

Science, Innovation and Technology Committee

Oral evidence: Digital centre of Government, HC 790

Tuesday 14 October 2025

Ordered by the House of Commons to be published on 14 October 2025.

[Watch the meeting](#)

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

Questions 191 to 269

Witnesses

I: Nick Davies, Programme Director, Institute for Government; and Jason Liggins, CEO, Crown Hosting Data Centres.

II: Gaia Marcus, Director, Ada Lovelace Institute; and Jeni Tennison, Executive Director, Connected by Data.

Written evidence from witnesses:

- [Crown Hosting Data Centres Ltd](#)
- [Ada Lovelace Institute](#)

Examination of witnesses

Witnesses: Nick Davies and Jason Liggins.

Q191 Chair: Welcome to the fourth session of the Committee's inquiry on the digital centre of Government. We will examine the procurement and infrastructure aspects of DSIT's plans to transform Government through digital technology, and hear civil society and research perspectives on the use of technology to deliver public services.

I want to welcome our first panel and I will ask each member of the panel to introduce themselves in response to the first question put directly to them. I will start with Nick Davies. Nick, it is noticeable that, while the Treasury has figures on procurement generally, it does not break them out into tech procurement, so we have to rely on market intelligence, as it were. I would like to know from you, if possible, whether we know how much tech we are buying; your view of the state of technology procurement; and the impact, if any, that the recent Procurement Act has had.

Nick Davies: First of all, thank you very much for having me. I am Nick Davies, the programme director at the Institute for Government, where I lead our work on procurement and on public services.

On the question whether we know how much we are spending on technology, as the Committee may know the quality of the data around contracts and spending is mixed at best. There are various ways to try to ascertain how much we are spending, by categorisation of the suppliers that are used and the codes used in contracts for what is purchased. Historically, it has been quite difficult to connect the contract data with the spending data.

Q192 Chair: No, then—we do not know how much we are spending.

Nick Davies: I do not have an exact figure. There will be market intelligence firms that will be able to give you a best guess, but it is not as precise as it could be. That is clearly one of the things that the Procurement Act was intended to improve. It includes quite a lot of additional transparency notices. The evidence on that, to date, is a little bit mixed. Use of all the different types of notices is growing, month on month. However, some parts of Government are still publishing fewer notices than they were before the Act came into force. There could be a number of reasons for that. It could be a sign of non-compliance; or it could be, for example, that procurement authorities are choosing not to publish notices voluntarily for below-threshold tenders.

The transparency picture is a little unclear to date, but in theory the Act should improve that. One of our big concerns about whether it will improve it is that there have always been a reasonable number of transparency requirements, but not all public bodies have always met them. That has been, in part, because it has not been prioritised, or seen as a political priority. It is also about the capacity and capability of



HOUSE OF COMMONS

commercial teams. They are often stretched pretty thin, and ensuring you are meeting your transparency requirements is therefore not always the top priority.

Q193 Chair: When you talk about transparency requirements, this is how we will know what has been spent, and on whom, and who the suppliers are. Are there any challenges, in terms of UK tech procurement, that are not addressed fully by the Procurement Act?

Nick Davies: Yes. I think there are a number of challenges, for procurement more broadly. In general, I think that Government is insufficiently strategic about how it uses its buying power. We spend a huge amount, and it potentially has great market-shaping power; but, in general, Government is often quite unclear about what it wants to achieve. Often, it goes to market with highly specified solutions rather than clear outcomes that it wants to achieve. It regularly fails to engage early with the market. Historically, that has been because of a fear of legal challenge down the line; but it means that you do not find out from the market what is possible, and you often preclude potential innovations that you might have been able to procure.

Again, the Procurement Act seems to be helping to address that. There is a preliminary market engagement notice that should de-risk the process of engaging early with the market. In the first six months of the Act, according to data from Tussell, one of the market intelligence firms, more than 4,500 of those notices have been published. Likewise, more than 6,000 pipeline notices have been published. That suggests that Government or public bodies are now doing a slightly better job of engaging early with the market, which should help to achieve better value down the line.

Q194 Chair: Thank you very much, Nick. I am sure we will return to many of the issues around technology procurement in the rest of the sessions.

Jason Liggins, I want to come to you now. The State of Digital Government Review by the Department for Science, Innovation and Technology effectively found that we did not have a record of the legacy assets in all the different Departments. They estimated that between 10% and 50% to 60% of systems were legacy. How can we address the legacy asset challenge, and how can the Government Digital Service identify the funding needed to address that challenge if we do not know what legacy assets we have?

Jason Liggins: Thank you, Chair, and members, for inviting me today. I am Jason Liggins. I am the CEO of a joint venture company called Crown Hosting Data Centres. It is a joint venture between the Cabinet Office and Ark Data Centres, which is now the largest data centre supplier in the UK.

Crown Hosting's job is to save the public sector money, cut energy use, reduce carbon and accelerate digital transformation. We already help the public sector to save £1.5 billion a year through our customers. We do that by moving legacy IT from server rooms and cupboards across the



HOUSE OF COMMONS

public sector, and relocating it to very large, highly efficient facilities. This enables us to save 75% of the electricity used by the rooms, or the facilities. There is no change to the IT itself, because we are just moving it, but we can save that money on the rooms themselves. The potential from that is huge. DWP alone—these are their figures, not mine—save £150 million a year by doing that. We would like to scale—

Q195 **Chair:** They save £150 million by moving existing systems into cooler rooms.

Jason Liggins: Yes. They did that from 2018.

Q196 **Chair:** Or moving it on to cloud services.

Jason Liggins: No, moving it into better, more efficient facilities and consolidating their IT as a result, starting the change process. That is the key. They reinvested that money, then, to further accelerate their cloud transformation and move those workloads to public cloud. They are about halfway through that journey.

Q197 **Chair:** Okay, but the question I asked was whether we know what legacy assets we have, and how we can address the legacy assets without knowing what legacy assets we have.

Jason Liggins: I think that central Government has a better insight into the intelligence, there, than the wider public sector. That is because as part of the HMT ARA returns every Department has to return how much electricity was used by its IT every year, so that its carbon impact can be calculated.

Q198 **Kit Malthouse:** What is the total amount? It is £150 million saving on what total?

Jason Liggins: I am sorry; for the DWP's figures, you would have to ask the DWP what their total spend for IT was. I could not tell you.

Chair: This is a recurring challenge; we do not know what is being spent on IT.

Q199 **Kit Malthouse:** This is on power alone.

Jason Liggins: The DWP's savings are more than just power. They are about consolidation of their IT estate. The power part of it is minor in that total. I do not want to mislead you in that regard.

Kit Malthouse: We were slightly astonished, because we thought 150 million quid being paid to Octopus was a lot of money.

Emily Darlington: Other providers are available.

Q200 **Chair:** Exactly. Back to the question.

Jason Liggins: Central Government does know where their IT is. It is part of the ARA returns that are returned to HMT. DEFRA analyses those figures on behalf of all Departments, to work out the carbon savings.



HOUSE OF COMMONS

Q201 **Chair:** Are you saying that central Government knows where its IT is by looking at power consumption?

Jason Liggins: Yes.

Q202 **Chair:** That does not identify whether it is legacy or not.

Jason Liggins: All the carbon impact that is returned on that is legacy IT. That is because the cloud providers do not return figures that are publishable in those published results.

Q203 **Chair:** Are you not saying that all cloud is non-legacy, and all legacy is non-cloud?

Jason Liggins: I have a particular opinion on that terminology. The terminology that Government uses in there is that all non-public-cloud IT assets are legacy, no matter whether they are old, new or contemporary.

Chair: That seems a simplistic definition, to put it mildly. It is possible to develop new systems, but putting that aside—

Martin Wrigley: It is not the right definition.

Q204 **Chair:** I think we can agree on that. It is an interesting definition, shall we say, and one that the Committee would like to take up, but, putting that aside for one moment, you are telling the Committee that the Government know where their legacy is—using their own definition—by looking at power consumption, and that we can follow that up to try to get an idea of the level of legacy and the level of power consumption.

Jason Liggins: Indeed. I would encourage the Committee, as well, to look at the power consumed by the rooms themselves. The public sector as a whole has tens of thousands of rooms smaller than this one, which has very high ceilings—cupboards, small rooms, small server rooms—with their IT in them. On average, the electricity used by the room to do the cooling is three times the power used by the IT itself.

Q205 **Chair:** Is it possible to identify that through the information collected by central Government?

Jason Liggins: Central Government is encouraged to do submetering so that they can achieve that. I could not comment on where central Government has got in that process.

Q206 **Chair:** Thank you. You bring us to a really important aspect of the digital transformation, which is the move to cloud, hosted generally or exclusively in data centres. We have heard in the last month about significant increased investment in data centres in the UK. As you said, yours is a joint venture with Ark. Has your offer been affected by this huge investment in data centres in the UK?

Jason Liggins: We are investing as a company, ourselves, in such facilities. The investments that have been announced over the summer are long-term investments, and they encompass the whole of what is



HOUSE OF COMMONS

required. We concentrate on the facilities. We put money into building the facilities, and others put money into the IT that goes into those facilities. By doing that, we can concentrate on ensuring that those are the facilities with the lowest possible cost and that they are the most environmentally friendly.

Q207 Chair: Are you saying that, for example, Microsoft Azure or Amazon Web Services are part of your offer for public sector hosting; or are they in competition with you?

Jason Liggins: We are not in competition, no, because we offer a different thing. We offer the rooms and buildings in which the public sector or its public sector suppliers can place their IT. AWS or Azure, as you say, may use facilities such as ours to deliver their services.

Q208 Chair: But they may also use, for example, the £10 billion data centre that is being built in Blyth in the north-east of England to deliver those services.

Finally, on cloud computing, which is an essential part of digital transformation, I have been keen to understand whether the UK Government and public sector are being locked into particular services—AWS, for example, or Microsoft—and how our cloud computing base is distributed between different vendors. Is it possible to identify the extent to which the Government are dependent on any of these big cloud service providers?

Jason Liggins: It is outside my expertise to be able to comment on the particular cloud providers. All I can say is that, in my experience of what Crown Hosting provides, it was set up to break that lock-in from the managed service provider community, which was, and still is, endemic in public sector supply. Departments would be locked into their contracts because they could not move their IT away from a particular facility; so Crown Hosting was invented so that the IT could stay in a facility and the managed service providers could be rotated, as needed; but that is different. That is a private cloud, and not the public cloud that you are talking about, with AWS, Azure, Google and other vendors that are available.

Q209 Chair: How is it a different cloud?

Jason Liggins: Public cloud is where it is shared among every organisation that might be a customer of that cloud. Private cloud is a single customer.

Q210 Chair: Which in this case would be the public sector, as a single customer.

Jason Liggins: The public sector—that might be community cloud, because multiple public sector organisations would be using the same cloud, but the private sector would not have the use of it, for example. That is a community of use.



HOUSE OF COMMONS

Q211 **Chair:** The public sector.

Jason Liggins: Yes. Private is for a single organisation.

Q212 **Chair:** Right. And you offer—

Jason Liggins: We do not offer cloud at all. We just offer the facilities—

Q213 **Chair:** You offer the facilities for cloud and for cloud services, which may be AWS, Microsoft or any other provider, and they may offer community cloud, private cloud or public cloud. We need to understand what the public sector is purchasing but we do not have the full information to assess that.

Jason Liggins: Yes, and the ARA returns will return the private cloud elements hosted in the facilities owned by Government and suppliers such as myself.

Q214 **Chair:** But not public cloud.

Jason Liggins: Not public cloud.

Chair: So it is hard to assess the dependency on any one vendor, or the resilience of what is being offered. Thank you very much for that. I will hand over to Emily.

Q215 **Emily Darlington:** Thank you. That leads really nicely into things that I want to cover around security—our data security and capability security. The National Cyber Security Centre has today, as you will have seen, issued guidance for companies in terms of attacks. I was quite struck by the fact that the number of cyber-attacks, particularly at that significant level, has more than doubled in the first half of this year. We are very aware that it is a new form of warfare that is taking place. In your assessment, how secure is our data—Government and public sector data—and how good are we at combating the security threats?

Nick Davies: I must say that is not an area where I have any expertise, so I would not want to comment on it.

Jason Liggins: I will comment a little bit on it. We are a facilities provider. We specialise in the physical security aspects of that presence. When the IT is in small server rooms and cupboards, it lacks the necessary physical security to protect data in the way you would expect it to. Therefore, we relocate that IT to much more secure premises; we host it in premises that can hold any security classification and any criticality of data. That is the first step that needs to be taken in securing the data.

On top of that, organisations need to lock down their cyber-security to the degrees that NCSC recommends, and it is very good at recommending that. Most organisations follow it as best they can. Legacy IT is a problem. You cannot necessarily secure it to the level you would like because it is legacy. I would encourage any organisation to move as



HOUSE OF COMMONS

quickly as possible away from legacy to the wider concept of more modern infrastructures rather than the definition of legacy.

- Q216 **Emily Darlington:** As I know that five members of the public regularly watch, when you say the data centres that you run are more secure, in layman's terms what do you mean by that? What is the security in that? What is it about legacy systems that make them more insecure?

Jason Liggins: I will answer it in reverse order. What is it about legacy that makes it more insecure? In some cases, they have been built, designed and architected in a time before cyber-security was foremost in our minds, so making those systems secure becomes very difficult. Do you put more wraparounds and security around them to protect those vulnerable assets, or do you replace them with assets that are inherently more secure? Ideally, you replace them with things that are inherently more secure, but that is not always possible. Sometimes you have to wrap them in layers of security to make it more difficult to get to those vulnerable assets.

Crown Hosting is there to move those vulnerable assets from locations that are easy to break into and are vulnerable to things like power outages, or overheating in the summer. Security is not just about confidentiality; it is also about whether the data is correct. We all expect our bank details to be correct at every moment in time. If they are not correct, that is a problem. Think about medical records. Everything needs to be correct. It also needs to be available. If a server room in a hospital overheats and the IT is not available, that causes real-life problems for individuals using those hospital services. Therefore, we move that IT and put it into more suitable facilities so those things do not happen.

- Q217 **Emily Darlington:** How important is it that our systems are built for security purposes on sovereign capability, or our legacy systems are wrapped with a degree of sovereign tech so that it is UK-grown and UK-secure?

Jason Liggins: That is a wide question. We already know the answer to that. It is all to do with whether a foreign nation or foreign organisation could make our data not available so we cannot use it, change the data in some way so we cannot trust it—that is the integrity part of it—or know our secrets. All of those things play into that sovereign element. It is a question of whether we have full knowledge and control of all elements of our infrastructure and data to ensure those things.

- Q218 **Emily Darlington:** How important in GDS and Crown Hosting is their supply chain in looking at sovereign capability, or sovereign tech?

Jason Liggins: We are set up specifically to address that sovereign element. We are UK-owned; we joint venture with the Cabinet Office to ensure some of those things. Our facilities are in the UK; our supply chain is in the UK; and 95% of what we spend goes back into the UK economy. All of those things are extremely important, and we are examined very regularly on our own credentials.



HOUSE OF COMMONS

Q219 **Kit Malthouse:** You say "UK-owned". Who?

Jason Liggins: Ark Data Centres is the majority shareholder. That is a UK sovereign company.

Q220 **Kit Malthouse:** Who are they?

Jason Liggins: Ark Data Centres is a data centre provider in the UK.

Q221 **Kit Malthouse:** I am trying to find out who the ultimate controlling party is. If you say it is UK sovereign that is one thing; if it turns out to be Oleg Deripaska we have a problem.

Jason Liggins: All of the controlling parts of the company are UK and UK nationals that do that.

Q222 **Chair:** Is it intentionally set up to be UK sovereign?

Jason Liggins: It is.

Q223 **Chair:** As it is partially owned by the Cabinet Office, it will ensure that it remains UK sovereign.

Jason Liggins: If there is any change of control—because that is what you are talking about—the Cabinet Office has the right to veto it. That is over and above what exists in the National Security and Investment Act. Indeed, it can step in and take over the company if it is deemed necessary.

Q224 **Chair:** You may not be able to answer this. What proportion of the UK public sector's cloud services is hosted in Crown Hosting facilities?

Jason Liggins: I can talk to the legacy part and the bits that use electricity. I cannot tell you about clouds because it is harder to measure. I do not think we know.

Q225 **Chair:** You have no idea what the proportion is.

Jason Liggins: Between 3% and 4% of legacy IT, as measured by electricity, is with Crown Hosting.

Q226 **Chair:** You cannot talk to cloud, even though that is what your facilities provide.

Jason Liggins: No, not for facilities. GDS did a survey of Departments, arm's length bodies and organisations, and came back with the figure of 60% for services that are in public cloud.

Q227 **Chair:** I suppose what we are getting at here is that, if only 3% to 4% of our legacy systems are hosted on sovereign capability, how resilient and secure in terms of sovereign capability are we? It would seem that the answer is "not very".

Jason Liggins: The other side of the coin is that at least 96% of Government's legacy IT assets are in locations that are not Crown Hosting and, in my opinion, are not as good.



HOUSE OF COMMONS

Q228 **Chair:** To follow up Emily's line of questions with Nick Davies, can you tell us briefly what can be done to reduce vendor lock-in across the public sector?

Nick Davies: In part, it comes back to the point I have already raised. Government needs to be clear about what it wants to achieve and what outcomes it is looking for. Quite often, it does not fully understand what it is buying and the long-term path dependencies that are created by individual procurement decisions.

The other factor is about capability and capacity. The Government on commercial capability have done a pretty good job over the past 15 years in bringing more senior people with private sector experience into the upper echelons of the Government Commercial Function, but it is still a layer of people who are stretched quite thinly and it has similar problems when bringing in that senior digital expertise. Clearly, you are competing with private sector companies that can pay quite a lot more, but you need that expertise because often the solutions will be better developed in-house, or, if you are procuring externally, you can be a better customer if you have more of that expertise in-house.

Q229 **Chair:** You seem to be saying that the Government are not set up to avoid vendor lock-in because they do not understand when vendor lock-in may occur and it is not part of the procurement process.

Nick Davies: That has often been the case.

Q230 **Martin Wrigley:** Pursuing delivery on procurement, you talked about Government going for specified solutions versus outcomes. There are several new desirable features, such as increasing the reliance or weight of UK procurement, as opposed to overseas procurement, for solutions as well as everything else. What more can the Government do to encourage UK innovators and increase the weight of that procurement as a bias towards the UK in preference to other perhaps unreliable partners?

Nick Davies: You are right. Part of the Procurement Act allows that and some of the early data shows there have been more contracts reserved in that way.

As to how you can incentivise it more, there is quite a lot of flexibility, rightly, in procurement legislation and regulation, so a lot of the responsibility will lie with individual commercial teams, in particular public bodies. Where you are looking for them to do something slightly different from what they have always done, whether that is trying to focus on UK suppliers or on SMEs, or whether you are trying to get them to procure innovation, all those things require additional capacity and time to do well. It is much easier to continue doing the thing you have always done, so the question is whether we are investing sufficiently in commercial teams. Clearly, when public finances are tight, it might be a tempting area for cuts, but as to value for money that Government is achieving in the long term you will get a lot of bang for your buck in investing in those



commercial teams. Ultimately, that is probably the main way you can try to incentivise any new types of behaviour.

Q231 **Martin Wrigley:** This is the procurement version of early intervention, in that virtually every service saves money in the long run.

Nick Davies: I have done quite a lot of work on prevention as well. The problem with prevention and early intervention is that it is really difficult to define exactly what we mean by prevention and early intervention because of the long timescales over which returns are achieved, and the outcomes are the cumulative impact of multiple things rather than generally one intervention by Government. Measuring that is quite difficult. I think that, potentially, you have a similar attribution issue with commercial investments. The returns will be seen over many years.

Q232 **Martin Wrigley:** Turning to other aspects of procurement and thinking of my experience externally—I did a lot of work, unfortunately, with MOD PE—MOD procurement still seems to be tied up with working with big prime contractors and not looking towards SMEs and innovators, although there appears to be a desire within the forces to look at more agile ways of delivering things. Certainly, from experience of the way the war in Ukraine has gone, you cannot buy a fleet of 10 million drones 10 years before you need them because they change on a daily basis. The situation is changing. How does Government need to change its procurement guidance and rules to allow places like MOD effectively to buy agile solutions?

Nick Davies: To pick up your point about SMEs, obviously the MOD is responsible for a pretty large proportion of central Government procurement. In general, central Government has not done a good job at buying from SMEs. Between 2018 and 2023 the share of central Government procurement spend with SMEs fell from 12% to 7%, at the same time that overall public sector spend with SMEs stayed flat at around 19%. That is because in local Government, for example, over the same period, spend with SMEs increased from 24% to 30% of total procurement spend.

Probably a number of factors contribute to that. A key one is that central Government contracts, in general, are substantially larger than contracts set by local Government and other parts of the public sector. Large contracts often requiring a balance sheet of a certain size will necessarily exclude smaller potential suppliers. There is often a reluctance to split big prime contracts into smaller lots that might be open to a wider range of suppliers. What it means is that often, particularly in MOD where there is a small number of relatively large contracts, you have a pretty small pool of potential suppliers for that. That means that, often, you are not bringing in the innovation from smaller start-up suppliers who are not in a position to deliver a £100 million contract, but might be in a position to deliver a £5 million contract and then scale up over time.

Q233 **Martin Wrigley:** Are we falling into the trap of one size fits all in terms



of process? To buy a highly defined, precise transactional processing system is quite different from, say, a user interface app on a phone—for example, an NHS app versus an electronic patient record—and we should be using different procurement for different styles of systems.

Nick Davies: I think this comes down to the capability and capacity point. If you want Government bodies to be engaging early with the market, to be iteratively refining specifications throughout a procurement process and you want them to be working with a much wider range of smaller suppliers, they need to take more time and have more capacity to do that.

Q234 **Adam Thompson:** I want to come back to the Government Digital Service that we talked about a little while ago and look specifically at the responsibilities and opinions on how those have changed. Jason, do you think it was the right decision to transfer GDS out of the Cabinet Office and give it the new procurement responsibilities that it has?

Jason Liggins: Yes, I think so. Before that, responsibility was split between the Cabinet Office, DSIT and HMT. Personally, I do not think it has gone quite far enough. The Cabinet Office is more than just a supplier; it is also a different way of doing procurements. It was done to centralise procurement so there was one procuring body. The important part of it was to stop every organisation being a buyer and make them a consumer of a service. That was done by centralising the specification and that enabled an economy of scale that not even a group of Departments could achieve as a result.

I would encourage Government—DSIT—to adopt that kind of model for digital procurement more widely, because it would enable greater economy of scale to procure. That is not only a benefit to the public sector; it is a benefit to suppliers because they can then deliver less fragmented solutions and apply economy of scale to what they provide as well. I think that is to the public good. I also think that what was missing from the movement was the ability of DSIT to do and deliver rather than just write policy and guidance. I would encourage Government to consider giving DSIT the authority to deliver digital on behalf of the whole of the public sector and making the digital community consumers rather than buyers, because they all buy different things and that divides and conquers.

Adam Thompson: That is really interesting. There are a couple of tangible steps there that the Government could take moving forward.

Q235 **Chair:** When you say “give them the authority”, what is that? Give them the budget?

Jason Liggins: Just for my benefit, how would you accelerate Crown Hosting? That is at the top of my mind. The only way Government could accelerate more than we can do ourselves, which is to supply the Government market and get customers, is for a team within the central authority to go out and find the assets, the IT, that would move to Crown



HOUSE OF COMMONS

Hosting and move it, and take over responsibility to do that, because if you leave it to individual Departments it will fall to the bottom of their to-do piles. It is not something they are incentivised to do, or are even interested in doing, so it needs somebody to take charge and own that problem.

Q236 Adam Thompson: In the current instance, do you think the GDS as it is set up at the moment has the capability to deliver on what it has been tasked to do?

Jason Liggins: I think that the expertise is right across Government. I think it has a challenge in how to tap into that expertise because there are not very many people organisationally. How do they even get across all the different problems that Government has a whole?

As to the procurement part of it, has it moved to DSIT—question? I put that as a challenge to you as the Committee to ask. Has it actually happened? Is it still the Cabinet Office, or are they still arguing about it?

Nick Davies: On that, the commercial innovation hub that has been set up within DSIT is a multidisciplinary unit that includes people from the Government Commercial Function, as well as innovation specialists from the wider public sector innovation space. That seems to have quite a good mix of people, as I understand it. They are helping with some of the wider procurement issues around the digital centre of Government, but it is still quite a small unit. For example, I do not know what its resourcing looks like going forward, because I think business planning is still under way following the spending review.

Q237 Adam Thompson: Jason, you have raised an interesting point about whether it has moved or not and what is going on. Maybe there is a slight lack of clarity in the system at the moment. How do you think the various Government Departments—DSIT, Cabinet Office and GDS—can work together to make these things a little clearer and improve the system?

Jason Liggins: I come from a private sector background and I believe in meritocracy and democracy, but it does not achieve things quickly. You need a more direct way of doing things. This is where sponsors, and that includes you in this, have a good responsibility to ensure things happen, keep following it through and celebrate successes. As for DWP, none of you has heard of that. That is a resounding success because, if you had heard of it, it would have meant it had gone wrong; things would not have worked and it would have been headline news in the newspapers. We are completely silent about it.

Q238 Chair: I am struck by the question of capacity within the public sector for digital transformation and capacity within central Government, but more generally. We have a note here that £26 billion was spent in the public sector on digital data in 2023, but only 20% of it was spent with permanent public sector staff. Therefore, 80% of it was spent with contractors, managed service providers and IT consultants. Nick Davies,



HOUSE OF COMMONS

how can we build the skills in the public sector if we are not spending the money within the public sector?

Nick Davies: There is often a reasonable case for outsourcing; you cannot expect the Government to be an expert in everything. There are external providers who have specialist expertise and experience, and it is cheaper to buy that in than to develop it in-house. Clearly, there is a role, but the question is: what is the right balance? Should it be 20:80, or should it be closer to 50:50, or flipped?

Ultimately, as with so much of this, it is a question of political prioritisation. There has to be a deliberate decision to build up that headcount and also to offer sufficiently competitive salaries and overall packages for the people you are looking to bring into those posts. It is one of the ways in which the Government Commercial Function has been able to bring in more people from the private sector as they have been given some flexibility over their overall packages, which has helped. There is potentially a role for doing that more around digital as well.

Q239 **Chair:** Would you agree that the 20:80 balance is not what we should be aiming for?

Nick Davies: I think it depends on who those 20 are and what they are doing. Overall, about a third of Government expenditure is accounted for by procurement, so if 80% in this case is procurement clearly that is quite a way off what the general balance is across Government, so it would suggest that reducing that and upskilling internally would potentially be the better route forward.

Q240 **Chair:** We have talked a lot about public efficiencies. Can technology and AI in particular deliver the savings to the public sector that the Government have started, as stated in the State of Digital Government Review and the spending review?

Nick Davies: There are two different sets of figures there. The State of Digital Government Review gave the figure of £45 billion. However, it did not provide any breakdown about how that £45 billion was calculated. The only reference in that paragraph is to a House of Lords briefing, which cites the ONS as saying that public sector productivity has fallen, which is true; it did fall as a result of the pandemic, but it is not a meaningful way to create a £45 billion figure.

The other point about that figure is that it talks about savings and efficiencies. If by savings we mean cashable reductions in spending, that is quite difficult. The £45 billion is a huge amount given that most of what Government is spending on is either salaries or infrastructure investments. Unless you have serious plans to make pretty meaningful headcount reductions, or reduce capital expenditure, it will be very difficult to achieve that £45 billion.

If you are talking about productivity improvements, i.e. improvements of service to the value of £45 billion that could be delivered with existing



HOUSE OF COMMONS

spending, that is more achievable. There is certainly inefficiency and duplicative spending across the public sector that you could spend more effectively, but without knowing more about where that £45 billion comes from it is harder to say.

The figures that the Government included in the two-page efficiency plans published for each Department at the spending review total approximately £8 billion or £9 billion in efficiency savings, which is a much more reasonable figure. About three quarters of those departmental plans mention AI in one way or another. While we think it is a good innovation to publish those plans, it is great that the Government have committed to renewing them every two years. It is also great that in response to a PAC recommendation the Government have said that individual Departments will report annually on their progress against their efficiency targets. But, again, the problem is the vagueness of those plans; it does not really give any detail about individual initiatives and the savings or efficiencies that are expected from each of those.

For example, the plans of the Department of Health and Social Care talk about increasing retention and reducing staff sickness, which I agree would be a good way of improving productivity, but it does not give any indication about how it will actually achieve that.

Q241 Chair: The Committee sought further clarification from DSIT about this £45 billion figure, and one of the things that it said to us is that the methodology was based on the assumption that 100% of routine tasks could be automated. Would you agree with that? Yes or no?

Nick Davies: I do not know what a routine task is. I do not know if the Government know what a routine task is either. Clearly, there are some potential, big, long-term benefits that could be delivered by technology. My fear is that a lot of the AI tools are at a pretty early stage. They have not been scaled up and are often dependent on having high-quality data and data architecture, which in many cases we do not have.

Chair: Yes, as we know.

Nick Davies: From my experience, as I am sure from yours speaking to people working in public services, often the biggest efficiencies could be gained from much simpler things like making sure the wi-fi worked or giving them a new laptop that did not take 30 minutes to turn on in the morning. There are definitely some big productivity improvements from technology and eventually from AI, but in the short term I do not think that is where the lowest-hanging fruit is.

Chair: Having spent three hours on LNER trying to do some productive work yesterday on the way from Newcastle to Westminster, I can certainly say that working wi-fi is definitely a low-hanging fruit across the country.

Thank you very much to both of you for your contribution. It has been

very insightful, and we look forward to working with you in the future as well. Thank you very much.

Examination of witnesses

Witnesses: Gaia Marcus and Jeni Tennison.

Chair: Welcome to the second panel in today's session on the digital centre of Government. I will ask our two panellists to introduce themselves in response to the first question. I welcome them and thank them for their contribution this morning. Our first question will be posed by Lauren.

Q242 **Dr Sullivan:** Lovely, thank you, Chair. Welcome to today's proceedings. This timing is quite interesting given the recent announcements. As a local MP, I have had many people getting in touch with me about the digital ID and the change that it will be mandatory. Those people have been concerned about who is managing the database, whether it will be Government or outsourced, and the safety and security of people's details, among other things. Do you think digital ID should be mandatory?

Gaia Marcus: Hi, I am Gaia Marcus. I am director of the Ada Lovelace Institute. My colleague, Jeni, will have a lot more comments on the different nature of what digital ID might be. When we talk about digital ID, it is important to disaggregate the different models that we might have. Personally, I want to step back from giving an opinion as to whether it should be mandatory. I can share the research that the Ada Lovelace Institute has done.

We have not conducted specific research on digital ID. However, we can draw quite a few lessons about public trust in technology that has either tracking or monitoring capabilities from our work on general public attitudes to research, especially to AI, on biometrics and vaccine passports during covid. I also draw on some of the findings from the previous Administration's public dialogue on digital ID, which will be very useful for the work of the Committee.

In terms of public attitudes to technology, we know that the attitudes to AI will shift depending on four key things. The first is the purpose of the technology. In our data, it is no surprise that there are very different attitudes to AI that is used, for example, for assessing cancer risk from AI used for loan repayment risk. How digital ID is presented and the reasons that we are giving for digital ID will be important in terms of public attitudes.

To answer your question, there is a very big difference in trust depending on who the deployer is. Is something seen as being deployed in the public interest by a public body? Is it being deployed by the public sector? When it comes to people's personal data, they will have very different views on profit motive where that data are being used, around the risk driven by



HOUSE OF COMMONS

large multinational corporations being linked to that risk because it opens up attack horizons, and whether people who have control are private or public sector.

We also see that demographics will play a large part. In our general polling, we see that Asian and black British people are far more likely to be concerned about facial recognition. In our qualitative research, we see that your prior interactions with the state will very much colour and change your assumptions about how technology will be used, either for you or against you, and we will see that playing out in the digital identity debates.

Finally, you will see a divergence in public attitude and trust depending on how the scheme is implemented, for which functions, for whom, and whether it is seen as working for everyone equally. What we see from covid-19 technologies, and these are important—I was in Government at the time—is that, for data use, covid-19 was given as the high watermark of data use. If people were nervous about data or digital use in covid, that tells us a lot about how they will feel outside the pandemic. Adequate regulation is not going to be sufficient for there to be public trust.

During covid, we saw that public trust very much fluctuated in the use of technologies for covid-19, and that has an onward impact on public legitimacy, despite the fact that the UK probably had some of the best regulations and oversight mechanisms for these technologies.

We see that trust in these technologies will vary significantly by demographic background, with black, Asian and minority ethnic individuals far more concerned about how their data will be used, and consequently far less likely to use these tools.

We also see that traditional digital barriers meant that some people were not able to use contact tracing apps. If there is a roll-out of digital identity, especially where it is mandatory, we need to make sure that reliance on digital ID will not create similar exclusions—for example, when it comes to right to work. We saw consistently during covid and in other work that the public are very nervous about anything that is felt as driving a two-tier society and any sort of scope creep. It is incredibly important that any digital identification system or other public technologies are privacy enhancing by default and are set up to be right respecting by default, because once you have infrastructure such as digital identity, scope creep becomes a minimal cost. There should be something there about how we bring the public with us.

Finally, I draw your attention to some of the findings on the public deliberation that was done on digital identity services by the previous Administration. It was a very rigorous piece of work. One of our associate directors was on the oversight panel. We saw that 96 members of the public, when taken through a dialogue and deliberation on digital identity, came to see the ability to identify yourself as a human right. People start



from a point of convenience and come to the point of saying, "Is this something that's helping to build the kind of society that I want to be in?"

We see that they, therefore, do not see convenience on its own as a compelling reason to do it. They want to be sure that any identity verification is not digital by default and that it is always possible to use paper documents, which is relevant to the current dialogue on right to work. They were keen to ensure that biometric technologies were only used if they could be assured as being non-discriminatory and unbiased, and they were worried about the potential trade-off between convenience and the exposure to identity theft.

There is a lot there. I will pause. It is a really rich dialogue that is worth looking at in this context.

Q243 **Dr Sullivan:** Your thinking is incredibly deep. Is that published anywhere?

Gaia Marcus: This is a public dialogue that was published by the previous Administration. We can share it with the Committee. It was published by Sciencewise.

Q244 **Dr Sullivan:** That is great, thank you. Could I ask the same question to you then, Jeni?

Jeni Tennison: Sure, thank you. I am Jeni Tennison. I am the founder and executive director of an organisation called Connected by Data, which campaigns for communities—that is the people who are affected by technology—to have a powerful say over those technologies. Before that, I led the Open Data Institute, and before that I was a developer and worked on legislation.gov.uk, among other things. That is my background.

I am not an expert on digital ID at all, so I am going to pull together some things that are based on what I have read more recently around it. One thing I have observed is that, when people talk about digital ID, it is about a range of different kinds of things, and getting specific about what we are talking about is essential for working out what we want to do. There is the GOV.UK Wallet. There is One Login. There are the private sector digital verification services that are enabled by the data Bill. There are the international examples of the Estonia X-Road and Indian Aadhaar. The EU wallet is being developed at the moment. Some people use digital ID just to talk about having a single identifier that is used across databases within public services.

People are talking about very different things, and the design of those systems can be very different. You can have fully decentralised kinds of approaches and stuff that is a lot more centralised. Each design enables different things and has different kinds of risk associated with it.

I looked at the BritCard proposals from Labour Together and that particular paper, which was for a mandatory ID. A couple of things really



HOUSE OF COMMONS

leapt out to me about that. First, an essential feature of how it would work for immigration checks was that there would be a record of every check that was done so that the Home Office could tell whether a particular employer or landlord was doing the checks that they needed to do and that they are legally obliged to do over their workforce or over the people to whom they are renting.

Having that centralised record of what checks are done by whom in what places is of particular risk, because that can reveal a lot about our lives and how we go through our lives, especially when you get the kind of scope creep that Gaia talked about, where you have to have those checks every time you verify your age, you open a bank account, you enter particular places perhaps and you vote. That is one of the places it talks about.

If you imagine that record of those occurrences, that is a very rich dataset that could be used to target people. If I was in your position and I was scrutinising this, the question about what gets recorded behind the scenes, about the checks themselves, who has access to that data and the governance around it—those kinds of things—would be the area that I would be looking at in particular.

The other aspect that I thought was interesting in the Labour Together report was that it talked about the need to bring the public along to design this carefully, to not just say, “We’re going to do it,” and then have a fallout, but to do the work, to lay the groundwork. They also had some public attitudes research within it that showed that 40% of people were concerned about future Government misuse, which is the scope creep issue. There is that piece about how to make sure that the scope is curtailed and have some good protections around that.

To support what Gaia says, when we do polling about digital ID, we are likely to get a different kind of result from when we talk to people and expose them to some of the broader kinds of risks that there might be. As Gaia said, some particular groups are not supportive, and it is worth looking into why they are not supportive and what they are afraid of so that we can design a system that works for everybody.

Those are the two things that I would encourage the Committee to dig into a little bit more: the actual design, how much of it is centralised and who gets access to that data and the governance around that, but it is also about how the range of people who will be affected by digital ID, and in particular those who are most concerned about it, are able to shape what that digital ID looks like and how it works.

Q245 Dr Sullivan: That is again a very nice, rich answer. Thank you very much for your expertise in this.

I suppose different bits of our society are at different stages in thinking about this. Even in this room, there are very differing ideas about this. One thing that has struck me is the potential digital exclusion—so, people



HOUSE OF COMMONS

who are already digitally excluded, those who may be older and who do not want to have a smartphone. We have an ageing population in that sense who perhaps do not want to do this and are excluded. Could the idea of having a paper copy or something else and not being discriminated by the services be designed into a new system?

Jeni Tennison: I definitely think that that can be designed into a new system. There are examples of that kind of digitally enabled ID that is not necessarily digital on your phone ID out there in the world. The thing that I would look at there is whether there is discrimination against the people who are using those paper copies. My analogy is that I did not let my child have their fingerprints taken for access to the library or to the canteen in school, so they had to type in a code every time, and that gave them an extra barrier. As to the people who are excluded, are they excluded more because they are in the special circumstances kind of area? That is the bit that I would dig into a little on that.

Q246 **Dr Sullivan:** Great, thank you. I will do some digging. Gaia, do you want to say anything on that?

Gaia Marcus: Specifically on the paper, no; I think that has been really well answered. The only thing to look at as well is around data assurance. Whether this is digital or a paper QR code or similar, the public will still have real questions about risk minimisation, any redress were that data breached, and, from the earlier work, real control over their data access.

Dr Sullivan: That is great, thank you. I will leave it there.

Q247 **Chair:** Thank you. I have a couple of follow-up questions. Gaia Marcus, you talked about the public having more trust in public sector digital ID than in the private sector. One thing that is often said to us and to others is that Tesco's Clubcard knows exactly what you are buying. You have Facebook. The public shares its data with private sector companies on an enormous scale. Why do you think that digital ID specifically is something that they want to see done by the public sector, not by the private sector, and are you overestimating people's reluctance to share their data?

Gaia Marcus: That is a really good question. First, on the difference between public sector and private sector, that data specifically pertains to the use of AI by the public sector and the private sector, not digital ID. We do not have our own polling on digital ID. As to public attitudes to public sector use of technology, AI to digital ID, we see that the public hold the public sector to a higher account because they do not have the ability to opt out. That is the fundamental question. If Tesco had an enormous data breach, I could decide to take my data away from the Clubcard system and maybe shop around. I do not have that luxury if there is public provision.

Q248 **Chair:** Thank you very much. Jeni, I was going to ask you this, given your experience in digital development and your observations about public sector digital capability. You also heard the last session. Do you think that the state has the capacity to deliver digital ID safely by the



summer of 2029? Can you answer that yes or no?

Jeni Tennison: Honestly, I don't know. I could not answer that yes or no, again, because I do not think that it has been specified exactly what we mean by digital ID for this purpose. I also point the Committee to the work that has been done by Rachel Coldicutt on surveying the attitudes. She digs into that a little bit more. One piece there is that it also matters who is doing it in the public sector. There is different trust for the Home Office, for example, than there is for other public bodies. That will also make a difference.

Q249 **Kit Malthouse:** I want to ask some questions about the interaction with the private sector and the large databases it holds. With digital ID, if Tesco said when you want to open a Clubcard, "We're going to bypass all this by just having your digital ID to prove who you are," you then start to get a linkage between those two databases that could be usable in both directions.

Tesco might come to a position where it says, "Well, yes, Government, we will provide you with the data because that is very useful from a public health point of view, but in return we'd quite like some data from you about behavioural stuff." The second thing is that, if it is all phone related, it also has location data available for linkage to me, so the Government will be able to tell, broadly, if they want to have that deal with Apple or Samsung, where I am as well as who I am.

Does this feel like the natural progression? Often these things start with, "Well, it's actually all just about you proving who you are and it's just an easy way to do it," but, as the Chair said, when those big lumps of private sector data start to be linked through the initial verification process to be part of it, you get a huge behavioural picture of every individual.

Gaia Marcus: This really points to the importance of ensuring that any system is privacy and rights protecting by default. There is a distinction between what is technically feasible, what is built and then how there is purpose limitation. Having worked on Government data for quite a long time as head of national data strategy and in other roles, there are real problems at the moment with linking Government datasets. That would not be my initial worry because a lot of that work is not happening in practice.

However, you are right. How you build it—whether it is centralised, decentralised, public or third party—will drive how easy it is for that mission creep to occur. All our evidence tells us that what the public would like is clarity on who has that data access and control as to whether that happens, clarity that there is the involvement of the most marginalised in setting up the parameters for that, ensuring that this works for everyone and you have risk minimisation. We need to ensure that these things are done technically. I know you have done a lot more thinking about this. These are just questions at this point for us, are they not?



HOUSE OF COMMONS

Jeni Tennison: Yes, I agree with what you said there. It is worth looking at other places where they have rolled out digital ID systems and there has been scope creep. That has just happened over time. Because it is easy to do, it becomes something that gets done. There are particular protections in data protection law against just sharing data back and forth between the public sector and the private sector, but those were reduced a little bit in the data Bill. It is an area to be vigilant about rather than something to panic about immediately.

Q250 **Kit Malthouse:** We learnt from these technologies that mission creep is basically inevitable. We have learnt it in the private sector but also in the public sector. Could you see a situation in the future where, with life insurance for example, I have to give life insurers access to or declarations about my medical records? If there is a single identifiable ID for me, they could also ask Tesco if what I say is true, because I buy great vats of mayonnaise every weekend. Do you see what I mean? I might say that I am a member of a gym, but my location data says that I never actually go to the gym, and suddenly all that data, effectively, allows large-scale discrimination. Is that inevitable?

Jeni Tennison: I think it is a concern. I am not sure it is inevitable. That kind of picture we need to hold up as something we want to avoid. We need to test the protections that are put around the digital ID system, whatever it looks like, the governance that is put around it, who gets to make decisions about what data flows to what places and who gets access to it.

Q251 **Kit Malthouse:** The trouble is that the private sector makes it conditional on participation. Insurance companies will say, "If you want all that protection that's fine, but if you want my product you have to allow us to have this data." For example, I have digital scales at home. I do not think it will be long before an insurance company says, "Well, actually, you need to give us the log-ins to your digital scales so that we can see you're weighing yourself every morning, or whatever it might be, and we can see that your weight is fluctuating." This kind of micromanagement might get there. I know you are shaking your head, Emily, but where is the inevitable endpoint?

Emily Darlington: I had that image of you on scales. I am shaking my head to get it out.

Kit Malthouse: It is true. We do. There is our digital blood pressure. Real-time health monitoring by the insurance industry could be round the corner.

Gaia Marcus: This is where the importance of regulation comes in. You cannot coerce access to special category data such as health data currently, and we have to ensure that the regulation is there.

Chair: Kit makes an important point in terms of testing the boundaries of potential mission creep. It is worth saying that, yesterday, the Secretary



HOUSE OF COMMONS

of State said, first, that the architecture would be federated, so it would not be a single database, and, secondly, that individuals would be able to know when their data had been accessed. He did not give commitments with regard to the metadata of knowing who had asked or how it had been transferred, and this raises an important point that we should follow up on and continue to hold to scrutiny.

Kit Malthouse: I buy all that. It is just the question of private sector conditionality: "That's fine, but if you want my product you're going to have to give me access to all this data," which is what we get with social media platforms already.

Chair: The state can put limitations on private sector conditionality, and has done. We should move on now to Emily, who I know has something to ask and to say on this subject.

Q252 **Emily Darlington:** I do. This is where you will start to see the difference in views. Obama was famous for putting that conditionality on to health insurance, of course, and what you were able to ask and what you were able to disallow insurance for. It is always right to push the boundaries so that we know where we do not want to be as well as where we do want to be. Also, your point about location services is quite important. I do not think there is any suggestion that the Government are looking to track location through a digital ID in the way that some people on social media have.

I want to talk about the relationship between the citizen and the state, and the inequity in that relationship at the moment. Looking at Estonia, the purpose for the digital ID was to flip that relationship to make sure that the power was in the citizen's hands rather than the state's hands. The Government hold a huge amount of data on each of us. I use this example because it is the one that I am most familiar with most recently. Both of my in-laws, who were retired, were given terminal cancer diagnoses. We have lost them both. This is not an unusual situation. They get a terminal cancer diagnosis and, instead of worrying about their health, they now worry about informing 500 other Government agencies and Departments. It is quite paper-intensive and quite ridiculous that you have to prove and repeat your story about your terminal cancer diagnosis.

I know that this is also a frustration for my constituents. Often, I am in the position where we have cases from DWP, the same Department. My constituents are now being fined and they are saying, "But you know, because all my benefits come from the same Department." DWP say, "No, you didn't tell us."

Do you see a role for digital ID in dealing with the frustration that citizens currently have in negotiating particularly among the public sector Departments? Could Estonia show us some of the advantages to that kind of approach?



Jeni Tennison: In the conversations about digital ID, we tend to project our view of what would fix our particular problem on to what the design of digital ID would be. Certainly, linking up data behind the scenes so that there are easier flows between public bodies, so that you do not have to repeat yourself and you can more easily move between public services, is a goal for a lot of people.

Types of designs of digital ID like the One Login system that is currently being developed can help facilitate that. The kind of design that I talked about in terms of having a single identifier behind the scenes in order to link records together is the kind of design that will facilitate that kind of flow, but that is quite different from checking the right to work kind of digital ID. So, yes, those kinds of steps can be taken, and, yes, different forms of digital ID can help with some of those kinds of barriers and challenges, but other forms of digital ID will not do anything to help them.

Q253 **Emily Darlington:** That is important. You are absolutely right; digital ID means many different things. In some ways, we need to start with the problems and then figure out the solution to the problems that we are trying to address.

I also wanted to raise fraud. We see a huge amount of fraud. It costs the economy about £12 billion per annum. About £2 billion of that is identity theft, because it is quite easy to steal someone's NI number. I do not even know where my plastic card is, but it is somewhere. Literally anybody could hold it up and pretend to be me. Do you see a role for digital ID in combating fraud? If you took it further into public sector fraud—let us say DWP fraud or HMRC and tax fraud, because most of the fraud is perpetrated against public services—there is the data within the public sector that would catch that fraud quickly.

Jeni Tennison: Again, depending on the design of the digital ID, certainly that can be a goal. You can get different kinds of verification through a digital ID as opposed to, as you say, a card or something like that, which can be easily stolen or of which a fraudulent copy can be made. There are different kinds of security characteristics for those things. That is distinct from the detection of fraud automatically behind the scenes by doing lots of clever big data and AI analytics to identify people who might be committing fraud from a DWP or HMRC perspective, and I do not think we should muddle up those two things too much.

Q254 **Emily Darlington:** At the moment, we are asked to prove our identities quite often. It may be to vote. There is a significant equity issue there because you need a passport, which is expensive and you don't get one if you don't travel, or a driver's licence, which is also expensive and difficult to get at the moment if you are trying to book a test. Currently, there is not a free form of ID that the Government accept as a proof of who you are for voting.

Martin Wrigley: Voter authenticity certificate, which you can get.



HOUSE OF COMMONS

Emily Darlington: Yes, but you know how much ID you have to bring to prove who you are and the amount of paperwork in order to have a voter authenticity certificate. I am sure, as MPs, we have all tried to support people to get those. Again, it is a huge barrier.

Martin Wrigley: It was easy to get mine.

Emily Darlington: Okay, it was easy to get yours. Other than Martin, there are things that we are being asked to prove. The voter issue is one of them. Also, one of the big criticisms of the Online Safety Act and the age restriction was not necessarily the age restrictions, certainly when I dug into it. It was the fact that they were giving their data to third-party verifiers and did not have confidence in that, whereas a digital ID that is free and confirmed by Government would allow people to access age-appropriate things online without giving away their data to third-party verifiers or increase the ability for people to be verified to vote and making that more equitable, especially for those people who cannot afford the current forms of acceptable ID.

Gaia Marcus: It is really important to disaggregate between proven links between these things and dialogue on them. First, to your earlier point, I am really sorry for your loss. I was in Government from 2018 to 2023. There was an ambition to have a Tell Us Once service, which was there to solve that problem.

Q255 **Emily Darlington:** It doesn't work.

Gaia Marcus: It doesn't work. There are various technical initiatives trying to do different things, and we need to ensure that we point at the right ones. There is an assumption that digital ID might reduce irregular work. You have national identity systems in places like France and Italy that have far higher problems with irregular work than the UK does. As ever, there is ensuring that a named thing is not posited as a solution where it is not the cause of the problem.

It is the same thing with voter ID. Views vary as to whether voter ID leads to reduced voter fraud. Anything that is onerous in terms of having to prove your identity will not necessarily be solved by having that identity digitised. There were a lot of attempts in Government to have different ways of verifying, such as Verify. When we think about online safety, other mechanisms allow you to prove your age without having to send your passport to a third-party provider—for example, attribute exchange. This goes back to Jeni's point. The question is how we do this technically. Something like attribute exchange, which would not need necessarily a digital ID, is a privacy-enhancing way of checking if someone is over 18 without sharing information about who they are.

Q256 **Emily Darlington:** But that is based on analysing what they are looking at and what they are doing. I think that is quite invasive.

Gaia Marcus: With attribute exchange, it would be like a ping to your bank. It has been a while since I have had a look at the technical detail,



HOUSE OF COMMONS

but it is that question of what requires us to prove our identity and what requires a system to ask a trusted third party to verify an element of it, which is just a privacy-enhancing way of doing it.

Q257 **Emily Darlington:** Yes, and it is not precluded that that would not be involved in a digital ID as well, is it?

Gaia Marcus: No.

Q258 **Chair:** Thank you very much, Emily. Moving away from digital ID, which I know is incredibly topical at the moment, data and technology transformation is a perennial and ongoing issue. Do headlines about mass breaches of data held by the MOD on Afghan nationals undermine public trust? Gaia, perhaps you could answer that.

Gaia Marcus: Anything that suggests that your information is not secure will undermine public trust in that use. The question is less about the headlines and more about what is happening on the ground, and whether the systems that we are using are trustworthy.

Q259 **Chair:** You say that the question is more about the systems. Certainly, this Committee is interested in the systems and is investigating that, but that is not the consequence. Trust is not necessarily based on evidence but on perception. I suppose the question is whether those headlines undermine public trust regardless of the underlying system security.

Gaia Marcus: I do not particularly have a view on the headlines themselves. The question for me is: are public bodies incentivised to comply with GDPR, and therefore what is the onward impact on public legitimacy?

Q260 **Chair:** You are interested in the substance rather than the debate about it. Jeni Tennison, would you agree?

Jeni Tennison: If you look at what influences trust—some quite good work was done by the Centre for Data Ethics and Innovation, as was, around digging into the mechanisms behind trust—the two fundamental bits are whether we believe that the Government are competent and that the Government are well intentioned. Headlines about data breaches undermine the first of those. Do we think the Government are competent? Are they going to hold our data securely? Are they going to be able to do what they say they are going to do? We also have concerns about intent, which is why we might see some of those discrepancies. How people feel about the Home Office using data for particular groups is different from how they feel about the NHS using that data.

Chair: That is helpful. Competence and intent: we need to get both of those right. That leads nicely into Adam's question.

Q261 **Adam Thompson:** Yes, thank you very much, Chair. Good morning, both; thank you for joining us. Jeni, you have said previously that the Government need to address the real challenges in tech adoption across the public sector. Since you said that, a bit of time has passed. Could you



elaborate? What are these challenges? Do you think the Government are doing that work?

Jeni Tennison: The pieces that I care about around adoption are coming from the work that we have done with real people talking about how they feel about technology. One thing that we observe is that when people feel out of control of technology they tend to resist it rather than embrace it with open arms. If we want to have good adoption of technology—that goes for citizens using particular apps on their phone as well as public sector workers behind the scenes—we need to make sure that they feel they have had some say over that technology. It makes the technology better because it means it is suited to the actual task that they have to fulfil. Also, that feeling of control means they are more likely to embrace it.

Do I think that the Government are currently doing the work to get that kind of embracing? I do not, currently. There are pockets within the public sector that do good engagement work with the people who will need to adopt those technologies—good deliberative engagement work, not just doing a poll, but talking through and involving them in things like shaping evaluations or shaping the actual technology. There are pockets where that is happening, but it is not happening everywhere.

Q262 **Chair:** Can you give examples of the pockets?

Jeni Tennison: Yes. The Department for Education has been doing some good public deliberation work on the use of AI in schools. The Home Office has been doing some good public deliberation on police use of AI. Of course, there has been a lot of investment by the NHS and DHSC in public engagement in the health service, although not to the kind of nitty-gritty that I would really like to see. It needs to be a systemic way in which the organisations that are developing digital public services have the people who will be affected by them involved in shaping them.

A lot of what we see are very broad-brush questions about what makes you trust Government, when actually we need to get down into the specifics. For this technology, what kinds of protections do you think we need around it? What would help to build your trust around this? What particular concerns do you have about this specific proposal that we are putting forward so that we can mitigate those risks and address those concerns? Listening and demonstrating that you will be responsive to those kinds of concerns and that you will be able to adjust it towards what people need in their jobs and in their lives will be a lot better for adoption of that technology.

Q263 **Adam Thompson:** Thanks, Jeni. That is so constructive. Beyond that deliberative engagement that you have covered there, is there anything else that you think the Government should be doing as well to address those challenges?

Jeni Tennison: To address the challenges around adoption? I think it is recognising that the public are not just one public and that different



people need different things. Whenever we develop a system, I often think about the kinds of chatbots and systems that we use in order to access Government services like that. Different people need different things at different points in their lives and also in different levels of distress. Enabling people to have some control over which of the various mechanisms they use in order to access Government is another place where that will help get appropriate use where people really need it.

Q264 Adam Thompson: Fabulous, thank you. Gaia, we have seen quite a lot from the Government about the roll-out of AI and how it is going to solve all our problems, et cetera. Using your background and your understanding of the evidence underlying that, how convinced are you by both the evidence and the Government's rhetoric on this about the roll-out of AI and data-driven tools for use across the public sector?

Gaia Marcus: In terms of AI and data-driven tools, just solving all productivity and other issues, for example.

Chair: I think we got the answer.

Q265 Adam Thompson: Elaborate on that.

Gaia Marcus: We have been discussing evaluation quite a lot. I thought Nick's reflections were really helpful as well. When you think about what the use of AI will be or other data-driven technologies across the public sector, it is incredibly important that you are really clear on your theory of change. At the moment, we hear this idea that there will be time and productivity savings; efficacy and efficiency will somehow go up; and we are just not seeing that. That is not just evidence in terms of AI use in the public sector; that is evidence on AI use in the wider economy. There is a recent MIT study that suggests that only 5% of companies with integrated AI actually have any sort of revenue acceleration.

You see quite a thoughtful evaluation by the Department for Business and Trade on its six-month evaluation of Copilot. It is very varied in terms of tasks. It is better at some tasks. For other tasks, data analysis, using Excel and PowerPoint, actively made it worse. Even where it is able to find some time savings, it does not really find a relationship between time savings and productivity. Actually, it finds that a lot of the time savings are through self-report, and those tend to vary from observed time savings in their task. It has a part of the study where someone watches people doing tasks. There is really granular thought, but the evidence isn't really there at the moment.

When we look at the Government's evaluation of Copilot use across 20,000 civil servants across multiple Departments, the only measure that we see to justify claims of 20 minutes of time saving per day is self-report, which we know from other work is notoriously unreliable; it is just not very rigorous as a measure. We need to ensure that we have the right evidence and that we encourage the public sector writ large to share



HOUSE OF COMMONS

lessons that help adoption and scale rather than always having that time-saving metric, which I am always quite nervous about.

The Assist tool is a communications tool that has been rolled out across Government. Somewhere there is a stat, which I do not know the evidence for, of three hours being saved on average from the use of Assist. On the other hand, there is some really thoughtful work on how you evaluate products and how you look at barriers to deployment. We need to encourage colleagues who are really thinking quite sensibly about what this is. In terms of the general stats, I do not think there is any evidence for them. I worry that we are conflating many things. Shall I pause?

Adam Thompson: No, please carry on.

Gaia Marcus: We have work that looked at six years of data in AI use across the public sector and 30-odd reports. We find that we do not have enough granularity and specificity about what we mean when we say AI, and that is really inhibiting learning because we are comparing apples and oranges. Often, we are using use cases of narrow or very specific uses of AI or even old AI, pre-gen AI, to justify investment in gen AI where there is really no evidence there for the productivity savings.

We all have the scars on this. We cannot forget about the plumbing. You see a lot of pilots and a lot of uses of AI that are on top of the top of services, but they are not dealing with legacy IT debt, the kinds of problems that we raised earlier, and the fact that, as one of your colleagues said earlier, if the data are not fit for purpose you will not have the tools to do what you want them to do.

We really believe that, if the Government are serious about AI adoption across the public sector writ large, they need to think about what works centres, evaluations, and how we really share lessons such that we are going from below the headlines to helping people. A lot of people are doing a lot of very good work and they are trying to make these things work. I just think they need more structural support there.

Q266 **Adam Thompson:** Do you think it is still technically possible that we can achieve some of these lofty ambitions that the Government have set out, or are we just riding the highest point of the hype curve with AI and it is not capable?

Gaia Marcus: I just don't think we have the evidence at the moment.

Adam Thompson: Thank you, both. Thank you, Chair.

Chair: Thank you very much. We only have a few minutes left. This is very fascinating. There is a lot to bring in. I would like to go to Martin now.

Q267 **Martin Wrigley:** Thank you, Chair. Gaia Marcus, I think your organisation has argued about public procurement of AI. What needs to



change to fix the problems that you have seen there?

Gaia Marcus: That is a very good question. It is worth saying that most of our work on public procurement AI was done on local Government procurement of AI. We found that, even just from doing a very basic documentary analysis, guidance is mixed at best. A lot of definitions vary. People are trying to do good work but they are really not helped by the infrastructure around them. Although of course we now have the new Act, it does not actually talk about AI, so it does not necessarily help people who are seeking to do AI procurement. There is a real challenge around transparency in terms of the information that you get from vendors, knowledge asymmetries between the people trying to do procurement in local Government and the companies that they are interfacing with, and an insufficient focus on what almost like market shaping might be in terms of where Government puts its money will really shape what the market gives you.

When we looked at procurement in local Government, given these very nested problems around gaps and guidance, imbalance in power and knowledge, market failure with a very concentrated number of suppliers and real lack of clarity on what people were buying, quite unusually for Ada, we suggested that what you really needed was a taskforce to look at these problems in the round. We thought that a taskforce might help local Government by setting out clear aims for adoption across the many services that local Government provides, giving them one strategy and one way of learning lessons. Really think about how you address market failures through rebalancing power between suppliers and technology buyers through, for example, model contracts or better approaches to assurance and assessment. Really engage the public, especially those who are affected by the use of AI technologies and really understand their views. Finally, look at the regulatory context. In the absence of overall regulation, you have the risk that the liability is being pushed out to deployers of technologies. There is the real risk that you have the public sector paying the price for a lack of regulation upstream.

Q268 **Martin Wrigley:** That is very interesting. Thank you. Having come to this job from local Government, I saw one example of it being phenomenally useful, which was in analysing public comments on things like local plans. We had more and more comments from more and more people, and getting the summary of that was saving weeks and weeks, if not months and months, of officer summaries. It does, however, come up with one of the things that you just mentioned, which is the fundamental problem of AI being a non-deterministic system in that you do not get defined data, defined process and defined output. You talk about assessment, and clearly it is not possible to test such a system. Do you have ideas on how that assessment and testing, whatever takes over user acceptance testing of such a system, would go?

Gaia Marcus: There are a lot of methodologies for testing and assessing AI technologies. There is a lot of focus currently at the foundation model layer where there are many evaluation systems. We are really interested



in the evaluation systems to look at how they impact on people on the ground—the deployment layer. We are helping a local council in understanding how it might evaluate a transcription tool. We find that at the moment there is a real focus on time-saving studies. The Government have a lot of guidance on this. We are also interested in ensuring that there are sociotechnical ways of evaluating these tools. With this transcription tool, we found that there was an example of a hallucination—a fabricated fact, essentially—where this tool hallucinated or erroneously generated that one of the clients had had a suicidal intent episode. It is very hard when you evaluate a system to trade off general time savings with what the risk is with judicial review when that has gone quite so badly. I think it is so important that we evaluate it. This is forthcoming work that we can share.

Q269 Martin Wrigley: That comes back to this fundamental impossibility of testing it and predicting what its answer is going to be, because it will make it up. It is a probabilistic answer, not a deterministic answer. You cannot prove it.

Gaia Marcus: It is a really good point. We need to be really clear when different types of AI or data-driven technologies are appropriate for different use cases. There are ways of testing it. You can do one-shot evaluations where you ask the system the same question 1,000 times, but that may not be technically in the remit of a local council. You really hit the nail on the head; we need to be very clear when a generative system, as you say, is appropriate for the use case it has been given for. It might be that, in generating responses to queries from the public where there is somebody with the time and space to make sure that response is correct, it may be a good time saving. It might be that in a high-risk situation it will never be appropriate. The more work that we can do to be really clear on what those red lines are where a generative system will never be appropriate, the better for public trust.

Martin Wrigley: Thank you.

Chair: Thank you, that is very interesting. It takes us back to the points that were made in the earlier session about the public sector knowing what it is procuring, and that includes how to test what it is getting.

The Committee has found these two panels really illuminating. I am not sure that we have found them reassuring, but I really do want to thank you for your contributions and your presence here today.