Fraud Act 2006 and Digital Fraud Committee

Corrected oral evidence: Fraud Act 2006 and digital fraud

Wednesday 17 March 2022

9.15 am

Watch the meeting

Members present: Baroness Morgan of Cotes (The Chair); Lord Allan of Hallam; Baroness Bowles of Berkhamsted; Lord Browne of Ladyton; Viscount Colville of Culross; Lord Gilbert of Panteg; Baroness Henig; Lord Sandhurst; Baroness Taylor of Bolton; Lord Vaux of Harrowden; Lord Young of Cookham.

Evidence Session No. 6 Virtual Proceeding Questions 52 - 60

Examination of witnesses

Lulu Freemont, Professor Lorna Woods and Professor Victoria Nash.

The Chair: Welcome to this evidence session of the Select Committee on the Fraud Act 2006 and digital fraud. A transcript will be taken and published on the committee's website and you will have the opportunity to make corrections to that transcript where necessary.

Thank you very much to our three witnesses for the session this morning on digital regulation. We are joined by Professor Victoria Nash, who is a director at Oxford Internet Institute, Professor Lorna Woods, who is professor of internet law at the University of Essex, and Lulu Freemont, who is head of digital regulation at techUK. Without further ado, Lord Gilbert will ask our first question.

Q52 **Lord Gilbert of Panteg:** Good morning, witnesses. My question is primarily for Professor Nash, but other witnesses may want to contribute, too. Professor Nash, I am trying to establish how and indeed whether a platform should be held responsible for harmful, especially fraudulent, content on their websites, either through advertisement or user-to-user content. Should they be held to account for fraud they have facilitated, and, if so, how? I suppose there are two ways of looking at that. Should they be held to account for all fraud that is facilitated on their sites or services, or should they be held to account for fraud they might reasonably have prevented?

Professor Victoria Nash: Obviously, there is an awful lot in that question. I would probably begin by suggesting that we should distinguish in the first instance between fraudulent activity that is facilitated and fraudulent activity that is advertised. Thinking about the different responsibilities that might apply to platforms is a good starting point, because we might distinguish between user-generated content and content that is part of, if you like, the core business purpose actually purchased or engaged in—commercial relationships by the platforms themselves. That was a key principle of the Online Safety Bill at the beginning.

In relation to content that is merely facilitated, I think the burden of responsibility for the platforms should be less, and your focus on what might reasonably be prevented is appropriate there. One key point about scams in particular, and online fraud, is that they are so problematic because they are very difficult for us as individuals to identify. The assumption that platforms will automatically be better able to identify and prevent them occurring is probably mistaken.

What we might expect in that context is the following. First, when fraudulent activity is reported, platforms might have a responsibility to act to remove content or consider censoring those users. Secondly, there might be scope for more information sharing between platforms, perhaps to identify patterns of activity or common language, et cetera, which might possibly inform prevention.

On the advertisement side, there is probably more scope for holding platforms responsible, simply in so far as you might expect them to undertake appropriate checks of corporations and individuals advertising on those services. For me, that is the key distinction between advertisement and facilitation.

Lord Gilbert of Panteg: Thank you. Professor Woods, do you have anything to add?

Professor Lorna Woods: Yes, I agree with Professor Nash's distinction between the facilitation and the advertising. I also agree that there are different responses that you might usefully expect platforms to take. Particularly with advertising, there is more that can be looked at in the systems, and, in targeted advertising, what controls exist around the sorts of targeting that can go on. Could a bad actor use targeting to identify particularly vulnerable people, or particularly vulnerable people in relation to certain sorts of scams or adverts? I think there is more there.

I would like to take this opportunity to make the distinction between liability for an individual case of fraud and the underlying systems around that. It is of course the underlying systems that the Online Safety Bill gets to. As to the actual fraud itself, on the whole, I believe there is intermediary immunity, but that is, of course, conditional. Once the platform is aware that there is a fraudulent post up—in the context of user-generated content, obviously—and it is notified, if it does not take steps, in principle it loses immunity if the other elements of the offence

are made out, of course. Historically, there has been no enforcement, and I suppose that raises a question as to why that is, whether it is resources in policing or whether it is more difficult. That may be a question to explore.

Lord Gilbert of Panteg: I want to explore the issue of intermediary immunity. You say that is conditional and you lose it if you do not take action when you were notified. Do you lose intermediary immunity if you did not take reasonable steps?

Professor Lorna Woods: No, the immunity is from the early days of the internet. I think people were just thinking about takedown and when there is an obligation to take content down. It comes from the e-commerce directive. In that directive, the recitals actually said that the question of immunity was different from the question of whether intermediaries could be put under obligations in relation to duties of care. The immunity provision was simply that you are not liable unless you knew about it.

Lord Gilbert of Panteg: Got you. Lulu.

Lulu Freemont: I will introduce techUK for those who may not know it. We are the trade body for the tech sector. We have over 850 members, the majority of which are SMEs. They range across all sorts of different areas, including cyber, defence, telecommunications and some of the online platforms.

A really important distinction is the fact that not every online platform is the same. What they witness is often very different, based on how users interact with different platforms. So, when we talk about online platforms, we need to think about which types of platforms we are speaking about and how their differences will impact their responses.

Professor Nash made a point about information sharing, which is really important across the tech sector. It extends to thinking about other private sectors that might also experience and witness fraud. We hear a lot about incentives to act and where the responsibility should lie. From our perspective, we also need to think about the incentives to collaborate. This is not a siloed problem. Fraud is not seen only on online platforms. It is a transfer where a fraudster takes a victim across different sectors. If we can think about how we can work together and streamline information sharing across the different sectors, we might get into a position where we are matching the sophistication of fraudsters. That is just a point of nuance on responsibility and collaboration to add to the other two witnesses.

Lord Gilbert of Panteg: On information sharing, and this may be more for Professor Nash, are there any legal or other barriers to information sharing that we might want to look at?

Professor Victoria Nash: The argument that is most frequently made is around privacy and, clearly, platforms have a responsibility to protect the

private data of their users. Beyond that, there are none that I am aware of. Lorna, do you want to add anything?

Professor Lorna Woods: You would need to look specifically at the Data Protection Act and the Police and Criminal Evidence Act. That is going closer to the process of prosecuting, but you would not want inadvertently to undermine civil liberties. You would need to think about how Police and Criminal Evidence Act protections intersected with what the obligations were. I think that is less data sharing between the industry members and perhaps data sharing with the police, in particular. The only other possible thing, not barrier but concern, would be how it intersected with competition law, and to make sure that data sharing did not tip over into anti-competitive behaviour.

Lord Gilbert of Panteg: Got you. Very useful answers, thank you.

Q53 **Viscount Colville of Culross:** Good morning. You have just been talking about facilitated fraud and we all know that the Online Safety Bill is to be published this afternoon. There have been changes this year to the Bill. The Government have added an extra priority illegal offence written on the face of the Bill, and fraud is one of the offences. They have now said that firms have to be proactive and prevent people being exposed in the first place. Lorna, do you think that goes far enough when we are looking at facilitated fraud, or should more be done to try to make the platforms accountable to deal with the problem?

Professor Lorna Woods: It depends on what the proactive measures turn out to be, and the answer to that question will depend on what Ofcom requires. We cannot expect perfection. There is a difference between what we can expect in the context of advertising, as I said, and the organic content, which is more problematic. With advertising, there is probably quite a lot more that could be done on identity checking. In that regard, I would say that the concerns around identity and anonymity and pseudonymity that you get, say, in normal organic contexts are much less in the context of advertising, which is commercial.

It would also depend on the platform, picking up Lulu's point. They are different. You probably have different expectations of, say, a dating platform than you might have of a more general platform such as Twitter or Facebook. The purpose of something like a dating platform, and the fact that it is about getting to know people potentially for romantic purposes, may justify closer oversight, perhaps around identity sign-up, looking for patterns of behaviour, and things like that.

It is interesting that in the online advertising programme consultation the Government listed some general points that might be considered with regard to advertising. That would be programmatic advertising generally. My one-line answer to your earlier question is the irritating lawyer's one of, "It depends", and it will depend on the detail, potentially.

Viscount Colville of Culross: You just said that when it came to the facilitating of fraud you would like to know more detail about the

proactive measures that Ofcom will require. What sort of measures do you hope it would require?

Professor Lorna Woods: I think some have been mentioned. There are identity "know your client" sorts of checks on advertising. Where you have specific constraints on products or services, and where you have registered providers, it is about whether they are registered. That is obviously of relevance to the FCA, but may be more generally relevant if you are seeing fraud more broadly, and thinking about products and medicines and things like that.

I mentioned oversight as to how targeting criteria are developed, and whether there is any oversight. I read a few years ago that Facebook—I think it was Facebook—allowed people to be targeted on the basis of their susceptibility or interest in conspiracy theories, for example. How did they come up with that? Do we think it is a good thing that people can be targeted on that basis? It is questions around that and, I suppose, click-through links, and whether those can be tracked or monitored.

There are obvious things such as having decent terms of service in relation to advertising content that have some mapping on to domestic rules about good advertising practice, recognising prohibited products; juxtaposition; whether certain groups should not be targeted; transparency, so ad libraries; and some information about where the adverts are going. Moving beyond the consumer and the advertisers, you could look at whether advertising is being used to support organic content that is in the problematic category, whether it is supporting extremist content, terrorism and the like. It is those sorts of things.

Viscount Colville of Culross: Thank you. Victoria, there has been quite a lot of talk about advertising, which Lorna talked about. Do you think the Bill should include all paid-for advertising and that it should be brought into scope?

Professor Victoria Nash: I have been quite torn on this particular question. The Bill has obviously expanded quite a bit over the past year. For me, there is a risk that the broader its coverage, the less able it is to address effectively all the different harms that are in scope. On the particular topic of online fraud, I can see why there was significant pressure to bring scam advertisements in particular within the scope of the Bill in so far as it applies to platforms and search engines, but it leaves out the rest of the web and the other places where people might encounter advertisements and other forms of fraudulent activity.

Given that there is to be a consultation on advertising and online advertising over the next few months, I would be more in favour of there being more targeted instruments in the future that might enable us to address in addition some of the other issues that Lorna identified—particularly, for example, appropriate uses of data for the purposes of digital advertising, the development of profiles, and segmentations of the population, particularly vulnerable populations. That would also enable you to target sources that go beyond user-to-user platforms or search

engines, which are obviously the main focus of the Bill. I understand why you would want to include online advertisements, but I think it might have been better to deal with all online fraud and advertisements separately, to be honest.

Lord Browne of Ladyton: I am sorry to bring you back to the first question, Lulu, but I want to ask you a supplementary question that the others might also want to contribute to. I think it is a fairly fundamental question.

We very quickly got into the weeds and the elements of all this. I know it is very complicated and I accept that. The fundamental question you identified, Lulu, although we did not answer it, is that fraudsters do not need any incentive to collaborate. They are incentivised by the outcome to work together across all the different areas in which they work. Their business model relies on that. They do not need external stimulus.

It seems to me that the identification that prevention and prosecution of them relies on is, fundamentally, collaboration across the same people. For your business—the digital environment, techUK—what would incentivise you to collaborate with other areas, and to what extent do you accept the responsibility to be the initiator of that collaboration rather than waiting for an external actor, that is public policymakers, to create the environment or give you incentive to do it? Should you not have a business model collectively that is focused on preventing fraud and be generating these ideas? What would incentivise you to do it?

Lulu Freemont: To be super clear, I work at the trade body. I do not work at an individual company, so I cannot speak to individual company responses. At the trade body we have set up a collaboration with UK Finance and the National Economic Crime Centre, which is very much looking at how we can collaborate across tech, finance and law enforcement, to think about collaborative and effective responses targeted against fraudsters. We are starting that collaboration from our perspective. Much of the conversation that comes towards techUK and tech companies is around responsibility and, while that is important, we also think we need to zoom out and look at how fraudsters are manipulating sectors at each step of the way, and think about how we can work together, so that we can be more effective with our interventions.

That is our approach towards it. It is not to say that there is no responsibility, because every single sector that experiences fraud is responsible for intervening and for combatting it. We always accept that more needs to be done, but we believe we need to work together across telecoms, tech, banking and law enforcement to be effective in our response, and to streamline our responses so that they can be digitised and brought into real time action. That is our perspective. I do not work in individual companies, so I cannot speak to business models, et cetera.

Lord Browne of Ladyton: Do our other witnesses have any ideas on how we deal with an organic and systemised problem in a systemised

way?

Q54 **Baroness Taylor of Bolton:** Can we go back to the Online Safety Bill? A lot of us are very pleased when we have draft legislation because the idea behind it is that you can get some consensus as to the way forward, iron out some of the potential unintended consequences and make sure that we get legislation that will actually work. When you are introducing new regulations, you often get a lot of pushback. It sounds as if there has been some pushback from techUK and that there is concern about the level of regulation. Issues about Ofcom being overburdened have been mentioned. Is it possible to get a genuine partnership between government and the industry that will at the end of the day provide the kind of safety we are all aiming at?

Lulu Freemont: Thank you very much for the question. To start off, we really welcome this legislation. I do not know any of my members who do not support the legislation and support the objectives the legislation is trying to achieve. Fundamentally, they are the right objectives.

The Bill is trying to strike a balance between protecting children and adults online while supporting free expression and privacy. It follows an approach that is principles-led, and can be flexible and adaptable to potential new harms, while supporting innovation. It relies on those systems and processes. There is much to support in the approach of the legislation and in the objectives, and that is our starting point.

Our focus is on the workability of the Bill. The Bill will impact, on a conservative estimate, 24,000 tech companies. That is far greater than the tech companies that people think about when they think about the Online Safety Bill. Our job at techUK is to think about those tech companies and the broad sector, and how this regulation will be workable for them.

We think the ultimate test of the legislation will be whether it provides enough clarity and coherence for both the in-scope companies and the regulator to make quick and effective decisions. Ultimately, if companies know what they need to do under the Bill, they will be able to act faster and will be able to deliver on the objectives sooner. We are really looking at the workability question.

Where some of the challenge comes, and where we have seen some concern from our members, is around the need for greater clarity, and whether the legislation will remain effective, flexible and targeted enough to be able to deliver. Obviously, with a draft Bill there are lots of gaps. Later today, some of those will be filled. We do not expect that the draft Bill will give us all the answers, but there are risks of unintended consequences if the Bill as we see it later today does not provide clarity and does not continue to focus on a principles-based approach.

There are unintended impacts for content moderation. A company needs to identify the context in which content exists. That is quite difficult if you do not have definitions. It is likely that there could be inconsistent

application across the sector in relation to different areas if we do not get some guidance and clarity on definitions of the categories of harm, which we understand will still be left to secondary legislation, and we would not support that.

Secondly, there are unintended consequences for competition. Many of those 24,000 companies are small businesses, and there is a risk that they could be edged out of the market if the requirements are too burdensome. Thinking about capacity, smaller businesses will not have compliance teams. They will not have the resources in place. They will be diverting existing staff away from what they are doing, in order to comply with the regime. That is not to say that they do not need to comply—they do—but we would like the regime to be flexible enough to support smaller business, and not to introduce requirements that have only been consulted on with larger companies.

Thirdly, and the last point, there are some unintended consequences for society. This again comes to the smaller businesses point. Senior management liability and sanctions set have a chilling impact on the sector. We do not want to get into a position where companies feel that they need to remove too much content, which might violate free speech or undermine one of the objectives, as the easy route to compliance or as the only route where they feel confident that they can comply.

We are very supportive of the Bill but we now need to focus on how it will work. We hope that the conversation as it moves through Parliament starts to really consider the workability question and resists a wide expansion of scope that could significantly impact that. We are not saying that the issues that people want to put in the Bill are not important. They are often very emotional when people want to extend the scope. That is totally fair enough. From our perspective, we are thinking about the right legislative vehicle for the issues and thinking about how we can make the Online Safety Bill work.

Baroness Taylor of Bolton: Some of us would agree with what you said about too much being detailed in secondary legislation. That is across the board on legislation, not just on this.

You are saying that you are worried not about the cost of compliance but about the clarity. Is that fair? You mentioned compliance for some of the smaller companies, and I accept that some of them will be very small start-up companies with just a few people who are very keen to pursue a particular form of your industry, but should all companies not have a responsibility to up their game on compliance, when some of the consequences of letting things through the net can be so devastating?

Lulu Freemont: Absolutely. On the first question around clarity, it is clarity and proportionality. The regime intends to be flexible, and it intends to rely on systems and processes, but we need to see that come into action. For example, if you are a parent networking site that might be in scope of this legislation, and you already have systems and processes in place, and you already have terms of service that control

what it is and is not okay to say on that network, we would like the Online Safety Bill to support those existing systems and processes, and not require smaller businesses such as the one I referenced to have to rewrite everything they are doing in order to comply. Proportionality and flexibility and supporting the existing systems and processes that companies have in place are really important as we move through this process. Clarity and proportionality are important.

The costs of the legislation are one of the unintended consequences if we do not have clarity. Companies may resort to acting in a certain way that might have costs to society, but it might also affect them because they might not get new business in, or they might not be able to innovate in the same way. Clarity is at the heart of this and the unintended consequences include impacts on cost.

Baroness Taylor of Bolton: But a lot of this is about innovation. As soon as you start doing something new, you open the door to different methods of fraud. Is there not an obligation, even before you embark on a new form of activity, to consider what the impact will be and how you will comply with the legislation in its broadest form?

Lulu Freemont: I am trying to think about how smaller business would possibly foresee that and what sorts of processes it would need to undertake. I know that the Bill is very much focused on risk, and we support a risk-based approach. We need to have that in place. What is important when we talk about fraud, and where it is really complicated for our members, is that the actual definition of fraud is not very commonly understood. There is a complete lack of understanding across multiple different sectors about what they are talking about when they say fraud, online fraud, or scams. Scams are a bit easier because we can see what the process is, but fraud is a huge term that encompasses many segments, so clarity in definitions is really important to companies in order for them to understand what they need to do.

Viscount Colville of Culross: I want to ask Lulu a little more about her view on advertising and whether she felt that, if there was wider scope for advertising to be included in the Bill, it would be unnecessarily burdensome on the tech sector.

Lulu Freemont: To pick up Lorna's answer, it depends on the detail. We have concerns that widening the scope could bring in a significantly larger number of companies. There is a question about whether this is the right legislative vehicle to deal with that, which is not to say that nothing needs to be done. We have the online advertising programme and ongoing collaborations; the Online Fraud Steering Group, for example, is looking at online advertising. We have had changes in the FCA lists, as I think you have all heard me say previously, whereby companies now require financial services advertisers to be authorised by the FCA prior to serving adverts. Activity is going on in that space.

We have serious concerns that putting advertising in the Online Safety Bill could derail the legislation. We need to think about the outcome we

are trying to achieve with that, and if we will achieve that outcome by putting it in the Bill and following the Bill's process. We do not have the detail about how it will be done, if it will apply to a small subset of companies, or if it is just about the removal of scam ads, but it will be really significant for us to be able to assess the implications.

Viscount Colville of Culross: That is very helpful.

Professor Lorna Woods: I find some of these concerns about clarity a little overstated. I think they focus very much on definitions of content that has to be taken down. When I looked at the draft Bill, what I saw was a requirement to do a risk assessment, following guidance on that risk assessment by Ofcom. I do not think that in itself is that unclear. We expect companies to do risk assessments in other contexts, so I do not see why this context is different. Obviously, the idea of criminal content has specific obligations in the draft Bill, particularly for priority illegal content, where there is a list of obligations, but in the running of the system, the idea of doing a risk assessment is not that difficult to understand. I agree with the tenor of Baroness Taylor's remarks. It is about asking, "If you are doing something new, what happens when it scales? What happens when the bad people get hold of it?"

I do not think the expectation is a perfectly sanitised environment. The objective has been to try to stop exacerbating the problem, rather than anything else. For that reason I am not convinced that the argument that putting more than one type of advertising in the Bill will make it more complicated, because what is being looked at is the system for delivering advertising. You have a KYC system in place across the board. It is one system and one set of things to think about.

The point is that that is different from saying that Ofcom is a content regulator on adverts. If you are saying that Ofcom is a content regulator on adverts, then, yes, the width becomes a problem, but if we are looking at systems I am less convinced.

The Chair: That is very helpful. We know the debates about the Bill are only just starting and will take a lot of time in Parliament.

Q55 **Lord Vaux of Harrowden:** First, I want to ask a supplementary to Lord Browne's question. We have seen in evidence so far in this inquiry that the sectors that have a real financial incentive to do something, and are on the hook financially, are taking real action. The sectors that do not, frankly, are not. There are always reasons not to take action.

Lulu, how do we incentivise the tech sector to take action? It has not happened very much to date, and now that we have the Online Safety Bill I think people's minds are being concentrated. Where is the incentive for the tech sector to deal with a problem that is becoming so huge?

Lulu Freemont: I would humbly say that the sector is doing stuff in this space. It may not be vocalised enough or seen enough. I know you will be hearing from lots of different companies during this process, so I hope you will get a sense of what is happening at different parts of the value

chain. Whether it is cyber companies, defence companies, telecommunications services or platforms, there is a lot going on at each step of the fraud journey.

On the question of incentives, one of our real concerns is that if we engage with this debate on blaming sectors for various things and thinking about incentives, we might lose the opportunity to work collaboratively. From techUK's standpoint, we believe that we need to work with the banks, the platforms and law enforcement—[*Inaudible.*]—to understand the journey—[*Inaudible.*]—information across sectors. That is a way in which we think we could effectively solve this problem, and we think that if we could—[*Inaudible.*].

The Chair: Lulu is having trouble with her internet, by the sound of it. Lord Vaux, when Lulu rejoins us, we will get her to finish that answer.

Q56 **Lord Vaux of Harrowden:** Let us have the broader question, in that case. Professor Woods might be a good person to answer it. It is fine to have regulation, but effective implementation of that regulation is critical. What do you see as the main challenges for effective implementation of the UK's regulation regime? How successfully do you think the members of the Digital Regulation Cooperation Forum work together, and does that forum have the right membership? Finally, do you think that regulators have sufficient resources to do all this stuff?

Professor Lorna Woods: Getting regulators of varying sorts to work together will be one of the challenges in this field. I would not like to overemphasise that, though, because, in a way, we have that challenge offline as well as online. It is just that the digital environment has added an extra layer of complexity. You might find that some of the regulators have a longer track history of at least talking to each other, even if we do not have them doing joint enforcement actions or the like. That is a general context question.

We need to distinguish different types of co-operation. One of my concerns about the draft Online Safety Bill was that it did not deal expressly with an obligation to co-operate. I think the thought was that some of the general powers of Ofcom could cover that, but I thought those general powers related to delegation—for example, when Ofcom had the obligation and then delegated it to the ASA in the context of broadcast advertising. That is different from co-operation between regulators, each of which operates in their own field of competence. There will be questions, I think, about the level of integration of operations. When we are talking about co-operation, are we talking about just a general talking shop, future scanning, and trying to understand the issues at a general level, or are we looking at a much more granular level of co-operation, even file sharing, which goes back to some of the earlier questions?

We need to give some thought to that, and to mechanisms where regulators in one field can flag an issue, probably for Ofcom, as regards systems and processes. For example, if the FCA becomes aware of a new

genre of scams, or a new way of portraying that, how does it get the message across to Ofcom? Is Ofcom obliged to co-operate? Are we envisaging that, say, the FCA is, in effect, nothing more than a body that could use the super-complaints mechanism in the draft Bill?

I think that would be insufficient, but we need to think about how that mechanism works, because you do not want Ofcom becoming the de facto enforcement arm of a range of other regulators, and then losing control over its work flow. More thought needs to go into that. My suspicion is that although the Digital Regulation Cooperation Forum is a good start, and the work plan is a good place to start, we need to go to a slightly more granular level going forward. As regards resources, I do not know how much is enough, but we certainly need to look at that and to make sure that it stays enough.

Lulu Freemont: I am so sorry. That is the first time that Zoom has kicked me out. I very much apologise for that.

I do not know where I had got to with my sentence before I was booted out, but I believe I was talking about the incentives for collaboration and how we need to think about this across the sectors. You will hear a lot from tech companies, and whoever you have here, about how they are acting to combat the issue, and it is not true that nothing is being done.

From our perspective, we need to shift the narrative to think about what is the issue we are trying to solve, which sectors it involves and how we can work collaboratively. TechUK is trying to work with our members on building trust, transparency and good working relationships with the banks and with law enforcement, because that will be really fundamental for us to solve this. I am not commenting exactly on how to incentivise our members, because I think they are already doing a lot of work in this area. Our focus is on collaboration, because we think that is the most effective route to success in solving the problem.

Lord Vaux of Harrowden: Thank you. Professor Nash, do you have anything to add on either of those two questions?

Professor Victoria Nash: I am quite happy to move on to the next question if we are out of time.

Q57 **Baroness Bowles of Berkhamsted:** Might the proposals for greater identity verification online raise any ethical, logistical or operational challenges for users of the internet? Are there any concerns about privacy with respect to the proposals, and how might that impact fraud?

Professor Victoria Nash: As we have said several times, it will all depend on contexts and the proportionality of what is appropriate within those contexts. Identity verification, for example, when undertaking financial transactions or purchasing things online, and at least having the two-factor authentication that is now being rolled out more widely, seems like a good step, and I do not think it is disproportionate or particularly damaging to privacy.

Measures such as those that I think will be introduced in the Online Safety Bill around the possibility of allowing individuals to choose to interact only with verified users, again, will be a valuable step in addressing potential fraud. I am very keen that that remains optional. The possibility of having anonymous speech and anonymous engagement online is key, and I would not want that to disappear. Last but not least, it is worth making a differentiation between things like identity verification and age verification, and ensuring that we only ever require the minimum amount of information needed to carry out whatever the activity is in a risk-reducing way.

For me, the key distinction relates to proportionality and ensuring that it matches the risk that has been identified, never seeking more than that, and, ideally, ensuring that these things are, wherever possible, optional.

Baroness Bowles of Berkhamsted: Given that fraudsters are pretty good at using technology to get around identity safeguards, I think the identity issue is fundamental, but, in fact, identity theft itself is not an offence. Would it help if identity theft were a criminal offence, so that there was more focus on stopping it in the first place, or at least having in place the necessary checks?

Looking more broadly at fraud in general, what about failure to prevent offences? Ultimately, something has to be actionable, and you have to be able to give the firms the incentives, as has been done with bribery, to look through their chains to make sure that they have done everything they could. With failure to prevent offences, you have your defence there. It is a bit like immunity, but does it have more teeth?

Professor Victoria Nash: I will let Lorna reply from a legal perspective in a moment. In all these cases, if in-depth analysis of the problems that we are facing identifies that law enforcement lacks the capability to act because certain things are not currently defined appropriately within the law, movement in that space is definitely worth while. Again, this seems to me to be moving beyond the Online Safety Bill and suggesting that there is a wider area of work that I think we would all say was very welcome, and there might be scope for more legislative instruments later on. Lorna, would you add anything to that?

Professor Lorna Woods: Just to agree. I do not really know anything about the detail of fraud offences, but it would probably be worth revisiting that in the light of the online context. Failure to prevent offences usually has the defence of having decent systems in place.

I have a slight unease in this field because of the freedom of expression context, in particular if we are looking at organic content and fraud there, and whether this is pushing platforms to a much greater level of user surveillance. That sits uncomfortably from a freedom of expression perspective. The liability in the Bill, as I understand it, is for information offences, so in a way non-compliance with the investigation rather than the primary content existence. If you were to look at that, you would

need to focus it very tightly, because there is a risk of unintended consequences.

Baroness Bowles of Berkhamsted: I think the point on failure to prevent fraud would be a much more general thing, as it is perhaps for bribery. Would you support identity theft being a criminal offence?

Professor Lorna Woods: In principle, it should of course be looked at, to see whether there are any gaps. You do not want to add to the criminal statute book if there is no need. As Victoria says, if the consensus is that there is a gap, then yes.

Q58 **Lord Sandhurst:** I want to ask about UK efforts to legislate for online safety, in particular with regard to fraudulent activity, comparing them with what is in the EU and the USA. To give a bit of context, as I understand it, the EU Digital Services Act sets out to protect consumers from illegal content and products online, and impose obligations on platforms. The Digital Markets Act will regulate the platforms and try to ensure competition, particularly where a parent company owns both WhatsApp and Instagram, to ensure that they do not share information between them.

On the other hand, the USA is apparently much more laissez-faire, not least because of the first amendment. There, they are considering bringing matters up to date, as I understand it, by removing immunity from suit at least in respect of speech that the platform is paid to carry, but not information. There are different approaches. How do we fit into all that and should we be picking things up from one or the other? What can we learn, or do we have a perfect middle way? It is a big question, but there is a lot out there.

The Chair: Shall we start with Professor Woods, although it is relevant to everybody?

Professor Lorna Woods: I am not up to date on the detail in the United States. I am aware that a lot of Bills have been introduced in Congress. There is quite a bit of attention in the States on looking at the problems from a lens of consumer protection and competition law. In a way, I think they are not tackling it quite so head-on. There is also more movement on data protection, certainly in the individual states. Some US states have taken the GDPR as a model and I think California is taking the age-appropriate design code as a model. That is perhaps an example of a world-leading initiative, quite genuinely. I suppose it just tells us that there are lots of ways into the issue.

The Digital Services Act covers criminal content, whether criminal within the national systems, or at EU level. For very large online platforms, it has a risk assessment and mitigation element as well. I think there are similarities between what is proposed there and here as regards that model. Yes, the Digital Markets Act looks at gatekeepers and their impact. That is the competition perspective again. I suppose it is similar to what we are seeing with the Digital Markets Unit and the Competition and Markets Authority, although the terminology for the two is different,

and I am not precisely informed enough to be able to give you an idea of whether there is any gap in reality between the two on that.

Professor Victoria Nash: I am not a lawyer and not an expert on the different regulatory regimes, but one thing we have observed, which is interesting, is where we have examples of similar legislation in other countries; for example, the NetzDG hate speech law in Germany, or the age verification laws around pornography in France. Some of the lessons we can learn are very much about enforcement and the effect on the problems that they are trying to address. For example, in a pornography case in France, they very much focus on tackling the biggest players, the largest companies, which obviously has been effective, but what it has not done is make it impossible for underage users to access pornography online, because they have been diverted to smaller sites.

We have similar frameworks to those being explored elsewhere in Europe. In a couple of cases they may be ahead of us, and in other areas, in things like the laws we have just discussed, they may be a bit more ambitious. Probably the best thing we can do is to watch and learn from the enforcement of existing law, and see if we can use that as we roll out with Ofcom our approach to regulating this activity in light of the Bill becoming an Act. I think we are innovative and ahead of the game, but there are others we can look at to learn lessons that will improve our application of this new legislation.

The Chair: Lulu, how about from your members' perspective?

Lulu Freemont: It is a really interesting point. Equally, I am not a lawyer so I cannot offer the legal detail. Where we come from with this is thinking about the tech companies that are in scope of the UK's regime but will also be in scope of the DSA, the DMA and regimes in the United States. We are thinking about areas for convergence, for having streamlined processes that do not result in them having to duplicate efforts for each different region to achieve the same kind of outcome. Thinking about the convergence and divergence of regimes is a big priority for techUK; and providing clarity for our members on what are the clearest and most simplified processes that will achieve the outcomes, and what areas we should have in the UK regime that are working really well in the EU, for example.

The EU's focus on illegal content and the definitions, and having a very clear understanding of what kind of content is in scope of the EU regime, is welcomed by our members because it has the clarity that I spoke to earlier. We are thinking about the tech businesses that are in scope of multiple different regimes and the importance of convergence and simplicity across different regions.

The Chair: Thank you very much indeed.

Q59 **Lord Allan of Hallam:** We want to look forward as well as backwards. There is a lot of buzz at the moment around the metaverse and metaverses, and I am curious to explore that. I guess the shorthand

description is that we will move from living our lives on the internet to living them on the internet. We are keen to understand whether that will make any significant changes in the fraud area. Is meta fraud different from good old-fashioned online fraud?

This is not entirely novel. I can remember being with Professor Nash at an event talking about Second Life, the original attempt to build a metaverse way back in the day. Perhaps I could start with you, Professor Nash. What do you think about whether fraud will look the same or different as we move into this metaverse world?

Professor Victoria Nash: I hope we will have a chance to recreate that conversation in this new context. I do not know about you, but I feel like I have been around the block a lot of times on this sort of question. I think it is very clear that we have yet to see a form of criminal activity that does not relish adapting to new technological contexts. It is also very often the case that new technological advances are driven, to some degree, by the less palatable aspects of human nature.

I am less convinced that we will see completely new forms of fraud or scam in the metaverse, but if I think about it as a social scientist, it is clear to me there may be some aspects of that type of activity that may make it easier in some ways for individuals to be duped. There are possibilities for impersonation, for example, or personalisation, or perhaps a greater array of social cues that we might have in a virtual context, and if we think about traditional forms of scamming, which are about building up trust and responding to individual desires, if you like, to be duped, a lot of those will be much more feasible within something like the metaverse.

Yes, I think online fraud will continue to be a significant problem. I doubt we will see dramatic new forms of crime, but we will need to ensure that any legislation we have now is future-proofed.

One thing I would flag is that I would be wary of us focusing only on the most glamorous forms of technological innovation. The metaverse is very exciting, but we need to check that other technological innovations are covered by this—for example, the role of smart speakers, non-screen based technologies. What does it mean, for example, if I ask my smart speaker at home to give me information about a financial product? Are we sure that the sorts of cues and information we rely on platforms to provide will work in that context? Equally, with IoT—internet of things—devices, such as navigation systems, is there any way your navigation system can be hacked to push you towards particular garages? There could be new forms of mobile phone scams. I think, yes, we should focus on emerging technologies, but we should not get too carried away with the most glamorous ones. That would be my view.

Lord Allan of Hallam: That is super helpful. As somebody who gets regular scam SMS messages, I think advice to look at the old technology is very important. Professor Woods, I am curious from a legal point of view whether you think that the Online Safety Bill, because it will be the

framework for the next few years, will cover sufficiently anything that might occur in the metaverse world.

Professor Lorna Woods: Obviously, it is a bit difficult to tell, because we do not know what the metaverse will look like. From my best guess as to the elements of a metaverse, I would have thought it should fall within the definition of user-to-user service currently found in the version I saw of the draft Online Safety Bill. In principle, yes. A mechanism based on risk assessment and then trying to mitigate at a very general level translates. The risk assessments themselves will have to take into account the specificities of the metaverse, and I suppose a move away from the text-based to the visual and personal, and in some way take that into account.

There are two particular questions. I do not know how the takedown of content—everybody's favourite remedy—works in a metaverse because it is much more a livestreaming context. If we look to livestreaming platforms now, say, to online games, they do not tend to record what players are doing. You get players recording themselves, but the platforms themselves do not, so I suppose there is a question there about evidence. Solutions might have to look at being different. Going back to Baroness Bowles's point about identity theft and what Professor Nash just said, perhaps it is in that sort of new context, if we are looking at identity theft and a criminal offence, that we need to make sure it is future proof.

Lord Allan of Hallam: Thank you, that is very helpful. Is there anything to add, Lulu, from a broader tech sector point of view?

Lulu Freemont: I do not have loads to add specifically, except that, as has been indicated, the fraudsters will inevitably adapt and prey on the vulnerabilities in new technologies. As Professor Nash said, we have seen that happen for a long time, and we do not expect it to change. It comes back to how we are approaching the issue and looking at patterns and responding to them in a coherent way.

The Chair: I am not quite sure whether in the metaverse we will have House of Lords inquiries and Select Committees. Who knows in future?

We have talked a lot about platforms this morning, but of course in the perpetuation of fraud a lot happens in the online messaging services that often run alongside the platforms. They could be alongside dating apps. I am thinking of Messenger or WhatsApp. Do any of our witnesses want to say anything specifically about messaging services as channels of fraud, or as regards the Online Safety Bill? We do not know yet whether the latest Bill will cover messaging services. Did the last draft sufficiently cover them? Does anybody want to cover messaging services?

Professor Victoria Nash: There are a couple of points. First, I reiterate the point that Professor Woods made earlier about ensuring that we do not move to an ever-more surveyed society, where every communication that we send to another person is subject to surveillance. We need to be wary of that. There may be scope in the context of messaging apps—I do

not know whether they will fall within the scope of the Bill—to ensure, for example, safeguards in the form of reporting. There are other measures that may be just as relevant to messaging apps, even when surveillance or prevention may be very difficult.

The Chair: To expand on that, when you say reporting, do you mean by the providers of those?

Professor Victoria Nash: Yes. If we are thinking about social media or platforms where you engage in user-generated content, there is often the possibility to report fraudulent or other abusive content. If we are very serious about dealing with the capacity for online fraud via messaging services, ensuring that users know what to do when they encounter problematic content in those means is an important safeguard that might be looked at.

The Chair: Thank you. That is very helpful.

Professor Lorna Woods: We need to look at the function of the service. There is a difference between a messaging service where you have, essentially, one-to-one communications, which is very much in the heartland of privacy of correspondence, and an app such as Telegram that allows you to broadcast to 10,000 members of a group. Looking at the features of a service rather than how it is described is important.

Q60 **The Chair:** Thank you, that is very helpful. We ask all our witnesses this final question. Specifically thinking about fraud being conducted, is there one policy recommendation that you would like us to reflect on and to make to government when we are preparing our report? I do not know who has a fully formed policy recommendation. If you do not, that is absolutely fine. Professor Nash, perhaps I could come to you. Is there anything you want to add?

Professor Victoria Nash: I do not have a fully formed new policy recommendation. I guess it would just be a request that we ensure that the resources are there for enforcement, including training for the agencies that will enforce both prevention and detection of fraud, and for education. A few times we have commented on the fact that this is a really complex area. Obviously, there is a role for platforms themselves to engage in media literacy and education, which I hope will be included in the Bill, but education more broadly, even beyond the platforms, is needed.

The Chair: Professor Woods, a recommendation.

Professor Lorna Woods: It is looking at how the regulators work together to make sure that they have the appropriate competences and powers, as well as resources.

The Chair: That is very helpful.

Lulu Freemont: Ours would be very much around encouraging the Government to look at how we need a whole-system change response to

tackle this issue effectively. Continuing to work in silos and continuing to think about individual pieces of legislation, without co-ordination and without collaboration, which could be legislative or non-legislative, would be a real mistake from our perspective. It is thinking about the bigger picture and the whole-system change response, which obviously encompasses the commercial ecosystem, law enforcement, criminal justice, tech companies, banks and telecoms, and the infrastructure to support users and consumers who might become victims.

The Chair: Thank you. That is very clear. Thank you, all three of our witnesses this morning. Lulu, we are delighted that you were able to get back on so that we had the benefit of your evidence. Preparing for a Select Committee is quite a task, so we are really grateful to you for your time this morning. I thank my colleagues for the questions. Thank you all for your time.