviously offensive they cannot even be uploaded. That goes to your point about that really early intervention stage. There is a problem, they explained to me, given where the technology is at the moment. Suppose you had a scenario where a child was bullied at school all day and they were being called a dog all day. They get home and they receive one message via social media that says "woof". The system cannot yet identify how distressing that would be for the child, but I believe they are trying to work on precisely those proactive measures. I hope that will set the market standard.

Mark Stephens: It is important to say that those things are coming and we are going to see design building them in to address these issues, as you say Instagram is doing. But there is also a need for a review. If somebody has something taken down and we effectively have monopolistic platforms, how does somebody get redress in those circumstances? There has to be some kind of ombudsman. If you look at newspapers, for example, they have independent ombudsmen, but we see them in all sorts of sectors. I see no reason why this ICT sector

should not have an independent ombudsman who could address complaints where people think their material has been wrongly taken down.

- Q62 **Baroness Kidron:** I am just going to declare my interest, in that I know Jenny Afia very well. Mark, can I ask you a tiny question about whether you think there is a role for consumer law in this? I was interested in what you were saying about universal standards of reporting. What about universal standards for terms and conditions or community rules? We could perhaps say, "If you post community rules, you have to stick to and live by your community rules". Is that a way to avoid the German problem, as we might put it, and get companies to do what they say they are going to do? Is that an interesting way forward?

Mark Stephens: It is an interesting way forward and it is increasingly going to be an important way forward as we get to the internet of things, where our fridge or our home could be hacked. We may have a device that streams music or other communications into our homes. Increasingly, that kind of information is going to be available. Take cars, for example, and the data around them. It will be important that we have security around that data. Whether that falls into what some might call data protection laws, into encryption or indeed into consumer law, it probably has an overarching consumer perspective, because we should know what we are giving up and what the remedies are for breaches of those laws.

- Q63 **Baroness Bonham-Carter of Yarnbury:** This is something that has come up in previous sessions. You have been talking about Google and Instagram, the big companies, but of course there are myriad little companies out there too. How do they feed into this? You sound quite optimistic about the way forward, although, Jenny, you mentioned that we have to be happy that we are being a bit reactive. I just wondered how the smaller companies fit into your scenario of self-regulation.

Jenny Afia: I tend not to have a huge amount of dealings with the small companies, mainly because by the time a client comes to me they are concerned about information going out to a huge market. If it is a very small platform in terms of audience, they tend to have the fortitude to ignore it. I do not have a huge amount of experience of those small companies. I have experience of the pesky, annoying ones that are outside the court's jurisdiction and so on. The issue with small companies is to build in safety and privacy by design and hope the foundations are right for all companies.

Baroness Bonham-Carter of Yarnbury: I suppose this is going back to children and so on.

Mark Stephens: Little companies are the vulnerable spot here. You are right to alight upon it. They invariably do not have the bandwidth or the resources to manage the challenges their technology may produce. This has been recognised in the ICT sector, where there has been a considerable amount of sharing of knowledge and technology, particularly

when working in foreign markets, but also in relation to the terms of business. A small company may not have the capacity to pay many guineas to lawyers such as Jenny and me to draft terms of business, but they have the ability to share the technology of their terms of business and how they have developed. That goes back to the point that was made to me earlier about holding people to account to their terms of business. If they are state of the art, you can hold them to account to those contractual terms.

Q64 Baroness Bertin: I would like to start by declaring that I work for BT. Can we come back to the design point? We are all agreed that this could be a force for good but, let's face it, ethical design might not be the most profitable. It is about trying to work out who should be responsible for overseeing this process. What principles and values should define the safety by design principle?

Jenny Afia: In terms of who should be responsible for overseeing the process, either we have a huge global regulator or it is on each sector. If we are talking about fridges, it might be the food standards industry; if we are talking about social media, it might be in the Digital Economy Act. In terms of the principles that should go into safety by design, from my perspective children's interests should be paramount, as recognised by article 24 of the European Charter of Fundamental Rights. It will not be any surprise that I, as a privacy lawyer, would like the right to privacy and to freedom of expression to be baked into privacy and safety by design.

Mark Stephens: Increasingly, we are at a point where safety by design is coming forward. At the Global Network Initiative, we have encouraged companies to come forward with their proposals for the standards by which they should be judged. It is an evolving sector, as you will understand very clearly, but it is absolutely critical that we now start to have companies state exactly where they stand on these issues and what they are going to do to protect us. Whether that is, at one end of the scale, self-driving cars or, at the other end, the sorts of things Jenny is talking about, you have to have that design baked in, and increasingly it will be.

We then have the problem of how you communicate that. There is a whole issue around communicating what people are doing to protect you, but also what they are then going to do with your data. We have just seen the tip of a very large iceberg with GDPR. People have made a lot about it but, when you drill into those consents and see who is sharing the information and what they are doing with it, it is considerably broader than what anyone in the street really has any conception of.

Q65 Lord Allen of Kensington: In your opening statements, you both talked about the key principle of having the same protection online as offline. I am interested in understanding whether the current legislation affords that protection in both areas.

Mark Stephens: It does, by and large. That is where I came back—my analysis says this is the core principle. Can we identify a lacuna where that is not the case? We could take a topical example: upskirting. If you happen to be in England and Wales, and not in Scotland, it seems to me that, aside from it being a criminal offence, you might think digital dissemination of that should be a separate criminal offence. Therefore, that is something you might want to include in those kinds of things and it may be a gap in the law. I have not thought about it in enormous detail, but that seems to be something you could do. But there is no point in making extra laws just for the sake of extra laws. We have to say what we are likely to do.

To the point Jenny made right at the beginning, we do not know what will happen. We cannot predict the future; we are not prognosticators. We have to work with what we have and then encourage the companies, which to some extent share our own concerns about this, to ensure they are complying with their own terms of business.

Jenny Afia: We have the same theoretical protection online as we do offline, but the major issue is that the internet highlights the problem of the conflict of laws. If somebody in America defamed me in an after-dinner speech to a room of 30 people, I would have the same rights as if someone defamed me on an American blog. The principle is the same, but I would probably hear about it more if it happened on a blog. The internet brings into sharp focus the conflict between American laws and our laws, but theoretically we have the same protection.

Lord Allen of Kensington: Can I build on that? What are the practical challenges in prosecuting and suing people who have done something illegal or defamatory online? Can you explore that a little more?

Jenny Afia: It is incredibly difficult if they want to be anonymous. It is so easy to hide your identity on the internet, which makes taking meaningful action extremely difficult. You face the whack-a-mole problem and you are constantly chasing your tail. It means it is expensive, because you have to go after different platforms. There is also the effect we have dealt with for many years known as the Streisand effect: the fear that, if you take action to remove content on the internet, there will be a whole group of people who will delight in magnifying that content and making it a much bigger issue. There remain a lot of practical deterrents to even trying to have information removed.

Mark Stephens: We have seen a lot of this in relation to harassment cases. For example, a woman we were representing had defamatory comments made about her in the UK. They were injuncted. It kept going, so the police became involved. The individual fled to southern Ireland, where the police became involved again. He then fled to Hungary, where the matter has languished for the past several years with him firing shots at intermittent moments. I suppose the takeaway I have from that is that we need to look at the international co-operation between states both at a police level, with the European arrest warrant, and perhaps in relation to mutual legal assistance. After Brexit, although we will be a separate

legislative nation, we need to maintain those connections to ensure our citizens do not lose out.

- Q66 **Baroness Quin:** My question really follows on from the mention there of Brexit and the situation of the UK after that. What effect will the UK leaving the EU have on the regulation of the internet? I noted that Jenny mentioned the European Charter of Fundamental Rights, and mention has just been made of things such as the European arrest warrant and the difficulties of getting them to take effect sometimes. It is fair to say we have probably had two versions of life after Brexit. One suggests there will be problems because we will not have the same influence in rule-making as before and we will not have the strength of belonging to a big bloc; on the other hand, other witnesses have talked about us taking the opportunity to become a global leader in internet regulation. What are your thoughts about this?

Jenny Afia: I have personal views but not a huge amount to add from a professional perspective, other than that the Brussels recast regulation is in flux, and that will have huge implications for enforcing civil and commercial cases against defendants. I assume something will happen in relation to the Rome regulation. As to the UK's role in all of it, I will leave that for others more qualified than I am to opine on.

Baroness Quin: Can you elaborate on what you meant by the recast regulations, the timing of decisions that are likely to occur and whether they will occur at a time when we are in the EU or out of the EU?

Jenny Afia: I am sorry; I am confused.

Baroness Quin: What exactly were you referring to there? I did not quite understand it.

Jenny Afia: The Brussels recast regulation, I understand, is one of the pieces of law that allow us to take action against Facebook in Ireland. If that were to change post-Brexit, it would be harder to take action.

Baroness Quin: I see. Is that something you have also thought about?

Mark Stephens: Yes; all the major American technology companies are based in Ireland, principally for tax reasons. As a consequence, if you wish to enforce, you invariably have to go to Dublin to do so, because that is effectively the chosen epicentre of the west coast companies. Being out of the EU, or it becoming more challenging to take those enforcement proceedings in a non-European Union context, could make things very difficult.

There are a couple of things I would add in order to address your question. The Americans are moving inexorably towards EU standards. They have recognised that they have to broadly comply with the GDPR if they are international businesses. If they are domestic American businesses, that is very different. The e-commerce directive, the e-privacy directive and other EU legislative standards are coalescing around an international norm. As one of my friends, a New York judge,

said to me, "When in Rome, do what the Romanians do". That is where the American internet companies are getting to, and they will align themselves with European legislation because they do not want to go as far as some of the other countries that are popping up, whether that be Russia, China, Turkey or wherever. They see that as a good middle ground.

For us, it is about ensuring that our citizens have the protections they have now afterwards. I do not see the EU allowing us or us wanting us to become some kind of state where we are allowing a wild west of the internet or, the other way, going to a more regulated environment. If we go to a more heavily regulated environment than the rest of Europe, in those circumstances, we will drive the economies yet further offshore because they will migrate to those more beneficial, benign regulatory environments.

Baroness Quin: Whether we are in or out of the EU, we are likely to remain fairly close in terms of regulations and legislation.

Mark Stephens: That is right. In order to do business with the EU, we will clearly have to comply with its GDPR and other e-commerce-type standards. This is one of those spaces where, while we may have our sovereignty and be able to make a decision, the wise decision is to maintain the standards of equivalence that the EU has.

Q67 Lord Goodlad: This is perhaps a question for Jenny, who has given us evidence on the jurisdictional challenges of applying British law to social media companies and other intermediaries. Most of them seem to opt for the United States courts as where the proper law of the contract, or whatever it is, should be. How do you see the way through this, if at all? Secondly, what should be the function of international organisations in the regulation of the internet, and the role of the British Government? Should it be the OECD or somebody else?

Jenny Afia: I am struggling to see a clear way through the challenges of applying English law. Unless we are willing to have huge, substantive change, I do not see how we get over an issue such as the SPEECH Act, for example, which was introduced several years ago. It put trying to enforce a defamation judgment on a par with an act of terrorism, if you try to enforce your rights in America. That was introduced by President Obama. It is a huge issue that we have faced for many years. The way we have dealt with it on the ground is we have had to ignore what is going on in the rest of the world.

A couple of years ago there was the case of *PJS v News Group Newspapers*, which went to the Supreme Court, which was all about trying to protect private information. The media argued very strongly that it was farcical to try to do so when the rest of the world, and even people in England going on Twitter, could view the content you were trying to stop. The court reached what in my view was the correct decision: that is as may be, but currently we are in a position to exert control over the British media and we think there is still a virtue in doing that. We are sort

of dealing with the problem by just trying to control what we can and resigning ourselves to the rest of it. It is not a satisfactory solution, but I am afraid I do not see a way out of it.

Lord Goodlad: Do you see any role for the OECD in all this?

Jenny Afia: I do not see a clear one.

Q68 **Lord Gordon of Strathblane:** Can I ask a supplementary? As a non-lawyer, if I take copyright, where the thing originates is irrelevant. It is where it is heard that you incur the copyright charge. Surely the same should be true of offensive material on the internet. Would the same logic not apply?

Jenny Afia: You would think so, but material that is subject to copyright is very easy to have removed from the internet because America places great value on intellectual property. Often, the way we try to get around the problems with protecting privacy is to find a way to assert copyright. It should be the same approach. It seems odd that it is not.

Mark Stephens: It is important to recognise that the SPEECH Act only applies to defamation; it does not apply to privacy. If you get a privacy injunction here in London, it will be enforced, along with the damage award, in America. The challenge we are likely to encounter is in relation to long reach and the jurisdiction. At the moment, with the PJS case that Jenny adverted to, we are limited to an injunction in the United Kingdom. But I found myself at Hudson News at JFK when that magazine came out, and there was a jumbo jet queue out of the door of people buying the magazine and bringing it back to London. That is problematic, and that is a real-world example of what is happening on the internet.

I know we are here talking about British law and how we change British law, but there is another issue here that we have to think about. If we start to take Turkish, Egyptian, Iranian, Russian or Chinese law and their decisions, and incorporate them and respect them here, there is going to be a challenge. Throwing away the jurisdictional reach of our laws needs very careful consideration before we do it.

Q69 **Baroness Kidron:** At the beginning, both of you said that there is not really a call for new regulation. Forgive me for doing a bit of a "best of", but you talked about harmonising laws, lacunae, universal standards, the IoT consumer piece and enforcement. We can go through a whole shopping list of things you have both suggested might require doing. I want to finish by coming back to the question of who is responsible. Who holds this brief? One of the things we keep on hearing is that it is so split across people: some of it does not sit with anyone, and then it sits with lots of different people.

Finally, to Jenny's point about reactivity versus proactivity, is there an argument, as we have heard from some witnesses and definitely in some written evidence, for having a new person, whatever the outcome is on regulation, to hold the brief for all this in one place and to work their way carefully through all these issues? You are asking for a certain level of

proactive action, reaction and thoughtfulness around the whole piece.

Jenny Afia: The brief would be for that person to be an anticipatory body. There is a real need for horizon scanning and to look ahead, so we are not just dealing with these issues through piecemeal legislation and the 11-plus bodies that touch on the internet. If that is the brief, it would be fantastic to have a body that was charged with looking forward and anticipating issues. That body would work with the existing regulators to ensure they had sufficient digital skills and could harmonise and provide an overview. That would be fantastic. It almost feels like a luxury, when you start seeing how much work is already going on. When we are talking about such important issues, maybe it is essential.

The Chairman: Horizon scanning is clearly important in this area, whether it is an individual or a body horizon scanning. Would they be well guided by a set of principles—either drawn from existing principles or a new set of societally agreed principles—that they are trying to apply to how they see the future developing in so many of these areas?

Jenny Afia: Yes, but I would say those principles are probably human rights: the right to privacy, the right to respect for private and family life and the right to dignity. They are the rights we already have. We do not need new principles.

The Chairman: It is all already there.

Mark Stephens: You are right: there is a “pulling the strings together” piece that needs to be done here. In your first question, you asked about regulation. The question here is how you draw those things together, such that it ends up being a more fleet-of-foot and proportionate response to the huge number of challenges, some of which we have isolated today.

I hate to suggest it, but we could have an internet tsar with an obligation and a remit to do some scanning of the horizon, and to look at whether the terms and conditions of business that ordinary folk do not read—I was going to say “none of us”, but we do—and just click “accept” are acceptable and being complied with. This internet tsar could build those relationships with the internet companies to draw attention to and understand where problems are, and alert Parliament where there are lacunae coming up or where there are problems, so you have an independent voice saying, “Actually, we need to do something about this” or “Actually, we can deal with this in another way”. That is perhaps the most effective way of achieving a positive outcome to what is obviously a shared concern. At the end of the day, everybody wants the right outcome; everybody wants to remove material that is unacceptable.

The Chairman: Thank you. We are drawing to a close, because our next witnesses are here.

Q70 **Baroness McIntosh of Hudnall:** This is very brief. Maybe there is no answer or you could write to us with an answer, but I was just wondering about case law. What quantum of case law exists already, in respect of

any of the issues we have been discussing? Who, if anybody, knows what that quantum is? How is it held and how is it accessed?

Jenny Afia: There is quite a body. I would be very happy to write and provide details.

Mark Stephens: One of the challenges is that the law is developing down different routes in different countries. We need a greater overview to inform the Committee, and more broadly, about the different ways the same problems are being dealt with in the same places.

Baroness McIntosh of Hudnall: Anything you can tell us about it would be welcome.

The Chairman: On behalf of the Committee, can I thank both of our witnesses for very helpful and very concise evidence, which we will certainly be relying on as we take the inquiry forward? We would welcome any further points that you wish to make. Please feel free to write to us if there is anything you think we omitted in our questioning, or anything in hindsight that you might have included in your answers. We have a voracious appetite for reading so, similarly, if there is any material published in your domain that you think might be of interest to the Committee, it would be helpful if you sent it to the clerk.

We have learned that there is somebody out there who reads the terms and conditions. Up until now, we were told that nobody reads them, so that was useful too. Thank you both very much indeed. Your evidence was very helpful.