HOUSE OF COMMONS

# Science, Innovation and Technology Committee

## Oral evidence: Information and data security across government and the work of the Information Commissioner, HC 1395

Tuesday 21 October 2025

Ordered by the House of Commons to be published on 21 October 2025.

Watch the meeting

Members present: Dame Chi Onwurah (Chair); Emily Darlington; Kit Malthouse; Dr Lauren Sullivan; Adam Thompson; Martin Wrigley.

Questions 1 - 91

### Witness

I: John Edwards, Information Commissioner, Information Commissioner's Office.

Written evidence from witness:

# Examination of witness

Witness: John Edwards.

Q1 **Chair:** Welcome to this session of the Science, Innovation and Technology Committee. We are examining lessons from the February 2022 Afghan data breach for information and data security across government, and the Information Commissioner's role in enforcing and advising on these matters. We are very pleased to welcome the Information Commissioner, John Edwards, to this session.

In August we invited the then Chancellor of the Duchy of Lancaster to appear before us to provide the Government's perspective on this incredibly important issue, and extended that invitation to the current office holder when he took on the role in September. However, the Chancellor of the Duchy of Lancaster told us just last week that he would not attend, and would send other Ministers in his place. We have yet to receive a proposed date for this hearing, two months after our initial request.

I speak for the Committee in saying that we are very disappointed about the Government's failure to send a Minister to this session, despite the long lead time, and about the long delay in proposing replacement Ministers. Accountability to Select Committees is a non-negotiable Government responsibility, and we want to assure those watching that we will continue to hold the Government to account on this important matter of protecting our constituents' data, and look forward to engaging with Ministers constructively and robustly on this question in the future. For the moment, I really want to welcome John Edwards. There are a lot of questions to cover, so let's get straight to it.

When I saw some of the details of the Ministry of Defence data breach, I was astounded that that could be part of Government data practice: a 33,000-line Excel file with top secret information bandied about like confetti. This is not an individual failure. Whoever was responsible for it, it was an institutional failing. As the Information Commissioner, you are responsible for regulating and enforcing good data practice. Were you aware that such lax data practice existed in Government Departments, and why did you choose not to formally investigate?

***John Edwards:*** Thank you, Madam Chair, for the invitation to attend. I welcome the scrutiny. I think the parliamentary oversight of my office, as well as governance, is incredibly important, so I am pleased to be able to attend and inform the Committee on these important matters. Your question was in several parts so, to the best of my ability, I will tackle each in turn.

Were we aware that there are poor data practices? Yes. We have seen them. The use of spreadsheets in an ad hoc way is a risk in itself. The transmission of spreadsheets to external parties always contains the risk that there will be concealed data. It is a risk that I was aware of from my previous job in New Zealand. We have seen incidents here and they

continue. When we learned about the Police Service of Northern Ireland breach, which we became aware of prior to learning of the MOD Afghan spreadsheet breach, we issued immediate guidance warning of the risks associated with uploading spreadsheets, particularly to public-facing websites. I termed that a moratorium. That is how seriously we took it—despite the fact that I have no actual power to issue a moratorium, we really wanted to put the public sector on notice that there was no reason for them not to be aware of this risk, and mindful of it. I agree with you, Madam Chair, that there is no reason to marshal data into a spreadsheet when you are looking at 30,000 lines. It is not a technology that is suited for that.

There are a range of concerns, which we can go into in more detail, but I think I should get to the final part of your question: why did the ICO not investigate this matter? There are a range of responses to that. I think we probably could have explained those better when the super-injunction was lifted in July, but the long and the short of it was that my office had been informed, as we would have expected. We were told the details as they emerged. We were given details of how the Ministry of Defence was responding, and we were satisfied with the steps that it was taking. There is always a judgment to be made when we are notified of a breach about when, and to what extent, we should become involved in a formal investigation. Early on when a breach becomes known to an organisation, there is an immediate need, within the organisation, to get to the root cause and rectify the problems and, in this case, to keep safe the people that may have been affected. This was extremely serious. There were people whose lives, as we know, were threatened.

If the ICO were to go in and start investigating, that can get in the way. While I take the enforcement and investigation obligation very seriously, there is a question of timing. We have a particular approach to regulating in the public sector, which is intended to maximise our impact, and therefore maximise the protections for public data for the whole of society. As to the judgment that we have made on that, I will come back to the specifics of the MOD in a moment, but I think it is important to understand the context. I have found that if we work collaboratively with Government to identify errors and raise standards proactively, we can have a much greater impact than with a formal process of investigation, which has to be conducted within quite strict legal parameters and can take years. That means that the findings that we make—the impact that we have—is delayed by years. Whereas if we are working together with an organisation in an open way to try and identify errors and take immediate action to ensure that corrective measures are taken, I think we can often have more impact.

There are times when a formal investigation and the use of our full sanctions is appropriate. We did one of those with the Ministry of Defence just a couple of years ago. We fined the Ministry £350,000 for a breach from the same unit that this breach emerged from. In that process, we learned quite a lot about the environment in which these breaches have

occurred. That was the chaos of the evacuation of Kabul and the need urgently to set up mechanisms to support those who had been working with British troops. The pace at which that took place meant that shortcuts were taken. I think we had learned those lessons by the time we became aware of this breach.

There is policy, and then there are practical reasons why we decided not to formally investigate. That decision was taken by a colleague in about June last year, and at that time we were satisfied that the Ministry had undertaken a thorough investigation, that the matter had been taken sufficiently seriously, that the causes had been identified, that the lessons had been learned, and that steps had been taken to ensure, to the best possible extent, that those things would not occur again. Also, the material that we would have needed to access in order to investigate was classified as top secret—or quite a lot of it was. That requires particular handling steps, which are quite resource-intensive. I don't have many staff with the seniority to investigate such matters who have that level of developed vetting. So a decision I think was made, on both the policy—how we would have the greatest impact, and consideration of what more could have been uncovered through an ICO investigation that had not already been revealed by the internal investigation undertaken by the MOD—and those practical implications. Of course, we are always making trade-offs and resource allocation decisions.

Q2 **Chair:** Thank you. That is a long and detailed response to the question. We have to rely on your response now because there is no contemporaneous internal record of this data breach, although the super-injunction did not prevent you from taking any steps in private that the ICO considered appropriate. You have spoken about the lack of resource that was qualified to deal with data. We should just be clear: as part of your job as the ICO—and with all the challenges that the Ministry of Defence has to deal with—you have the right to investigate how it handles data that is top secret. Why is there no contemporaneous record of the decision process that you went through and that you just outlined to us?

***John Edwards:*** The Ministry briefings were in person, so my staff had to travel from Wilmslow to London. I had a deputy commissioner, who was also being briefed. During those sessions, because of the classification, no notes could be taken, so when my colleague made the decision to take no further action he informed me of that, but did not document it immediately. It was only after the super-injunction was lifted that we recorded a formal decision and put it into the system.

Q3 **Chair:** Are you saying that you were prevented from recording your decision-making process because of the super-injunction? The super-injunction did say that it would not prevent any steps in private that the ICO considered appropriate.

***John Edwards:*** That is right. No, we were not prevented by the super-injunction. It is just that information systems make it quite difficult to

store classified material, and to make a meaningful decision note, I think, at that time—the decision was that we would not record that.

Q4 **Chair:** Is that still the case?

***John Edwards:*** Well, there is a relationship with the super-injunction, I think, in that certain material—

Q5 **Chair:** No, I mean, is it still the case that you cannot contemporaneously record investigations, or decision-making processes, where it refers to classified data?

***John Edwards:*** Look, I am afraid I don't have that level of operational knowledge. Can I undertake to come back to the Committee about it?

Q6 **Chair:** Yes, please do come back to us. I think the Committee is concerned at the description you have given of how that decision-making process takes place. I am concerned about it, particularly because this was not the first significant data breach from the Ministry of Defence. You have said that you felt that you might get in the way, given that there was an ongoing investigation, but there had been previous Ministry of Defence data breaches, from which clearly the lessons had not been learned. So, while you might have got in the way, do you not think you might also have helped to ensure that data practices came up to the standards that meant that another breach would not happen? Would you make the same decision again, in terms of not investigating, given everything that you understand and know now?

***John Edwards:*** We have undertaken a subsequent review of the information that we knew at the time and what we have learned since the super-injunction was lifted. We have gone back over the information and I have taken the decision that there is nothing to impugn that original decision, so I think the answer I would give is yes.

I know, Madam Chair, that my opening answer was long. I hope it was not rambling, but I wanted to refer to one last element: the decision was to take no further action in terms of the formal investigation. It was not a decision to do nothing. I wrote to the Chancellor of the Duchy of Lancaster immediately after the super-injunction was lifted, to say, "We have been working together for two years in this public sector approach and it is not working well enough; we need to raise our game." I think that we have got very serious engagement from the Cabinet Office and DSIT to work with the ICO to learn these lessons. I think that the chair and the permanent secretaries have written to the Committee to outline some of those steps.

Q7 **Chair:** They wrote to us yesterday, yes, to outline some steps, which we are glad that they are taking. I am still somewhat stunned that there are steps that had not already been taken and that, following previous data breaches, the level of data protection and security was such as to enable another data breach of this magnitude, even in the conditions that you describe of a fast-moving evacuation in Afghanistan. The cost of that data

breach, which is still being felt by those whose data was shared, as well as by the Department, is such that your assurances that the Ministry of Defence is finally acting are not reassuring to me, given the level of bad data practice and the length of time for which it went on, whilst you were responsible for putting in place good data management practices.

***John Edwards:*** I understand the point. Can I respond, briefly, because I think the timing issue is important? The way I have heard the question, it seems to assume that we investigated the Bcc breach, learned lessons and fined the Ministry of Defence, and then this new thing happened, and because the new thing happened it is clear that they had not learned the lesson. Actually, that is not the case, Madam Chair.

Q8 **Chair:** Just to correct you, because other members want to come in, that is not what I am saying. I am very well aware of the timing, but the fact is that these lax data management practices had been in existence for years, so, whilst your inquiry happened before the last Ministry of Defence data breach was known, your responsibility to ensure good data practice in the Ministry of Defence has been in place for years and we have not got good data practice in the Ministry of Defence; and you chose not to investigate that when you were aware of the data breach.

***John Edwards:*** That is correct.

Q9 **Chair:** And you stand by that decision.

***John Edwards:*** Yes, that is correct.

**Chair:** Kit, and Martin, did you want to come in?

Q10 **Kit Malthouse:** I share the Chair's surprise that, given the severity and significant impact of this data breach, both on individuals and financially on the taxpayer, you have, broadly, said to us—forgive me for shorthanding it—that it was dealt with by a few unrecorded meetings and a handshake. "See ya, nothing to see here." It seems extraordinary to me, given its severity and impact, that there was not a more thorough, in-depth, investigation or review, not just of this particular episode but of what may in fact be widespread practice in the field in handling significant data.

I guess my question is, who were the correspondents on the MOD side? You are indicating that you personally did not have any dealings with the MOD at a senior level, but the MOD and, in my experience, the armed forces have a way of wheeling out the top brass to exert a bit of influence over the direction they want something to go. This was obviously—hence the super-injunction—something that the Government really did not want to talk about at all, both for security reasons and, frankly, for reputational reasons. So the picture you have painted for us of the way the ICO handled it seems alarming.

From what you told us, how are we supposed to draw any assurance either that this will not happen again or that the consequence of it has been embedded within the thinking of the MOD in their future practices?

Would you be able to at least give us a list of the senior contacts—individuals—or meetings that were held by your office? So, for example, were there any ministerial-level meetings?

***John Edwards:*** No.

Q11 **Kit Malthouse:** Were there meetings above a certain rank? Did they wheel out, as it were, the Chief of the General Staff? Were high-ranking generals wheeled into the meeting to talk to your staff? I am referring to those kinds of human-level influential things with an organisation which wants to keep this very quiet, and went to court to keep it very quiet for a very long time.

***John Edwards:*** First, I would say that there was no handshake and there was no Orwell "See You Later". There was a commitment from my office to continue to monitor and ensure that standards across the public sector were raised and that the lessons of this terrible case were not lost or wasted. We determined that there was little we could add by way of investigation. I accept that one thing we can do is issue penalties, but if you take that out, was there anything we could learn from an investigation? I think the Committee has available to it a very detailed report commissioned by the Ministry of Defence, which we saw. That made a large number of recommendations to the Ministry to ensure as best as possible that these kinds of events would not occur again, from the governance level to the training level and operational and technical levels.

Q12 **Kit Malthouse:** I hope you would accept that an investigation is not just about learning lessons. There is also a deterrent effect from an investigation. Putting an organisation through a root and branch investigation is something it really does not want to do and will seek to avoid for the future.

***John Edwards:*** Yes. We had done that a mere 18 months prior with the same unit in the same organisation in relation to very similar practices when a staffer at the Afghan relocation unit sent on several occasions emails that were Cc'd, not Bcc'd. We investigated, we reprimanded and we issued a monetary penalty of £350,000. When this matter came along and was notified to us some months later, we were confident that the Ministry was taking it seriously and was investigating it appropriately.

Q13 **Kit Malthouse:** How do you extract that confidence, and from whom? A senior person comes out and tells you they are taking all of this terribly seriously? Without investigating the day-to-day practice how can you assure yourself, particularly in the light of a previous breach from which they had not learned the lessons?

***John Edwards:*** I think they had learned the lessons of the previous breach. But the breaches were quite closely contemporaneous, so I don't think it is fair to characterise them as an ongoing pattern of not learning lessons.

**Chair:** To clarify this, the breach took place in February 2022.

Q14 **Kit Malthouse:** Sorry, can you just answer my question about how you extract that confidence? Is it human contact?

***John Edwards:*** It is human contact, briefings, and experienced investigators asking questions and receiving assurance that the appropriate lines of inquiry are being followed.

Q15 **Kit Malthouse:** Therefore, it is what they tell you; it is a handshake.

***John Edwards:*** That is every investigation, Mr Malthouse.

Q16 **Kit Malthouse:** No, it is not.

***John Edwards:*** Yes, it is.

Q17 **Kit Malthouse:** An investigation looks at what physically happens to the data and what steps are taken in handling the data on a physical machine where the steps are auditable and verifiable; it is not just taken on the basis of, "Well, I did this; believe me."

***John Edwards:*** I think you are oversimplifying. We ask questions; we receive answers. That is every investigation.

Q18 **Kit Malthouse:** The investigation would never physically look at the software and hardware practice in reality; it would just take it as read on the basis of, "Whatever I send you in a letter is true."

***John Edwards:*** I don't think there was any mystery about the technology or the practices here. We knew that a spreadsheet had been emailed from within the Ministry of Defence to a trusted external party, and that from that party it had been further distributed, and that a screenshot of that had been placed on a social media post. That was what we were told. My staff had no reason to doubt what we had been told.

**Kit Malthouse:** It is more about what they told you about how they would go about it.

Q19 **Chair:** We need to move on. You did an inquiry into the first data breach that took place. What was the date of that inquiry?

***John Edwards:*** Do you mind if I first answer Mr Malthouse's question? He asked about the levels of the people who were briefed. I don't have that, but I will come back to you with that information. My understanding is that we would have been briefed by the data protection office of the Ministry of Defence, because that is usually the level at which we work. It certainly was at working level. I don't think there was the sort of rank inflation that I recognise in your question. I come back to your question, Chair.

Q20 **Chair:** You said that the first data breach in the Ministry of Defence was contemporaneous with the Afghan data breach.

***John Edwards:*** The email issue with the Bcc occurred in September 2021 and we were investigating—and the spreadsheet was emailed out in February 2022.

Q21 **Chair:** You felt that the investigation that you had done in 2021 effectively covered the period when the new data breach had occurred.

***John Edwards:*** We did not conclude our investigation into the 2021 breach until December 2023. There was a process of investigation. Unfortunately, it would not be unusual for a six-month period not to reveal much—

Q22 **Chair:** I understand that, but referring to Kit's questioning in regard to how you carry out an inquiry, that inquiry into the data breach was carried out in September 2021.

***John Edwards:*** Yes.

Q23 **Chair:** As for the Afghan data breach, no inquiry was carried out. So, the methods we are talking about were not used with regard to the Afghan data breach.

***John Edwards:*** I suppose we need to pause and think about language. We use the term "investigation" to mean a quite formal process whereby a controller is notified and that invokes a series of legal consequences. "Inquiry" is a much more informal term. We might be considering, we might be asking, we might be gathering information; we are being briefed. Here, we were inquiring; we were being briefed about the Ministry's response prior to making a decision as to whether we should initiate a formal investigation. We made that determination in June 2024 when we were satisfied that the Ministry had responded appropriately by commissioning what it calls an internal-external review.

Q24 **Chair:** In terms of what Kit was asking with regard to how you made that decision not to have a formal investigation, that was on the basis of a sort of question-and-answer, and communication with officials, and you are going to write to us to set out who those officials are.

***John Edwards:*** Yes. My staff would initially have been simply told what was happening. They were told of the super-injunction; they would feed in their observations about lines of inquiry. I understand that those were received with gratitude and followed. On the next occasion, they would have been given an update. They would ask whether they had pursued the lines of inquiry suggested last time; they would be assured that they had.

Q25 **Martin Wrigley:** Chunking this up to a sort of systems question, a few things you have said profoundly disturb me, alongside the details. First, you said that this concerned top secret information and you did not have the people who could do it. Secondly, you said that because it required such a security clearance—I apologise for paraphrasing here—you decided not that you could not do it but that it was too difficult to make

notes on what you were deciding and how to go about it. Both of those suggest to me that you do not have in place any sort of arrangements, or system or process, for dealing with top secret data leaks, which is profoundly worrying in itself.

Thirdly, you said that your only recourse was to fine people. Fining an individual is impactful—

***John Edwards:*** I didn't say that.

**Martin Wrigley:** Fining a profit-driven organisation can be impactful, but fining the MOD £350,000 is completely trivial and a waste of time and space, because you are fining a Government organisation to pay it back to the Government, which pays it back to a Government organisation. So, other than embarrassing a general, you will do nothing at all in any shape or form, and they are already embarrassed. So it is a pointless exercise, just as it would be pointless for any of the newly publicly owned companies— It is like fining Great British Railways. Government is being paid back from sums the Government is paying, so it is pointless. It strikes me that there is nothing in place where you can meaningfully investigate a top secret data breach and have an impact on it. What have you done to change that, so that you are in a position to fulfil your role in such circumstances where your hands were clearly tied when this first happened?

***John Edwards:*** I am sorry to have given that impression because it is not true. We are able to investigate top secret matters. We chose not to do so because it would have tied up resources that could have been better deployed elsewhere. We have particular communications technology that we can use to investigate. We have protocols and procedures. We don't have enough developed vetting staff and I am rectifying that. That is the key factor, and that is something I simply have to take responsibility for. Because in my first meeting with the intelligence community in about 2022 when I took up the job, I was told, "You don't have enough developed vetting staff." I thought we were getting more, but with staff attrition and the like we have not kept up. That is my responsibility.

If we had had plenty of DV staff, would we have investigated? No. We made a decision about where we deploy our resources. We are always making trade-offs. What would we have been wanting to find out—that a spreadsheet was sent? We knew that. That it contained concealed information? We knew that. That it was sent from the third party? Everything that could have been found was already known. In those circumstances, I think my staff quite properly made the decision that our resources are better deployed not with the single tool of investigation but with other means of influence.

My office is responsible for raising the standards of data protection. There are a number of ways of doing that. You are quite right to identify that fines have their place. I am aware of the criticism that in the public sector it is a money-go-round, so it may not have much impact. That is a

separate topic, but the important thing is that we have not done nothing. We are working closely with Government. We have secured undertakings to ensure that matters of data protection are elevated across Whitehall.

It is important to look back for a moment and look at the ICO, not just as the sole actor in this community but as part of an ecosystem. When the PSNI breach occurred, we investigated. We fined PSNI £750,000, but at that point the Cabinet Office commissioned an information security review which looked across the ecosystem to identify weaknesses. In this MOD case, we had the McIvor report which I understand has been made available to the Committee. That went into considerable detail and provided me with the confidence I needed to know that there was little extra we could add in terms of what was to be revealed from that. It is important to ensure now that I work with senior public servants to convey the lessons of those various reviews, reports and experiences so that they are not wasted and that standards are improved and increased across the system.

Q26 **Martin Wrigley:** I am relieved to hear that you are now pursuing more DV staff, if you have not already got them, because the impression I got earlier was that you didn't have any who could do it, so that is helpful. I am still concerned by your choice not to make any notes. What I heard—it may not have been what you implied—was that it was too difficult to do so given the nature of the topics you had to take notes on. What it comes back to is that, without an effective mechanism for demanding improvement, simply fining public sector bodies is a pointless exercise. What tools do you need? Rather than fine their data departments—are they going to sack five people? Their job will be even worse because they do not have the people—you need some other tool, such as to make them retrain.

***John Edwards:*** Thank you for reminding me of that part of your question. I agree with you that fines are a blunt instrument and should be used sparingly, but we do have a number of other tools. In the investigation pathway, for example, if we find that an organisation has been in breach we can issue a reprimand. We have increasingly been issuing reprimands to public authorities. They do, I think, take notice: they sit up and take notice because they are publicly held to account for their failing.

Q27 **Martin Wrigley:** It is career-limiting.

***John Edwards:*** It can be. There are enforcement notices. There we can get down into the nitty-gritty and say, "You need to do this," and get very practical about the steps I expect to be taken to rectify the failings that led to the breach. So there are a range, but I put the engagement that I have described in there as well. Since 2022 I have been speaking to the public sector chief operating officers' network every quarter and explaining to them what we have experienced in the intervening period, what lessons there are for them to learn, what questions they should be

asking of their data protection staff, and what questions their auditors should be asking. Since the MOD breach, that has been elevated.

We have a commitment from the former Chancellor of the Duchy of Lancaster and from the Secretary of State for Science, Innovation and Technology to raise the standards. I think the package of measures that has been drawn to the attention of the Committee is really important, and I will be supporting the Government in that endeavour. The Government have much more convening power and ability to command the resources to see those improvements than the ICO does on a whack-a-mole basis, which is what investigations are. I am interested in working at a system level, and I think we are starting to see progress with that.

Q28 **Chair:** We will come on to the information security review in a moment, but you say you think you are beginning to see progress. Do you accept that the handling of this breach could have undermined public confidence in the ICO?

***John Edwards:*** No, I don't think so.

Q29 **Adam Thompson:** I want to turn to the information security review. To start, simply, do you agree with its findings and recommendations?

***John Edwards:*** Yes.

Q30 **Adam Thompson:** Grand. As for the implementation of those recommendations thus far, can you comment on how far that implementation has gone so far and whether any of the 14 recommendations have not yet been implemented? How do you think it is progressing?

***John Edwards:*** I think it is a work in progress. One of the mistakes that get made in this field is that you have a crisis, you make a recommendation, you enact it and tick that off. It is one and done. These are enduring matters which need to be revised and updated on an ongoing basis. For example, one of the recommendations—I might be mixing up my reviews—is that the letter to the permanent secretary include an obligation. Well, permanent secretaries change, so that needs to be done on a cycling basis. Are there any particular recommendations that you want to drill into?

Q31 **Adam Thompson:** I was broadly interested in your assessment of how you think it is going. Do you think there are any holes?

***John Edwards:*** To Mr Malthouse's point, we can only act on what we are told. It is quite a challenging prospect to audit your way into assurance right across a system, but I am encouraged. I think it was an important piece of work; I think it was an appropriate piece of work. I understand that these issues are being taken seriously across the system.

Q32 **Adam Thompson:** Would it be fair to say that at the moment in your assessment there is nothing that has necessarily failed to be implemented?

***John Edwards:*** I don't believe so; no. Some of these involve degrees. For example, is there sufficient transparency in information collection practices? How do we judge that? Improvements in transparency do need to be made in some places. One of the challenges with data protection is that it is everywhere and infinite, so it is hard to get complete reassurance that there will never be some area that can't be improved.

Q33 **Dr Sullivan:** Some interesting themes are emerging. It sounds like your method of investigation relies a lot on honesty on the part of the person you are investigating. If people are perhaps not as honest as they should be in coming back to you, what have you got up your sleeve? What enforcement means do you have that can challenge that? How do you deal with that kind of honesty?

***John Edwards:*** I would like to think we are not quite so guileless as the question might imply. First, I need to clarify something: we did not investigate. It may seem a pedantic point. Yes, we were relying on honesty, but had we later found we had been misled, we could have investigated. We made a decision not to investigate based on reassurances, which are based on honesty, but we did not investigate. Had we chosen to investigate, we could have issued information notices, for example. These are statutory demands. We could have inspected the kinds of facilities on the basis on which Mr Malthouse challenged me—"Show us your documents." A new piece of law under the Data (Use and Access) Act will give us the power to commission technical reports. So I don't believe that we are merely the passive recipient of assurances. I think the Russian proverb "Trust, but verify" has probably been an indicator of our approach.

Q34 **Adam Thompson:** At the tail end of July you wrote to the previous Chancellor of the Duchy of Lancaster. I think you requested a meeting with him at that point. Did that meeting go ahead, and what were the outcomes? Were you reassured by what you heard?

***John Edwards:*** That meeting did go ahead. It was on a Friday. When I walked out, we heard the news that the Deputy Prime Minister had resigned, and within 24 hours there had been a reshuffle. I believe that was the last meeting we had with the Duchy of Lancaster.

**Adam Thompson:** Just before the reshuffle; interesting.

***John Edwards:*** It was clear to me that he took these issues extremely seriously. He was joined by his permanent secretary, Cat Little. There were other officials whom I have met subsequently to iron out some of the details of our further engagement. Those have been very productive. We have a draft memorandum of understanding which builds on the undertakings from that meeting. To return to your point, yes we had a meeting, yes we got a full commitment. I was under no illusion that the Chancellor was fully apprised of the criticality of maintaining trust, in terms of being able to execute the Government's transformation objectives, for example.

Q35 **Adam Thompson:** Have you yet had the opportunity to interface with the new Chancellor, who took over a few days later, to examine whether continuity exists on those points?

***John Edwards:*** No, I have not in this role, but I am confident that he will be receiving advice that the undertakings that were given by his predecessor ought to be honoured and taken forward.

Q36 **Adam Thompson:** Do you have intentions to hold such a meeting?

***John Edwards:*** Yes; I think our offices have been in touch.

Q37 **Adam Thompson:** More broadly, what do you think the Government need to do to address the concerns and, to go back to the data breach, to ensure that such data breaches do not happen again? What else do the Government need to do beyond what they are doing at the moment?

***John Edwards:*** I think the bringing of a centralised approach, as indicated in the package of measures that has been shared with the Committee, is really important. It is important to be able to hold individuals to account and that is what those measures will do. Data protection has been seen as a technical skill that is discharged somewhere else—for example, "Don't worry; we've got a DPO." In the modern age, that is not enough. There are not just technical and technological challenges; they have to be embedded in the culture. Most of the significant breaches that we have seen and discussed today have been a result of human failings and a failure to make pretty basic checks. Underpinning that is training; it is technical steps—for example, someone noticing that there are 30,000 lines on a spreadsheet and saying, "Why would you do that?" There are stop-loss mechanisms you can put into the software. And governance. That is where I think the letter you have received will make a difference. We now see responsibility in a Government chief digital officer who will hold to account counterparts across the sector. We will see audit committees demanding assurances and checks on these data matters as well as financial matters. That is another really significant step.

Q38 **Adam Thompson:** Using this particular breach as an example—30,000 lines on a spreadsheet shared with an external organisation and then disseminated through that organisation, accidentally or otherwise—I think we all broadly agree that that is not an appropriate way to share the data. In your view, what is an appropriate way to share the data in that particular example, and how do you embed that answer into the culture of the whole organisation?

***John Edwards:*** I will not answer the question about how the MOD should have handled that matter because it depends on the operational needs and the technology available. I don't think I am able to add much there. How do you embed it into the culture? From the top to the bottom. A colleague at the NCSC said to me a couple of months ago, "Can you imagine a chief financial officer going in to the board with the profit and loss accounts, the depreciation schedules and the like, and board

members saying, 'Oh, look, I don't understand all that financial stuff; it's too complicated'?" But that is what happens with cyber-security and data protection every day.

Q39 **Adam Thompson:** With respect, John, on the question that I asked, I appreciate you said you are not aware necessarily of the exact technology available, but if you cannot answer the question of what the appropriate route is and that is not embedded throughout even your own response, how can we have confidence that that is going to pervade through the whole organisation?

***John Edwards:*** I am sorry if I misunderstood. I thought you were asking me the appropriate way for the Ministry of Defence to share information in its particular operational context. The reason I cannot do that is that there are a wide range of technologies available, and the MOD needs to choose the one that meets its operational needs and has sufficient safeguards and protections. What we do know is that the way it did that was not appropriate.

Q40 **Adam Thompson:** Sure. In that case—and I accept that—is there a road map between where we are now and the position where every single person in the organisation can say, "Yes, this is the right way to do it"?

***John Edwards:*** Probably not.

Q41 **Adam Thompson:** Should there be?

***John Edwards:*** Everyone in the organisation should know whom to ask where they have a doubt or a concern. Everyone in the organisation should know that the reputation of the organisation and its licence to operate turns on its ability to safeguard the personal data that has been entrusted to it.

Q42 **Chair:** You are saying that you cannot say how the MOD should have shared that file because those are its operational choices, but you can say that it should not have been sharing a file with 33,000 lines. Surely, there are best practices that should be known and agreed across all Departments.

***John Edwards:*** Yes.

Q43 **Chair:** When the Cabinet Office wrote to me in August, it said, "Many Departments are already following the Microsoft 365 guidance for the UK Government," which implied that many Departments were not following it. There is a lack of best practice standards across government, is there not?

***John Edwards:*** I don't want to leave the Committee with the impression that there is a vacuum. We produce guidance all the time. We have data-sharing guidance that, if followed, would have avoided this situation. Nobody intended in that case to share 30,000 lines of data. That was contained in a hidden cell. The person had a legitimate need to share a

limited amount of information. They accidentally shared much more than they intended to, and that was where the fault lay.

Q44 **Chair:** I am sorry, but that really is not good enough, is it? There should be practices in place to prevent that happening, and there were not.

***John Edwards:*** Yes.

Q45 **Chair:** The question again is: is there best practice guidance across all Government Departments? If not, when do you feel it will be in place?

***John Edwards:*** There is best-practice guidance available to everyone.

Q46 **Chair:** Available, but not necessarily used?

***John Edwards:*** Whether they access it and whether they know to access it are some of the things that the Government would be ensuring are embedded within the package of measures that have been shared with you.

Q47 **Adam Thompson:** I must say I remain concerned, if I am honest, John, by a lot of the answers that we are going through today. A last question from me before I hand back: with hindsight, would you do anything differently?

***John Edwards:*** I would, actually. I would probably have held off announcing our decision to take no further action until we had been able to put it in the sort of context that I have been able to share with you today. There was a bit of fervour when we were told that the super-injunction was being lifted on a particular day. We knew there would be a lot of press coverage. We took the decision to issue a statement so that it was all there for those who were interested. In hindsight, it probably would have been better for us to take a little more time to reflect a bit further and perhaps to go back to the Ministry and get the sorts of assurances that we have subsequently been able to obtain that there was insufficient reason for us to invest further resources into a formal investigation.

Q48 **Chair:** Before we move on to other challenges as well as the data breach, just to clarify, in the letter that the Ministries have sent to us yesterday, they say that the Government will draw up a joint commitment with the ICO to work together to raise standards by the end of 2025. In your understanding, is that to raise standards by the end of 2025, or is that to have a joint commitment? How are you working on that?

***John Edwards:*** I wish we could raise the standards. I think we will. But we will certainly have settled that commitment, and we will have the kind of road map that the Committee has been asking for. I would look forward to reappearing in front of you next year and reporting on the progress that we have made, and I would expect the standards to have been raised.

Q49 **Chair:** So the joint commitment that we will see before the end of 2025

will have in it a road map to set out the standards that you are looking to achieve and what we can expect.

***John Edwards:*** We are in the early stages of discussing that, but yes. We need to be accountable. There need to be measurable standards by which you can have assurance that we have been doing our job.

**Chair:** Great.

Q50 **Dr Sullivan:** Do you expect that there will be more self-reporting of potential breaches if the awareness of the need to prevent data breaches is more embedded? You mentioned a lot about the human element. Of course, the human element means, sometimes, mistakes. How do you help people go through that process and learn from them and put their hands up and go, "This is what's happened; how do we learn from it?"

***John Edwards:*** Yes, you do need to have a culture of learning and reflection. You need to be able to ensure that people are supported to notify matters that might indicate a near miss, for example. Organisations probably will see an increase in breach notifications. I am not sure that we will see an increase—I would hope that we don't see an increase in notifications to us, because we have a threshold of harm prior to requiring notifications. I would expect to see internal notifications go up, but notifications to us to come down.

**Chair:** Thank you. That is it for discussions on the Afghan data breach and the levels of data protection and management in government. You can tell, John Edwards, that the Committee has outstanding concerns on what has been brought to light through the work of this Committee and through the evidence that we have heard. We are now going to move on to a topical issue that is closely related to our standards of data management and practice.

Q51 **Martin Wrigley:** I would like to talk about digital ID, which is clearly very topical. It is interesting that you talk about having the ability to report problems and to acknowledge mistakes. One of the biggest barriers to innovation in this country is the fact that we continuously point fingers of blame and say, "You have failed," rather than learning from failures—allowing people to fail and learn the lessons. You described data protection as "everywhere and infinite", which means there will always be errors in places because not everyone all the time is perfect. We are people, not robots. Thank you for what you do. We are coming down harsh on you, but we appreciate what you do and it is so important to us, which is why we are asking these questions. What is your view on the announcements of the Government's digital ID scheme?

***John Edwards:*** There is not enough detail for me to express a clear view. The new thing that was announced was the obligation to produce a digital ID when seeking employment. Beyond that, we don't really have much detail. There will be a whole lot of decision points in the preparation of the legislation. There will be a whole lot of decision points in the development of the technology to support the solution. I would be

expecting to work with Government to influence those decisions in ways that maximise the public's trust in whatever solution. It is for the Parliament, I think, to determine the legitimacy of the policy objective and, once that has occurred, for my office to help to identify ways in which those objectives can be achieved consistently with data protection and privacy values.

Q52 **Martin Wrigley:** I am very interested that you say that because some of the things that were described in the statements that were given to us in the Chamber were quite frightening. The right-to-work checks that were described were implied to include the ability to check on employers. That in itself therefore says that there will be a record of the employer checking your ID sent to some central system as proof. The same is discussed in the right to rent.

The digital ID has your age, so you now have a verified age check, which is probably better than any of the age checks that will be carried out anywhere else. As well as online systems—and again, this is an extension of how a well-intentioned scheme may go—you have a verified age check. This might save significant time at supermarket checkouts where you have to verify the age for buying a bottle of vodka, or a razor blade or a headache tablet. The supermarket will also wish to prove that it has complied with the law and the verification, so that will also go back to your central records. I think you can see where we are going. The supermarket probably also wants to check that little Johnny has not borrowed his mum's phone to do the age-verification check because he has her payment card on the phone and is buying a bottle of vodka. It will probably want to then also access the photograph on your age-verification check because it has cameras on the tills already. You now have an automated till system in the supermarket that does not require a member of staff to come and check the person who is buying the bottle of vodka or the headache tablets. All these records are going back. We talk about federated systems. Perhaps that is a blockchain record or something like that. You are now instantly getting to a point where we are starting to breach many data privacy rights.

The Government also indicated cross-systems data matching. They talked about matching data from different systems to look at different bits and pieces. We have data warehousing largely done by a company called Palantir, which has its fingers in a lot of these different systems. It has overview on medical, Cabinet Office and defence systems, and of course policing systems. All of a sudden, I might have to prove that an AI hallucination that has pulled all this data together and has assumed something that did not happen—because we know hallucinations happen—was wrong, and the imagined trail of digital ID implies some wrongdoing. I am having to dive into really detailed technical records and places to prove my innocence based on the existence of a digital ID that has suddenly spread to other very well-intentioned uses. What is the role of the ICO in preventing that happening?

***John Edwards:*** We would ensure that the design principles include data protection principles such as data minimisation, purpose limitation and a data protection impact assessment. The kinds of harms that "Future You" has experienced in that narration can be predicted from the design choices that are made now, and that means that if we examine them and predict them we can mitigate them. I don't know that it would be productive for me to go through each of the steps in your scenario.

**Emily Darlington:** It was rather a dystopian view.

**Martin Wrigley:** Of course it is. You look at the dystopian and work out how that is prevented.

**Emily Darlington:** It is not for us to debate what is in there.

**Chair:** We spent quite a lot of time on digital ID last week.

Q53 **Martin Wrigley:** How do you think the Government could ensure that we use this to keep existing data protection valid?

***John Edwards:*** There are a number of ways. As I said, there are policy choices, legal choices and technological choices. On the policy and legislative side, if you want to limit the ability of police or any other person in authority to require the production of a digital ID, you can put that in the legislation and say, "It can be used for this and it cannot be used for anything else." From a technological perspective, you can have a system whereby a digital ID does not retain or enable the linking of the data in the scenario that you described. I can prove myself to my landlord, to my employer and to the Tesco that I am buying my bottle of vodka from, but there is no one point at which those different data points can be drawn together simply from the fact that I have used that ID. There is a lot of water to go under the bridge in this. You can be assured that the ICO will be there informing those choices, to avoid the kind of dystopian outcomes that you are rightly concerned about.

Q54 **Chair:** Can I just clarify this? If you feel that it will bring you additional work, will it bring you additional resources?

***John Edwards:*** This is our work, and it just means we will have to make trade-offs within what we do.

Q55 **Chair:** The kind of trade-offs that led to you deciding not to investigate the Afghan data breach.

***John Edwards:*** Precisely.

**Chair:** It sounds like you are going to be having more trade-offs at a time when data protection and data management will be even more important and a fundamental basis of the Government's digital transformation. Lauren, do you want to come in?

Q56 **Dr Sullivan:** On digital ID, yes please. Do you think citizens broadly have the right not to be included in digital data?

***John Edwards:*** Have the right not to be? I am not quite sure how you would execute such a right.

Q57 **Dr Sullivan:** Supermarkets, as was raised earlier, have our buying habits; they have cameras and all that sort of stuff. You can choose not to have a loyalty card for a supermarket.

***John Edwards:*** Yes.

**Chair:** Many do.

**Dr Sullivan:** Do you think that that is a right that people should have?

***John Edwards:*** As I say, I think in today's society it is almost impossible to understand how you would execute that. The UK is probably the second most surveilled nation in the world. I simply cannot avoid shedding my digital ID dozens of times a day as I go about my business. You can try and pay with cash. Try getting on a bus and paying with cash these days. I genuinely don't know how you could achieve that.

Q58 **Dr Sullivan:** On a slightly different tack, this morning on BBC News they were talking about mobile phone thefts. Somebody on the channel said how he had his phone stolen. His bank accounts were securely in his wallet on his phone, but his life savings were gone into crypto. How can the Government show competence in being able to keep that ID safe? Is that something that is possible?

***John Edwards:*** That is absolutely critical to the success of any such scheme. You can legislate all you want, but these systems won't work unless people trust them, and people won't trust them unless they can be reassured that an office like mine has been overseeing the development. We are the proxy for the citizens. If we have reservations, we will share them, and I think Government will take those seriously.

Q59 **Emily Darlington:** Really quickly on the digital ID point, we have some major concerns in terms of identity theft, of financial fraud and of third-party providers verifying our ID and us not being clear about where that data ends up, even though they claim they erase it. Do you think there is a role for Government-issued digital ID in cutting through some of those issues—something that is more secure, something that is free and something that clearly does not have a commercial interest in it?

***John Edwards:*** There is. The original approach was to create a trust framework for the creation of digital IDs—sort of letting 1,000 blossoms bloom—and people can then exercise choice about what service they select and which ones they use in different places. The service offering that the Government might choose with a digital ID, if it is designed in a way that provides assurances about privacy and security, may turn out to be a default identifier for a range of different purposes. If people are concerned about the kind of misuse that Mr Wrigley described, they will say, "Okay, I need my digital ID to get my job, but I will go to the commercial sector to get the ID that I need to buy my vodka or show my

right to rent or whatever else." It is a marketplace. But there is certainly a need for people to be able to reliably verify themselves online, and I think the Government have a role to play there.

Q60 **Dr Sullivan:** On data access and use, I asked about consent of data and how we can help empower citizens. I think the digital ID has unlocked the fact that there is an awful lot of data out there owned by other companies and in other countries. How do citizens take control of their data and have that at the heart?

**Chair:** Could you just say a word about how the Data (Use and Access) Act extends both your powers and the Government's powers to share data, particularly with regard to automated decision making? How can we empower citizens in that context? How will you fulfil your remit to empower citizens in that context?

***John Edwards:*** Transparency and ensuring people have meaningful choices are key. The point that you make is important, and people need to have those choices, but I also worry about that conversation being overtaken by those in whose interest it is to manipulate those choices. We need to make sure that the agencies that are collecting data and profiting from it are held to account, made to be transparent and limited in the ways that they can repurpose data.

Q61 **Chair:** In terms of transparency and making them limited, that is part of your role in ensuring that repurposing and the reuse of data is fair and within the existing legislation.

***John Edwards:*** That is right, yes.

Q62 **Chair:** Do you feel you have the powers and the resources to do that? You have to choose your battles very wisely, do you not, because you have a limited set of resources and an almost infinite set of data?

***John Edwards:*** Yes, quite so. We do. We don't want to get in the way of innovation as well. There are huge opportunities for businesses to provide better services to citizens and consumers. There are enormous efficiencies to be made in government by better use of data. The rule of thumb that I use in talking about some of these is: if you are going to do something for people, you have a lot of latitude; if you are going to do something to them, you really need to have a thorough and close examination of your legal authority and of the potential negative impacts of that.

Q63 **Chair:** You said that we were the second most surveilled society in the world. That was a very precise position in a league table that I am not aware of. Where does that come from?

***John Edwards:*** I did caveat that with "I think". I recall some years ago a statistic that the UK was the most surveilled society in the world.

Q64 **Chair:** Okay. Well, come back to us on that.

***John Edwards:*** I know that some of the trends in China, for example, may have bumped the UK off the top position, but I don't know whether there are any reliable metrics on that.

**Chair:** We will come back to that.

Q65 **Emily Darlington:** Could you share that with us? I am not confident about that.

***John Edwards:*** Neither am I. I am sorry; it was not cited and footnoted.

Q66 **Emily Darlington:** Public sector data is being held in many cases by non-sovereign third-party providers such as Palantir, AWS and Microsoft services. How do you, as Information Commissioner, ensure that that public sector data is secure, continues to be owned by and the property of Government and public services, and is not being exploited by third-party providers for other commercial purposes?

***John Edwards:*** Those are contractual matters that the Departments using those services need to ensure. The kinds of outsourcing arrangements that you are describing, I would expect, would rule out commercial exploitation. They may use data to improve their service offering, but that is not—

Q67 **Emily Darlington:** To other people in other countries.

***John Edwards:*** When we talk about use of data, I don't believe that any outsourced provider of the sort that you have described would be using identifiable data in a commercial way.

Q68 **Emily Darlington:** You don't believe that, but what is your role as Information Commissioner to take that from, "you don't believe," to, "you are sure"?

***John Edwards:*** As the Chair noted, we have to choose our battles carefully. If I have no basis to suspect that there is inappropriate use of data by a third-party outsourced provider, I would not launch an investigation. If I had that concern, we would look at it.

Q69 **Emily Darlington:** That is not entirely reassuring. Do you have a role in monitoring or in the language used in those contracts to ensure that any use of it would be illegal?

***John Edwards:*** We have the law, which says to the controller, "You must take adequate steps to ensure that all the data protection principles are observed."

Q70 **Emily Darlington:** Who reviews if they are adequate steps? Is that not your office?

***John Edwards:*** Yes.

Q71 **Emily Darlington:** Right. So are you reviewing if the adequate steps are being taken?

***John Edwards:*** My expectation is that they are. If a Department chooses to use the services of AWS, Microsoft 365, Palantir or any of the others, my expectation is that they do that in a way that guarantees the security and safety of citizens' information.

**Emily Darlington:** Okay. That is something for us to note in our report—that there isn't any regular checking of this.

**Chair:** Emily, you have brought up an important point.

**Emily Darlington:** I am shocked.

Q72 **Chair:** Another important point, sorry. I am trying to formulate it in a way that makes sense. You are not a data advocate for people. You are not a proactive champion of people's data rights. You are a reactive guarantor and enforcer of existing regulation.

***John Edwards:*** I am not sure that is an accurate characterisation. We are many things.

Q73 **Chair:** If you are a proactive champion of people's data rights, Emily's point is that there is not very much proactivity.

***John Edwards:*** I don't know how productive it would be to go around inspecting every data transaction that happens in the economy without any basis for concern.

Q74 **Emily Darlington:** I am asking about public service data. We know that there is an over-reliance on non-sovereign companies. Let me put it this way: is the fact that there is an over-reliance on non-sovereign companies in terms of our data handling and use in the public sector of concern to you? Should there be prioritisation and moves within the Government to ensure that there is sovereign capability in order to feel that public sector data is more secure?

***John Edwards:*** Is there an over-reliance? I don't know. There are enormous efficiencies. These are business decisions that the Government are entitled to take. I know that I am here to answer questions, but I wonder if I can indulge in asking one.

Q75 **Emily Darlington:** You can. Go ahead. I don't know if I have the answer.

***John Edwards:*** Are you concerned that there is a misuse of data by a third-party provider processing public sector data? If there is, I would go and investigate. Could you give me an example?

Q76 **Emily Darlington:** I am concerned that we don't know. For me, the role of government and the role that we have is ensuring that our health data, benefits data, taxation data and any other bits of data that government rightly holds on us should be absolutely secure.

***John Edwards:*** I agree.

Q77 **Emily Darlington:** The fact that we don't know definitively, and you

don't know definitively—because it is your role in that assurance—worries me. I would love for you to say, "Absolutely, this does not happen," but you cannot say that today, and that is what worries me.

***John Edwards:*** Is it possible that you are asking me to prove a negative?

Q78 **Emily Darlington:** It is possible that I am asking you to prove proactiveness.

***John Edwards:*** We provide proactiveness. There are standards that apply to outsourcing. There are contractual measures that we would expect Governments to take. If your policy position is that government should never use third-party providers, that is an entirely legitimate position to take.

**Emily Darlington:** This I do know, as opposed to the other statement: we are the second most cyber-attacked country in the world after the US. That can be for commercial purposes to get money. It is also being done by malign actors and state actors across the world to destabilise us as a country. Yes, it is about the safety of our public sector data, which is under daily attack. We need to consider the question whether non-sovereign third-party providers put us at risk, given the fact that we know we are already in the firing line. That is an important question and one I would love for you to take away, consider and come back to the Committee on, because we need to consider if that would make us more secure. If you don't think it does, that is also a very legitimate point. It would be great to have the thoughts of you and your team in terms of whether this is something that the Committee should be continuing to pursue and ask questions about. Can I talk about online safety?

**Chair:** Yes. We only have 15 minutes left.

Q79 **Emily Darlington:** It will be quite quick. First, the Online Safety Act brought in age verification for access to over-18 material. Have you looked into the third-party providers and the safety of the data? That is what I get the most complaints about in terms of the Online Safety Act. It is not having to prove you are 18, but with whom you are having to prove it, which tend to be non-sovereign third-party providers that people are not comfortable providing that data to.

***John Edwards:*** We have issued guidance jointly with Ofcom about how to achieve the obligations under the Online Safety Act in ways that meet the data protection expectations of data minimisation, security and use.

Q80 **Emily Darlington:** What more could you do to increase confidence that, when people are proving they are over 18, that data is secure?

***John Edwards:*** We could audit. We could investigate. There are all the tools that we have to provide assurance across the economy. We are looking at a number of online services for their age-assurance practices.

Q81 **Emily Darlington:** Okay. You have investigations into TikTok, Imgur—I

never know how to pronounce it—and Reddit in terms of their use of data and AI algorithmic targeting of children. Imgur, however you pronounce it, has pulled out of the UK. It has been clear that that is not necessarily as a result of this investigation. TikTok and Reddit still operate in the UK. How have you found your investigation with them? Have they been forthcoming with the evidence that you have asked for? When will you confirm the outcomes of your investigations? Can you give any indication to the Committee of some early outcomes of those investigations?

***John Edwards:*** Sure. First, I will clarify. The Reddit and Imgur—I do not know either—investigations are about age verification. We are concerned that there were no efforts to verify whether users of those sites were under 13. As you say, the unpronounceable one has withdrawn its service in the UK. We have issued a notice of intent. If you could give me a moment, I have some updates in my notes. There are a couple on the TikTok one. The Reddit one is ongoing; we cannot give further details at this stage. We are at the stage of having given a notice of intent and receiving representation. That is fairly advanced.

Q82 **Emily Darlington:** Has it been happy to give that to you?

***John Edwards:*** I don't know about its level of happiness.

Q83 **Emily Darlington:** I meant it has been forthcoming. It has not disputed that it has needed to provide this information.

***John Edwards:*** No, I don't believe there has been a challenge to providing any information. That does not mean they are happy about it. With TikTok on the other hand, we have a couple of cases that are working their way through the court. The algorithmic processing of data case is one that we commenced to understand the ways in which children's data is used by TikTok to deliver content and make recommendations. It is an investigation into the recommendation system. We served an information notice on TikTok demanding to see data that would allow us to make an assessment of those algorithms. TikTok has appealed that information notice on the basis that it believes it is entirely concerned with processing data for special purposes, which means artistic expression or journalistic purposes.

I will pause there to complete the picture. We issued a fine to TikTok of £12 million in 2023 for failure to get the consent of parents for children under 13 on its platform. It took the same point, which was that it did not believe we had jurisdiction because that data was being used for special purposes. It took that on appeal to the tribunal as a preliminary matter. We won on every point that we argued; we do have jurisdiction. That is an encouraging sign for our ability to undertake the sorts of examinations that you are describing and hold those platforms to account.

Q84 **Emily Darlington:** Okay. We await the final outcome of the initial £12 million fine and the further investigation of TikTok. What is the timeline for that?

***John Edwards:*** I believe we have a hearing on the information notice scheduled for next autumn, but I can come back to you with those. On the substantive matter, the company has appealed further, so the timelines are not in my control.

Q85 **Emily Darlington:** I have a final question about personal data. There are two activities that happen online, unfortunately, on quite a nefarious basis. One is doxxing—publishing of personal details for people then to take their online attacks offline and be able to target people's homes. That continues to be a problem for people trying to get such information down. What is your role in making sure that our personal data cannot be published online, particularly as we know the intention is to further intimidate or attack us? When I say "us", I do not just mean MPs; I mean women, predominantly, right across the country.

The other one is deepfakes, which unfortunately a member of this Committee has just experienced this week, and that is why he is not with us today. He is arguing with Meta that his image and his voice were used in an entirely fake video that was then circulated on Meta. That is your data. That is your voice. That is your image. Somebody has created something that is meant to be quite damaging to the individual. It is not just happening to MPs. Most deepfakes, 95%, are targeted school-to-school at fellow classmates. What is the role of the Information Commissioner in holding social media companies to account for both the data breaches used for doxxing and the continued proliferation of deepfakes to cause damage?

***John Edwards:*** These are important issues and significant challenges. These are often the actions of individuals, and it is quite difficult for the ICO to intervene in those sorts of cases. You are quite right to point out that there is also a role for the social media platforms. It is hard for me to say in a generic sense. Your statement carried the implication that there was a data breach at the heart of it. I don't know how the doxxing might be being undertaken, whether it is a result of—

Q86 **Emily Darlington:** I can give you an example. Somebody calls Experian claiming to be an individual and wants a credit report on them. That credit report gets returned with their home address on it. That is a data breach.

***John Edwards:*** Yes, I agree.

Q87 **Emily Darlington:** There are other ways, particularly around domestic abuse, where people share somebody's data. It is not necessarily a data breach, but they share the personal data of someone they may know. We see this with some of the more prolific misogynists online. They will know the home address of their accusers because they will have done a private investigation. They will then publish it. That does not mean it was obtained illegally, but they are sharing somebody's personal data. You cannot stop it from happening, but is there a role for the Information Commissioner in fining social media companies that do not take it down

fast enough?

***John Edwards:*** People have a right to be forgotten. They can ask to have data deleted.

**Emily Darlington:** It does not happen quickly.

**Chair:** I am not sure that is what Emily is talking about. It is a very specific question for a specific case. Perhaps if you do not know what the answer is now—

**Emily Darlington:** It happens all the time.

Q88 **Chair:** No, exactly. Perhaps if you do not know what the answer is now, John, you could write to us, because it happens all the time and it is quite difficult.

***John Edwards:*** The scenarios that you are describing might better be the domain of the criminal law. You are talking about intimidation, harassment and even threats of violence.

**Emily Darlington:** The law will not pick it up because the only action within the post is personal data, though the intention is obvious.

Q89 **Chair:** Perhaps you could write to us with what your view is on those particular scenarios that Emily has set out so well.

***John Edwards:*** I will do that, thank you.

Q90 **Chair:** Before we leave, I have one more point that we have not raised with regard to a facial recognition technology audit. The ICO has highlighted the need to deploy facial recognition in a way that supports effective policing and has public support. Do you have plans? What more needs to be done to achieve this?

***John Edwards:*** Sorry, to achieve what?

**Chair:** Deployment of facial recognition in a way that supports effective policing and attracts public support.

***John Edwards:*** At the moment, the principles-based GDPR is the primary form of regulation of facial recognition technology. I understand the Government are about to consult on further legislative measures that will provide that balance. There is a lot of uncertainty. The principles that inform our oversight of facial recognition technology involve concepts of proportionality. It is not always obvious what the appropriate proportionality is and how many kinds of variables you feed into the mix. There was a situation reported in 2017 of a reference dataset used by South Wales Police including ticket touts. Is that the kind of level that you want to see a surveillance technology at? A lot of people would say that is probably too low. There is proportionality about the severity of the kinds of offences that you are trying to detect, the numbers of people whom you are scanning and the kind of technology and its reliability.

Q91 **Chair:** What is your role in assessing that?

***John Edwards:*** Our role is to make sure that the risks are considered at the outset and mitigated and to make sure that people's rights are protected. With a legislative proposal coming, that will be a further opportunity for us to input some of those. There is also a Biometrics and Surveillance Camera Commissioner to provide further oversight.

**Chair:** Okay. We will leave it there for the moment. I am sure we will be seeing you again. Thank you so much for your contribution this morning. You have heard that the Committee is concerned about the standards of data management across government. We look forward to seeing real progress in ensuring that those standards meet the needs, expectations and rights of British citizens. Thank you very much.