GLA Oversight Committee – Thursday 14 September 2017
Transcript of Item 5 – Personal Data in the GLA Group

Len Duvall AM (Chair): Then can we move to item 5 and welcome our guests? We have Bob Farley, Head of Information Law and Security at the Metropolitan Police Service (MPS). Paul Wylie is Director of Strategy at the Mayor's Office for Policing and Crime (MOPAC). Elizabeth Denham is stuck in traffic - the Information Commissioner - and so we will do that introduction later. Javier Ruiz is Policy Director of Open Rights Group; Renate Samson is Chief Executive of Big Brother Watch; Richard Bevins is Head of Information Governance at Transport for London (TfL); and we have our own Tom Middleton, Head of Finance and Governance at the GLA.

Sian Berry AM: Thank you all for coming. We have sent out a questionnaire to each of the GLA organisations asking about your use of personal data in some detail and we have a report back on that in our briefing packs. As part of the meeting, can I can ask each of you in turn if you can outline not so much in detail what data you collect but in general what are the benefits of collecting it and what do you use it for to get benefits for Londoners?

Tom Middleton (Head of Finance and Governance, Greater London Authority): Thanks, Sian. Just briefly in that case because there are quite a few people to go around, the GLA's use of personal data, as you probably appreciate, is more limited than some of the other bodies just because of the nature of our functions. Traditionally we have not really had much held here. In recent years, we have had slightly more held here and some of the Members will be familiar with Talk London, which is for polling purposes. You will be familiar with Team London, which holds personal data relating to volunteering. We also have something called Housing Moves, which is a housing initiative with details of people's personal addresses and so forth. Therefore, it is relatively limited, but there are some areas, the main areas I have just described.

We only have one formal data-sharing agreement and that is with TfL and that is to do with volunteering, actually, and to do with over-18 Oyster card customer data to see if people are interested in volunteering. That relates to Team London. That is the only formal agreement we have in place and so --

Sian Berry AM: We will ask about data sharing next as a separate question.

Tom Middleton (Head of Finance and Governance, Greater London Authority): Fine. At the moment, it is fairly limited. Going forward, there may be slightly more in the same sorts of areas as I have talked about, but nowhere the scale of some of the others.

Sian Berry AM: TfL?

Richard Bevins (Head of Information Governance, Transport for London): Thank you for this opportunity. There was a lot of detail in our questionnaire response and so I will not repeat that but, as Tom [Middleton] intimates, in contrast to the GLA, TfL does collect and process and hold a lot of personal data: from the ticketing system, from Oyster and contactless. We have customer accounts in quite a number of areas of our operations like the cycle hire scheme. The congestion charging scheme depends on customer accounts and is managed through customer accounts with an associated amount of personal data. The dial-a-ride scheme: we have the personal data of the users of that scheme, which is quite sensitive personal data,

often, as well. We regulate the taxi and private hire trade, which involves data of drivers and applicants to be drivers. You will, I am sure, be familiar with the closed-circuit television (CCTV) network that we operate on the Tube and elsewhere, which is quite extensive. Of course, we are also quite a large employer and so we have a lot of employees' personal data as well.

We collect all of this so that we can run our services. The ticketing system depends on the use of personal data and then that provides -- TfL could not run without a ticketing system of some sort. The CCTV cameras provide security on the Tube and help us manage the infrastructure as well. The cameras that we have on the street help us to enforce the Congestion Charge and enforce other regulations on the roads that we manage. We see it all as being essential to the delivery of our services, in summary.

Sian Berry AM: Thank you very much. MOPAC, you are strictly our GLA body; you keep data for your own purposes as well, separately from the police?

Paul Wylie (Director of Strategy, Mayor's Office for Policing and Crime): To a limited extent. It will not surprise you. It is a very small organisation and so there is the human resources (HR) information of our own staff and to a limited extent, a bit like Tom [Middleton], there is survey data of people that we can send newsletters to and people who reply to us in terms of consultations, but it is largely limited to that.

Sian Berry AM: Can I just ask quickly? You also scrutinise the police?

Paul Wylie (Director of Strategy, Mayor's Office for Policing and Crime): Yes.

Sian Berry AM: Do you have an oversight role over their use of data in any sense?

Paul Wylie (Director of Strategy, Mayor's Office for Policing and Crime): We do and I can elaborate on that now or later but, yes, there is an oversight function of the MPS, which clearly has much more of the data.

Sian Berry AM: You would be the person responsible for that, the information governance scrutiny as well as the information governance within MOPAC?

Paul Wylie (Director of Strategy, Mayor's Office for Policing and Crime): That is right, yes.

Sian Berry AM: Thank you. We will have some more questions on that later. MPS?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): Good afternoon. Yes, we process large amounts of personal data. The purpose of that is the prevention and detection of crime, the apprehension of offenders, the prosecution of offenders and safeguarding. The major objective is obviously to record crime incidents, the victims, offenders and suspects at that level, and also incident information, 999 calls, major inquiries and intelligence information.

In addition, as with the others, we are a large body and there is also the HR information around our staff and officers.

Sian Berry AM: We will discuss more about that later on.

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): Sure.

Sian Berry AM: Can I ask why the MPS only completed our questionnaire up to question 7?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): We did not, to my knowledge. It was --

Sian Berry AM: Is that right?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): I have a record of what we submitted, but I understand Steve [Wright, Scrutiny Team Manager] asked for some additional information that clearly did not come through at some point, but it was completed in full.

Sian Berry AM: We will check that out. I want to move on to data sharing now and that is where the data sharing questions start within our questionnaire. We have been provided with a diagram based on the information that has been given back to us and, obviously, the MPS is not linked into many of these things in the way that we would have expected. There might be a lack of information about the data sharing that the MPS does or rather what is shared with the MPS.

Can I start with the GLA again and ask you what data you share both with other GLA organisations and also if you share any outside of the GLA?

Tom Middleton (Head of Finance and Governance, Greater London Authority): Yes. As I was saying earlier, we have only one formal arrangement and that is with TfL formally when people renew or first apply for Oyster cards. That is to encourage young people to volunteer through Team London, which is on the back of the 2012 [Olympic] Games. That is purely names and email addresses. It is very limited. It is important that we do not disclose it, but it is very limited personal data. As you know, it is on an opt-in basis, which I am sure we will touch on later. That is the only formal arrangement we have. We do not generally share outside of that.

Sian Berry AM: Can I ask you about the Combined Homelessness and Information Network (CHAIN) database? That is a GLA-monitored database. It is the link database that the various homelessness agencies use to share information about people who they are helping on or off the streets. There has been some concern lately that the data from that is being shared with the Home Office. That does not seem to be in your responses to us yet. Is that something that you oversee or is that something separate?

Tom Middleton (Head of Finance and Governance, Greater London Authority): I have never heard of the CHAIN database, to be honest with you.

Sian Berry AM: It is not a GLA one?

Tom Middleton (Head of Finance and Governance, Greater London Authority): If it is, I am not aware of it, but I will hopefully clarify that point --

Paul Wylie (Director of Strategy, Mayor's Office for Policing and Crime): If it is helpful, I am relatively new to MOPAC but before I was five years as Director of Immigration Enforcement for London in the Home Office. I can tell you that the CHAIN data is only shared at a macro level and not the specific individuals or anything like that.

Sian Berry AM: It is shared?

Paul Wylie (Director of Strategy, Mayor's Office for Policing and Crime): It is. I do not know who owns it, I am afraid.

Sian Berry AM: We will find that out later as well. TfL, your data sharing is quite extensive because you are more like a commercial operator, are you not, and so you have lots of different relationships. Can you run us quickly through those?

Richard Bevins (Head of Information Governance, Transport for London): Yes, to expand, if I can, on what was in our questionnaire response. We share data with quite a large number of other mainly public-sector bodies but not exclusively. As Tom says, we have an arrangement with the GLA and that is our only formal regular data sharing with other GLA bodies, if technically you exclude the MPS from being a part of the GLA Group. Other public bodies that do share personal data with would be the police forces, primarily the London police forces but not exclusively, with MPS being the main recipient there. There is a range of other public agencies, particularly if they have fraud detection or prevention responsibilities, and so we are sharing personal data with the Home Office in a limited capacity relating to applicants for taxi and private hire roles in order to check the entitlement to work in the United Kingdom (UK). We have other arrangements for fraud prevention with the Department for Work and Pensions (DWP). We receive requests from Her Majesty's Revenue and Customs (HMRC) and similarly, with the same purpose of fraud prevention, we also exchange personal data with commercial organisations, insurers, the motor insurance industry, particularly. We share with a range of organisations that play some part in our delivery of service. That is under data processing arrangements rather than data sharing and so that is done on an entirely different governance basis. I do not know if you want to explore that here now as well. That would be with companies who are providing a service for us rather than when we are sharing data for an organisation's own purposes. A classic example would be Serco or Capita running a Congestion Charge or the cycle hire scheme for us under contract, but personal data is involved in that process. They are some of the main organisations that we share data with.

Sian Berry AM: Just on that last point, when you outsource something like running the cycle hire scheme, you rely on the company's own data protection policies and or do we, as London, have any additional requirements that we impose upon them?

Richard Bevins (Head of Information Governance, Transport for London): TfL has its own bespoke set of requirements that we are very strict about imposing through contractual arrangements, which place obligations on the company to do what we tell them so that they control the personal data as we require them to do.

Sian Berry AM: There is essentially one policy at TfL level that then cascades?

Richard Bevins (Head of Information Governance, Transport for London): Yes, there is one policy and there is one standard set of contractual clauses that forms the basis for all of our contractual arrangements and that flows out across the whole range of services that we outsource.

Sian Berry AM: That is useful. MOPAC?

Paul Wylie (Director of Strategy, Mayor's Office for Policing and Crime): Yes. There are a few data-sharing arrangements but they are limited to the evaluation of pilots or programmes that have been commissioned by MOPAC. MOPAC has a commissioning arm that deals with things like the Crime Prevention Fund and certain bespoke issues like knife crime. In that respect, there will be a limited amount of personal data to evaluate whether or not those schemes were successful. As an example, Red Fred works in the National Health Service (NHS) and, in order to ensure that we know it is working or not, we are evaluating its

success and so there will be a limited amount of personal data, which was covered by the original commissioning in terms of contracts.

Sian Berry AM: That is very useful. Thank you. The police, do the data you hold and which you share with other people -- do you want to start with that?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): Yes. Like local authorities, it is a major area in terms of sharing and supporting the Crime and Disorder Act, like housing, domestic violence, antisocial behaviour. We also share information with the fire and ambulance service around safety issues, the health service in general, and also we receive a lot of information from the health service on safeguarding issues, a lot of other law enforcement bodies in addition to other forces and TfL in relation to crime on transport.

Sian Berry AM: Essentially, this is data that you collect in the course of your work that then raises issues that other public authorities need to be concerned with and you can pass that on?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): Yes, as part of our general partnership arrangements. It is very much a multiagency approach, say, in cases of mental health and those sorts of things and safeguarding vulnerable individuals, which can only be dealt with collectively with information from all relevant parties. Where it is, say, a domestic abuse type of incident, it may be police information that is the catalyst for reported incidents and it is multiagency in terms of coming up with a solution. Yes, there is generally a lot of sharing of information, but each agreement that we produce goes through a rigorous process to make sure it is consistent with the policing purpose and that that information is protected through that sharing process.

Sian Berry AM: I am a local councillor and so I do appreciate this whole safeguarding and multiagency type of approach. All of this is very sensitive information, though, and so you must have quite rigorous training in the sensitive nature of the information to the officers who have --

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): Yes. All our staff undergo basic training on entry and then that is reinforced through specific computer courses and that sort of thing. All staff are subject to our information management policy around the appropriate use of that information. We enforce that. It has to be for genuine policing duties.

Sian Berry AM: OK. Can I ask about information that you gather in from other places within the GLA? You already talked about CCTV at TfL and I believe there is an agreement there. Can you run us through what you collect in for policing purposes?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): Yes. The congestion charging information is one piece through the reads on cameras. Then it would be case-by-case information coming in through incident response, primarily.

Sian Berry AM: When you say the congestion charging, that is the number plates that are captured by the congestion charging system?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): That is it, yes.

Sian Berry AM: How long do you hang on to those for when you are given that?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): At the moment it is two years and we are currently under a national discussion around reducing that to one year. That is the reads of the vehicles passing through the camera, not the images.

Sian Berry AM: It is the data that results from the automatic number plate recognition (ANPR) not the images themselves. Has that changed in recent years, that agreement?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): The national agreement has been two years and recent discussions nationally, which the Information Commissioner's Office (ICO) staff have been involved in, are now considering reducing that to a two-year retention nationally[1].

Sian Berry AM: Can I ask about Oyster data? Sorry, if I can ask both of you the same question at once, TfL originally, when it first started the Oyster system, kept hold of the data on where you have travelled for a month.

Richard Bevins (Head of Information Governance, Transport for London): Eight weeks.

Sian Berry AM: Yes. The last time I logged into my card, it was giving me two months' worth of data. Do you know when that changed?

Richard Bevins (Head of Information Governance, Transport for London): It has always been eight weeks.

Sian Berry AM: That is odd. When I asked about it in 2005 it was definitely one month it was being kept for.

Richard Bevins (Head of Information Governance, Transport for London): Oyster was pretty much brand new in 2005 and so was I in TfL. My understanding is that it has always been eight weeks.

Sian Berry AM: Fair enough.

Richard Bevins (Head of Information Governance, Transport for London): Technically, it is destroyed or disaggregated from the individual in the ninth week.

Sian Berry AM: Do the police have access to that in the same way they do to ANPR?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): Only through an individual request basis using the Data Protection Act's exemptions. So, if there is a genuine individual that we are interested in and we believe that they travel on the Tube, then there would be a direct request through a data-sharing agreement, would it not?

Richard Bevins (Head of Information Governance, Transport for London): Yes.

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): Yes, and then that information would be retained relevant to that investigation requirement. If it was going through the courts, it would be retained as evidence if it was relevant.

[1] Clarification was provided by Bob Farley following the meeting that a 1 year rather than 2 year retention is being considered for this data.

Richard Bevins (Head of Information Governance, Transport for London): We have a process at our end to assess those requests as they come in from the MPS and make a decision on each one on an individual basis.

Sian Berry AM: Finally, to the police, there was a recent case reported where a victim of crime ended up being investigated by the Home Office and it seems like the police had passed on that information. Do you have an agreement with the Home Office to do that if you have suspicions about somebody's immigration status, even if they are a victim of crime?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): I am not aware of an agreement, but if we identified a crime had been committed and that was by an appropriate investigating body, then I would imagine that would be a disclosure we would make. I am not aware of the specifics of this case or a specific agreement being in place with the Home Office. I can certainly clarify that for you.

Sian Berry AM: It would be very useful to know if there were any kind of requirements because, if somebody comes forward and there is clear evidence that somebody has reported somebody and all of that, it is different than if somebody is merely a victim to actually go and investigate their immigration status. It seems odd. Those are all my questions about data sharing but we are moving on now to Big Brother Watch and Open Rights Group, who are campaigners in this area to keep a very close eye on data protection. Starting maybe with Big Brother Watch, can I ask you what are the key risks of having these GLA organisations collecting data and sharing it with each other? What might go wrong?

Renate Samson (Chief Executive, Big Brother Watch): I would argue that it is just a fundamental issue of data sharing full stop in that we have heard that data is increasing all the time. I go to great pains to try to express to society as a whole that we are now all digital citizens and that we are our data and that data is not just a supplementary part of our lives; it is fundamental to who we are in a connected age. Therefore, a historical approach towards data - as in a piece of paper and photocopying a piece of paper and handing it and sharing it - simply does not exist when you can transfer vast quantities of data, acquire, share, retain and vast quantities of data, which is often very personal data or sensitive data.

All organisations are at risk of just the way we live today in that they need or want to acquire data and share data to improve services and improve customer experience or even people's lives, but there is an inherent risk that as soon as you acquire a piece of data and share it, it is out of your control.

We certainly find with reports that we have undertaken about data breaches that human error is a natural problem. You cannot ever account for human error and there are ongoing problems with data breaches. Our last report from the summer of last year entitled *Safe in Police Hands?* about police data breaches showed that between 2011 and 2015 there were at least 2,315 data breaches undertaken by the police, ranging in severity. Just sharing a piece of information inaccurately is one thing; providing criminal gangs with information is quite another, but they are quite rare. We find similar issues of data breaches across the NHS and other public services, but that is the area that the Information Commissioner knows much more about than I do.

Fundamentally, we have to all be very aware now and I do not think we are as a society or as leaders or as businesses or organisations that our data is so fundamentally critical to who we are as people that it requires greater protection and a greater sense of absolute need rather than, "Would not it be helpful?", than we have probably experienced before.

Sian Berry AM: Can I ask how the public ought to be consulted about things as well? This is one of the things where, like I say, I am asking these questions because things have come up but way after when maybe you would expect to have been asked if this could happen.

Renate Samson (Chief Executive, Big Brother Watch): Yes, education is a really critical issue. I believe that the majority of us, if not all of us, are effectively blind to what our data is and the impact that our data can have. Almost our five senses are obscured and we rely solely on trust. For those of us over a certain age, if you used to ask me my name, my address and my date of birth, I would give it to you because I could see the obvious purpose for why you were asking for it. In a digital connected age, it is not always that obvious. Often, we are asked to provide very personal data for no actual purpose, just purely because an organisation thinks that there is some value in it, but we cannot necessarily see the value ourselves.

We all have to learn what it means to be a digital citizen. That I believe will start to sink in more with us as we become victims of crime in relation to our data. With the Equifax breach that occurred at the end of last week, at the point when we find out if any British citizens have been involved in that, when we discover the eight years of very sensitive financial data that is held on us by credit reference agencies such as Equifax, a lot of people will not know what to do in order to seek redress for the sheer volume of data that has been lost on them. It is 143 American citizens who have lost very sensitive data. At the point that you find that you lose your identity or that you are vulnerable to data breach or you start getting weird emails or your general wellbeing and day-to-day life is impacted and it transpires that that is in relation to a data loss that has happened, then individuals will start to take greater control. Equally, they need to be provided with the facility and the regulations to ensure that the control is there.

Today the Data Protection Bill was launched. It is 200 pages and so do not ask me to go through it, but that is based on the forthcoming General Data Protection Regulation (GDPR), which is strengthening the current Data Protection Act and providing a number of rights that citizens do have to ensure that they can question how their data is used, raise a concern if a decision has been made by automated means or by machine learning, which as we go further into artificial intelligence (AI) and the world of virtual reality, is going to be absolutely fundamental.

Javier Ruiz (Policy Director, Open Rights Group): For us, we have been doing some work recently with a charity around the issues, risks and benefits in the public sector. We have been going to Birmingham, Manchester, Sheffield and another local authorities. An interim report will be published soon and it will be quite useful probably for the Committee to understand.

Something we found is that there are different types of risks when we look at data and there are the things we have been discussing like the risk of external abuse like loss and hacking. That is the concern that most people have in mind. To a degree, there is also the concern that Renate [Samson] has been explaining of the internal misuse or abuse when you understand that there is a misuse like a corrupt employee or unauthorised cases of sharing data without an agreement.

The areas that we feel are also important particularly for the public sector are the risks of unintended consequences of sharing. For example, before we were discussing the possibility of the Home Office being informed of the immigration status of a victim of crime. There is some data sharing that may trigger statutory processes or things that automatically set things in motion. You may not have thought about that. You may be looking at the systematisation. You may want to share data. For example, there is a lot of discussion around the school meals and children and the school knowing who deserves free school meals and there is also a big discussion around the stigmatisation. That is a slightly different risk and that is what public-sector bodies

need to start looking at in a more sophisticated way. They may not be in breach of any data protection legislation, but there could be an ethical or moral risk.

Finally, even more, you could have risks around the policy itself. For example, with a policy to share data about immigration status, you are probably not breaking any laws, but if you are in the public sector there is a need to understand what the implications are for some data sharing policies. It is particularly common now. They will be looking at fraud and that. Where do you want to put the limits? Where do you see the limits of the state and how much information the public sector should hold on citizens?

Then there are risks that cannot be understood completely in separation from the benefits that you intend and, there again, we have been looking at how different types of benefits really need to be understood. When you use data to improve public services for the direct benefit of individuals, that is a very clear benefit, but we hear about public benefits when you are looking at benefits to an organisation, whether it is efficiency or another type of improvement. In many cases, it will be somewhat like an automatic understanding that this will benefit citizens and the public, but in many cases you need to actually demonstrate that there is a benefit rather than just make an assumption that that will take place.

Finally, there is data used for punitive state functions like taxation, police, tackling fraud, and, again, that is quite different. Obviously, you are not going to look at anything to do with consent probably in that context, but you still need to look at how you do things fairly. In terms of risk, at the moment, we have a concrete concern here particularly I can tell you with ANPR, face recognition, etc, a few things where we have concerns, but we also think that it will be useful for a public-sector body or the London Assembly to have a broad understanding of how risks apply in the public sector.

Sian Berry AM: Just to clarify one thing that you said there, you mentioned that sometimes you can collect data that then gives you an obligation to share it, such as immigration status. Is that right?

Javier Ruiz (Policy Director, Open Rights Group): Yes, it could be. Sometimes if you know something, you have to do it. You have to take action. In that case, it may be the right thing to do, but you probably want to know that that is going to happen before you start sharing data and be prepared for the consequences.

Sian Berry AM: Can I ask the GLA, please? In response to the Government's consultation on expanding the sharing of personal data between public agencies, the GLA's response said that it was disappointed by the limited scope and wanted more powers to share more personal data. Can you explain why the GLA gave that response; in particular, when it said it wanted to share data with private companies?

Tom Middleton (Head of Finance and Governance, Greater London Authority): Yes. I will give it a little bit of context. Just like the other bodies in the group, our use of personal data only rests on the functions that we have and so we are not looking to collect personal data for the sake of collecting personal data. In fact, we go to quite extreme lengths not to collect personal data on occasions. I will just give you one example, which you are probably familiar with, Sian [Berry AM], the boiler scrappage scheme. That would be personal data of homeowners and so forth on that. That is all held by the Energy Savings Trust and we do not actually have that information. That is just one example where we are taking steps not to hold personal data. If I have it right, the particular consultation response you referred to was to colleagues who work more on the intelligence and statistics side. I do not think they are actually talking about personal data at all; they were just keen to have more data available, a bit like the Datastore stuff. Now, if that is in any way incorrect, I shall let you know, but if it is the same one that you are referring to, they were just talking about more data in general

as per the Datastore, which is a transparency thing rather than a personal data thing. As far as I am aware, we have very few ambitions indeed to get more personal data.

I am aware of a proposal - and there is probably a decision posted on our website and I know Jeff [Jacobs, Head of Paid Staff, GLA] might know a bit about this as well - the London Office of Data Analytics, which again that same team, the intelligence unit, is leading on setting up. That is about data sharing with boroughs but, again, a lot of that will not be anywhere near personal data. That will be the usual public-sector data. If it does stray into the realms of personal data, then we will have to be very careful, but that is not the intention. It is more the intention - a bit like the Datastore - just to have stuff that are of interest to the public around what public bodies are up to. I can assure you we do not have huge ambitions to have more personal data. In fact, quite the opposite. We do not need to do it extensively. As you have already noticed, risks are attached. The more you have, the more likely it is, just through human error, that it strays outside the building.

Sian Berry AM: Essentially, that was mis-speaking. What was meant was statistics and depersonalised 'big data': that is the phrase that is used for it.

Tom Middleton (Head of Finance and Governance, Greater London Authority): Yes, the Datastore stuff, which I hope is viewed as the good side of this coin, which is transparency and nothing to do with individuals. No one is identifiable and so forth. However, if there is anything that bothers you, we can have a look at it.

Sian Berry AM: Thank you. I have a question to the Information Commissioner. Thank you for coming. We will ask you a more general question in a moment, but if I could ask you just to comment on that last point where lots of data is collected, are there any additional benefits and risks to doing that if you can turn it into anonymised aggregated data or does it bring extra risks? What are you doing to look at that?

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): It is complex area. If you need data and you need to process data and you need to share data for good public policy reasons and for the flipside, the transparency that public bodies might want to have with the public, then we would encourage aggregating and anonymising data as a good practice. The challenge is many organisations do not do it properly. If you are going to aggregate information and if you are going to anonymise information, you need to be very careful that the dataset that you are putting out there cannot be reidentified by linking, let us say, datasets with other publicly available information. That risk of reidentification is addressed in the new Data Protection Bill that, as Renate [Samson] said, was tabled today and was published today. There is now a sanction and a penalty for reidentification of data. That is a good thing because it will drive good practice to properly deidentify or anonymise information so that it can be used for good public policy purposes. However, it has to be done well and it is a risky area because the more data that is out there the more ability people have to put datasets together and then somebody who was not identified in a new context now is. I hope that that makes sense to you.

Sian Berry AM: It does. Are the sanctions that are proposed against all the people who released all the data that was then reaggregated or --

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): If an organisation takes steps to purposely reidentify, then there is a sanction against them, and then our office would have the ability to investigate the lack of proper processes in the release of the data, if that makes sense, and so there are two sides to it. We want to discourage people from reidentification.

Len Duvall AM (Chair): Thank you very much for that. Let us move on to individual rights and Navin Shah AM.

Navin Shah AM: Yes, I have a couple of questions on individual rights and they are to our GLA, TfL and police colleagues. The first one is: how do you get consent from individuals to process their personal data? Do you want to start, Tom [Middleton]?

Tom Middleton (Head of Finance and Governance, Greater London Authority): If I could, thank you, just briefly. I am sure the others want a chance to speak as well. Our preferred approach, as you probably appreciate from having seen our website, is to ask people to opt in and not to assume consent.

In the context of our website, one thing I should mention, which Members and colleagues should be aware of, is we are combining the microsites and the main site to bring greater consistency. We have had a whole series of microsites in the past, which have their own ways of doing things, which include things like Talk London and Team London. There is going to be a process of being a single website and you go off the head into the various bits to get what you want, which will be helpful in this context rather than looking at different policies on different parts of the of the web.

There are two areas where we assume consent and we said this in response to your question: the CCTV here at City Hall, which I think you are aware of, and when individuals correspond with us because it is quite difficult to do anything about that, and so that is where we are at.

Richard Bevins (Head of Information Governance, Transport for London): In TfL we are very conscious that consent is only one of the bases in the current legislation that allows us to collect and process personal data. Often there is an alternative legal basis for us to do what we do with personal data. A lot of time that we are doing something only because TfL has a statutory power to do it and that is a legal basis for processing personal data. That is relevant to all of the on-street enforcement we do, whether that is the Congestion Charge or penalty charge notices on the road network. That comes back to the fact that we have a statutory power to collect the personal data that we need to do those enforcement activities; and similarly, with the revenue enforcement on the Tube.

Another basis is for the performance of a contract, which covers an awful lot of the processing that we do to deliver a ticketing product to an individual who has bought that product or signed up for that product. That is also very relevant to the employment context as well. We process an employee's personal data in order to fulfil our employment contract with that individual as well. There are other bases in the Data Protection Act and there will be other bases in the GDPR and the new Bill that will supplement the provisions around consent.

Therefore, we do not rely on consent an awful lot. We do gather people's express consent to receive marketing from us. We do not actually do very much marketing but we do gather people's opt-in consent to receive marketing information from us if they are registering their Oyster card, for instance. However, in general we do not do a lot that is reliant on consent.

Paul Wylie (Director of Strategy, Mayor's Office for Policing and Crime): I will be quite quick. It is similar to Tom [Middleton]'s position. It is consent where there is correspondence or as part of a consultation and then outside of that, as I mentioned earlier, in terms of using data that others have gathered for the purposes of evaluation. That consent or otherwise is obtained at the point of the third party rather than ourselves.

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): In terms of policing, we try to avoid relying on consent certainly when we can rely on our policing powers to gather information.

The areas where we may get involved in obtaining an individual's explicit consent is perhaps in some diversion techniques that we use with offenders to opt into some sort of diversionary scheme and, similarly, with victims to participate in those sorts of initiatives as well. Then victim support scheme referrals are really the only other areas that I can imagine that we regularly rely on consent. There are some public surveys that are undertaken as well where people or victims may get surveyed around their experience with policing where the individual will be offered the opportunity to participate in that survey.

That is it. As I say, really, we are relying on our policing powers in the majority of cases because consent can be withdrawn.

Navin Shah AM: My second question is about the scope for individuals to opt out of having their personal data being collected or those individuals to manage their own personal data.

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): Yes. In terms of managing it, there is limited scope at the moment for individuals to manage their data other than using the provisions within the Data Protection Act or for subject access to view information that we are holding about a member of the public or our own people. Individuals can raise an objection to that processing and that will be dealt with in accordance with the provisions of the Data Protection Act.

The only real dynamic thing that we have going on at the moment is the ability to report a crime online. We do not yet have, although I think the ambition is to have at some point, the ability for victims of crime perhaps to view the progress of their crime case, but at the moment that is not available, unfortunately.

Paul Wylie (Director of Strategy, Mayor's Office for Policing and Crime): In terms of managing information, if an individual wished to be removed from any communications database we have, they simply need to reply and we would absolutely do so. In addition, should they write in through the Freedom of Information or Data Protection Acts, then, again, we would process that and remove anything that they wished. However, as I said, the amount of information in this regard is quite limited for MOPAC.

Richard Bevins (Head of Information Governance, Transport for London): Similarly, if we are contacted with a request, whether that is to have communication or to have information deleted or removed from correspondence databases or from other databases, we will act on those requests in accordance with the current legislation and we provide the ability to opt out of any of our regular communications around services on the Tube or whatever it may be. You can unsubscribe to those very easily. More broadly, you cannot opt out of having some personal data processed, if you use Oyster to travel, for instance.

Tom Middleton (Head of Finance and Governance, Greater London Authority): Our position is very similar to MOPAC's in the sense of the limited amount and people are free to opt out. One of the things we are trying to do as part of the move to GDPR is to have a situation, say, on Talk London where people can manage their own accounts and can manage the information held on them or delete it entirely. That would be the direction going forward.

Navin Shah AM: On the same issue of individual rights, I have a question for Renate [Samson]. What else should organisations in the GLA Group do to help individuals control their personal data? Which other organisations do this better or as well?

Renate Samson (Chief Executive, Big Brother Watch): It is quite interesting. Just coming about to the points that were made earlier about wanting to gather more data but not realising that it is necessarily personal data, it comes back to my point that we are all our data and wherever we go. The fact we have a mobile telephone in our pocket and the fact that we have an Oyster card or a credit card or a debit card means that that is all data. That is data that is really interesting to want to see and analyse but it is still, more often than not, not industrial data but personal data.

Also, interestingly, about Oyster card, I used to have an Oyster card that was not registered. I do not know if you can still not register an Oyster card, but I was penalised for wanting to effectively be invisible but still be able to travel. I had to pay more because I was not allowed to buy a monthly or annual Oyster ticket. I had to pay a weekly ticket, which cost more. That is what I would say one of the key examples. (a) If you do not want to provide personal data or data for a service, you should not be penalised; you should be able to receive exactly the same service, not more expensive, not restricted, if you choose not to provide personal data.

Furthermore, we have heard a lot of examples where you can opt out from marketing, but what we now learn is that of course opting out of being caught up on CCTV means now basically not leaving your house and so is not actually functional. For example, TfL's recent study was published last week about Wi-Fi collection, and there is an awful lot from the publication that we are very supportive of. However, the signage that was put up that I saw did not tell me that I needed to turn off my Wi-Fi; it did not tell me that I had the option to opt out and that there was a way for me not to be picked up. You have since explained how that can be done. I would say that we need much more signage as we already have about, "You are now on CCTV", put up everywhere: "You are now being monitored via your Wi-Fi. Should you not wish to do this, please turn your Wi-Fi off". We need to move much faster at being more transparent and open and not feeling irritated about the fact that some people might drop out and not be part of your dataset, but that does not mean that your dataset still cannot provide benefits.

Navin Shah AM: Richard [Bevins], do you want to respond to any of that?

Richard Bevins (Head of Information Governance, Transport for London): Yes, I should. You can still have an unregistered Oyster card, quite definitely --

Renate Samson (Chief Executive, Big Brother Watch): You will still be penalised.

Richard Bevins (Head of Information Governance, Transport for London): -- but you are right. If you are going for a monthly or longer Travelcard, then we would say in your own interests you do have to register it to protect the balance on the particular product that you have bought.

Renate Samson (Chief Executive, Big Brother Watch): Sorry, that is arguably my choice whether I want to protect it or not, but you have made that choice for me.

Richard Bevins (Head of Information Governance, Transport for London): Yes, you are right. On the Wi-Fi pilot that was done before Christmas, we went to great efforts to explain how people could opt out. I agree that it did not actually appear on the posters, but it was explained in the articles in *Metro* and on our website and in emails to customers. There was plenty of information about how to opt out but just not at that point when you walked into a station on a poster. It was a trial. It was four weeks and we have very much taken on board what we needed to from that trial. Absolutely, we are going to look at reproducing the CCTV-type signs that we have on the Tube stations at the moment with signs that say, "Wi-Fi is being collected", as well --

Renate Samson (Chief Executive, Big Brother Watch): And how to opt out?

Richard Bevins (Head of Information Governance, Transport for London): Yes, we will include that as well and we fully accept that people will want to opt out. As you say, if they are out of the dataset, then that is fair enough; it will still be a good dataset.

Sian Berry AM: The main question I had was about the whole posters issue and the fact that the posters said on them, "Go to a website to look up how to opt out", instead of just saying, "Turn off your Wi-Fi", which was the simplest possible instruction.

Can I ask about the data that you collected and how anonymous it was? That is that is the main question that we have. You are collecting media access control (MAC) addresses from everybody's Wi-Fi-enabled devices, which includes phones, and then you are immediately anonymising that and turning it into a hash that is unique but not? The purpose of it is to track people through stations, is it not?

Richard Bevins (Head of Information Governance, Transport for London): Yes, we were immediately converting it into a number that was not the MAC address number and was a very complicated and long number. It was a unique number that was irreversible and so we could not go back to the MAC address once we had done that conversion and we cannot do that now. There was a key to it that was doing the scrambling. We have thrown that away now, in fact, and so, yes, it was pretty much instantaneous pseudonymisation of the data.

Sian Berry AM: Is the point of it that when they pop up in another Tube station you know who they are again because you are able to tell what route they took through the network? These are the lovely maps that you've produced.

Richard Bevins (Head of Information Governance, Transport for London): Yes, but --

Sian Berry AM: Are they still anonymous if you are still able to match them to the same --

Richard Bevins (Head of Information Governance, Transport for London): We cannot match that to an individual but it is still --

Sian Berry AM: You can match it to the same phone in different places?

Richard Bevins (Head of Information Governance, Transport for London): We can tell it is a unique device, yes.

Sian Berry AM: My concern about this is that this is reversible data in the sense that the Information Commissioner was talking about earlier on with these unique trips through the system and it is the same phone appearing in different places. Potentially, that is reversible, is it not?

Richard Bevins (Head of Information Governance, Transport for London): We do not think it is reversible to the extent that you can identify a person.

Sian Berry AM: If you know more about that person through another dataset, possibly, it is. This is the question that the Information Commissioner had earlier on.

Richard Bevins (Head of Information Governance, Transport for London): It is a risk that we are aware of and that we paid a lot of attention to when we were doing our privacy impact assessment and when we were talking to the ICO about what the risks were around the processing that was inherent in the trial. It is something that we will be thinking about a lot, still, as we think about making it a permanent thing. However, we do not think that you can get to an identifiable individual from the dataset that we are collecting.

I should say it is well of course that we have absolutely no desire to identify individuals from it. That is very far removed from why we would like to collect the data.

Sian Berry AM: No, I understand. I used to be a transport campaigner and this kind of detail for transport planning purposes is really useful.

Can I ask the Information Commissioner just as a final thing: are you content with the way this trial was carried out? Have you asked for any improvements? Do you have concerns about the reidentification of people?

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): The TfL Wi-Fi trial was a really good example of a public body coming forward with a plan, a new initiative, consulting us deeply and doing a proper privacy impact assessment. I was not involved in it but I know my staff gave a lot of feedback --

Richard Bevins (Head of Information Governance, Transport for London): It was very helpful.

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): -- and TfL responded to that. We agreed with them that at least for now, in the one-way hash that they wanted to implement for the trial, it was not reversible and it was impossible at this point to identify or follow the person through the various Tube station. I would say it is a good example of privacy by design and good conversations with the regulator to try to get it right. There is a lot of effort there.

Sian Berry AM: That is good. You will be keeping an eye on that in future and potential matching of datasets?

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): Of course.

Richard Bevins (Head of Information Governance, Transport for London): Yes, we are planning to continue the dialogue with the ICO.

Navin Shah AM: I just wanted to get back to Javier [Ruiz] in terms of having heard the GLA bodies about how they manage personal data. What more, or what else, can they do to help individuals to control their personal data?

Javier Ruiz (Policy Director, Open Rights Group): I would agree that in the case of the police or perhaps going back to the justifications represented before of the state and community functions, it would be quite hard to operate purely on the basis of consent but there is a lot of room for more transparency and accountability. Just the fact that we are discussing now the type of data and agreements that you have instead of you having been able to look on their website before the meeting to find out; that, for example, is an example. From that end, for the police and MOPAC, it is about definitely transparency and accountability. Even if you cannot give people full control over their data, there is a lot of room.

For other types of public services, there is definitely a lot more room for a completely citizen-centric approach. When we look at the data for the London strategy, what we saw was actually that it is very clearly market-driven, their strategy, but when you look at their theme of building public acceptance, their approach towards personal information in the strategy is based around making people trust institutions so that they will give you the data. This is quite an instrumental view of privacy in the sense that, "We are going to do something and hopefully it will be for your benefit and now we are going to get you to trust us".

Other cities like Barcelona are taking a much more citizen-centric approach where citizens are at the centre of this. They own the data and we are the stewards of the data. We are going to want it for them and with them, rather than try to more or less - I do not want to be too disrespectful - trick them to give you the data, let us say. In that sense, there is a lot more to do. When you look at things like integration optimisation and behavioural change, again, those are approaches where citizens are almost like managed rather than producers of services. In that sense, there is still a lot more room for giving citizens control of their information.

In terms of the specifics that were in the document, the discussion around identification is important but there is another development. I do agree with Renate [Samson] that there is a lot of room for opt-in and even more opt-out if that is not possible because, when you need big data, it just has to be big enough. You do not need 100% of the people that pass through a station. As long as your sample is not biased by the opt-in or the opt-out, you should be able to give a lot more control to individuals.

There is a more important aspect almost nowadays, which is that even if people are not identified, they can still suffer consequences from the use of the data. It is like there is a whole new field of group privacy in academia. There are things, for example, like the postcode mapping of the police or anything that involves changes. For example, the Society of Actuaries insurance premiums, when they use the data from hospital episodes. Individuals had their insurance premiums changed not because their individual data had been accessed but because as a class their conditions were known still to be different. There can be a secondary effect and that is something that generally escapes the strict limit of the ICO but, again, going back to the need for a wider approach regarding the private sector in that it would be good to not just try to stick to what the letter of the law on data protection says but try to look a bit wider about the implications of data. What you will find in many cases, particularly around the big data, is that there are effects there that affect the individual.

Also, what you will find is the public perception in many cases does not match the law. Despite all the attempts to try to make people understand that once the data is anonymised it is not their data and they have absolutely no legal right to it, people will still believe that it is their data. Why is this company benefiting from my information? Why are they doing this? In that sense, to a point, it is true. From a strict data protection point of view, it is not their data, but from the point of view of value creation, still, the data, there is quite a big issue.

In terms of consent then, what we think is the most important question about the GDPR is going to be revoking consent because everyone has been focused on how you obtain consent and how you give people the best information possible, but the big challenge is that with particularly GDPR people should be able to revoke their consent. If you are operating on a consent basis, you need to have very clear mechanisms for the revocation of consent and also the set of consequences that that implies, which could be the deletion of data. That is again probably not for the MPS but for some of your other public bodies. Being able to implement those mechanisms is going to be quite a challenge and that is something that you should really be looking at now in terms of GDPR.

Len Duvall AM (Chair): Let us move on to the issues of security. Keith Prince [AM]?

Keith Prince AM: Thank you, Chair. My first question is to the Information Commissioner, if I may. What are the key security risks to the public sector around personal data, in terms of both internal and external threats, please?

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): The biggest risk is people, but that is also the biggest solution. You can have a very strong network security system where the software is being updated, there is good training on passwords, but the system is only as good as the weakest link. Again, training and awareness is just so very important.

Part of the problem is everybody is focusing on big cyber hacks and criminal actions and that is where the newspaper headings are going, but I can tell you that 95% of the data breaches that are reported to the ICO are low-tech and are not criminal hacks and they are completely preventable through training, up-to-date software, clear roles and responsibilities and evergreen IT security practices. Legacy databases, which are an issue in the public sector, as we saw with the NHS ransomware attack, is just not keeping up with the patchwork management. It is those lower-tech problems that are creating most of the security risks and the security gaps and that is frustrating for everybody.

I would add another security risk and that is devices taken outside of the network, use-your-own-device policies. There are issues with that.

The good news is that the GDPR, because it is the gold standard for data protection legislation, is going to incentivise better practice and more implementation of good practice as well as more investment in security. That is a great thing for the public sector because the law has more significant fines and sanctions for gaps in security that end in compromise for citizens.

What we have to remember - and I go back to what Renate [Samson] said earlier - is that the new law and data protection is really all about people and so it is really focusing on people, the people whose data is compromised or is vulnerable, but also the people who can create a better and safer environment to secure public-sector and private-sector data.

Keith Prince AM: That was very helpful. Thank you. My next question is to TfL, MOPAC and the GLA. What is the most significant data loss you have suffered in the last few years and how did you respond to it? We will look to TfL first of all.

Richard Bevins (Head of Information Governance, Transport for London): We have had a small number of data breaches over the years. Just to add to what Ms Denham was saying about the lower-tech end of the threat spectrum, my example probably relates to a breach involving paper, which certainly at the time TfL did still have some of. It involved Oyster application forms. There was a paper-based process for that particular product and quite a large number of forms were unaccounted for in transit between post offices and our service provider and ourselves. That was an issue that we reported to the ICO and we took action as a result of that, obviously, and investigated and followed through and changed some processes. It is now it is now an online secure process, partly as a result of that incident. The breach did not result in any enforcement action being taken against us because of the steps we took to mitigate the consequences at the time.

Keith Prince AM: Did you find them?

Richard Bevins (Head of Information Governance, Transport for London): We never found them, no.

Keith Prince AM: Thank you. MOPAC?

Paul Wylie (Director of Strategy, Mayor's Office for Policing and Crime): As befitting quite small organisation, you will not be surprised that there have not been that many. There was only one that we are aware of back in 2015, which was informed to the ICO. It was to do with a personal data breach of an individual and it was dealt with as a training and personnel issue in terms of how we operate as MOPAC.

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): Similarly, it was case papers. There was a theft from a pub where an officer had taken papers out. He had called into a pub on the way home. It was a classic bag theft, but the officer was dealt with through disciplinary measures because he should not have done what he did. It was reported to the ICO. Again, it just reinforces that human element. You can put all the technical measures you like in place, but you have to address the behaviour. That is the challenge. People do things that they realise afterwards that they should not have done and, in some respects, no amount of training changes that. We have to reinforce that with ongoing awareness and the appropriate sanctions when that goes wrong.

Keith Prince AM: Any in the GLA?

Tom Middleton (Head of Finance and Governance, Greater London Authority): Yes, we have had one notifiable breach, which we reported to the ICO. I mentioned the Housing Moves database earlier. In response to that Freedom of Information [FOI] request, unfortunately someone was sent out an Excel spreadsheet. It contained some information which was obviously deeply regrettable. As far as we are aware, the one person who received that response deleted it and we have not heard anything since and no enforcement action as a result, but given the steps that we took.

Speaking about Excel spreadsheets, we have found quite often not just about personal data but just data beyond what people ask for. You have to very careful with tabs on spreadsheets and forwarding on spreadsheets because you think you are being helpful by giving people Excel spreadsheets but you can open up a whole world of pain doing that. That is beyond personal data; that is just any sort of data. That is the one we have had. As far as we are aware, no damage was done and, a bit like my colleagues, it was regarded as a training issue for colleagues in Housing and Land.

Keith Prince AM: Thank you. Again, to all four of you, how significant are external threats to your security systems and where do these threats come from?

Richard Bevins (Head of Information Governance, Transport for London): There are, obviously, just from what you read in the press and there are obvious external security threats and cyberthreats to anyone running services that are dependent on digital systems. We do see evidence of that in attacks on TfL's network. They are picked up and blocked and I could not say where they come from. I do not know if that is known in a lot of instances, but I do not know where they come from or what the motivation is. One can only presuppose.

Paul Wylie (Director of Strategy, Mayor's Office for Policing and Crime): In terms of MOPAC, we have two sets of data systems coming in. The majority of our correspondence is dealt with through a contract with the GLA and so the GLA runs the IT system for most of our work. In terms of our secret and top secret and wider MPS work, we also have A Windows Application in a Resilient Environment (AWARE) terminals in our building for accessing MPS systems, which of course is run by the MPS.

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): In terms of cyber, foreign state and organised crime are the two with the most capability. That is our defence posture. It is to

protect against that. I would not say in reality, but the greatest risk is someone clicking on an email link that they should not, assuming all the right measures are in on the infrastructure. That is a behavioural culture thing which we regularly brief staff on through awareness initiatives.

As Paul says, we have our own infrastructure, which we extend out. That is regularly checked with a health check to ensure it has the right defences to protect against the known risks.

Keith Prince AM: Thank you.

Len Duvall AM (Chair): Sorry. It does beg a question. Have we ever lost any data from an external threat?

Richard Bevins (Head of Information Governance, Transport for London): We had an attack on the cycle hire website last year, which, as far as we could establish, was a criminal, actually not a very organised criminal. It was an individual lone act that penetrated the cycle hire website and certainly accessed some data about customers and we think took some data.

Len Duvall AM (Chair): The outcome of investigations, presumably?

Richard Bevins (Head of Information Governance, Transport for London): Yes, we took all the steps that we needed to do to manage the incident and to audit what might have happened. We contacted the affected customers. We offered them credit protection service and that kind of thing and, separately, the police investigated the actual attack and somebody was successfully prosecuted.

Tom Middleton (Head of Finance and Governance, Greater London Authority): Chair, the GLA has not lost, as far as I am aware, any personal data as a result of that. What you are probably recalling is once our website was successfully hacked and made to look different and say strange things, but no personal data was involved.

Keith Prince AM: Finally, then, really, to the four of you, how would you decide when and how to inform individuals about a potential data loss?

Richard Bevins (Head of Information Governance, Transport for London): The Information Commissioner has some helpful guidance that explains what the current position is in legislation because we are not under any obligation to inform affected customers but, as you would expect, it is something that we would want to do in certain cases. There is a set of criteria that the Information Commissioner, as I say, has published that it is what we benchmark against if we are looking at an incident. It is around the type of data that is been affected and the number of people that have been affected and the use that it might be put to in the wrong hands. It is an exercise that we go through to weigh all of that up internally.

Keith Prince AM: The question was how would you decide and I am just wondering who makes that decision to contact affected people.

Richard Bevins (Head of Information Governance, Transport for London): Internally, that has been a decision that has been made at the highest level when we have referred it up within the organisation.

Keith Prince AM: Thank you. Paul [Wylie]?

Paul Wylie (Director of Strategy, Mayor's Office for Policing and Crime): In the 2015 incident I mentioned, we were able to identify who was the subject and we were able to write to him and issue a formal

apology. In terms of the process more generally, as Richard [Bevins] said, there are good tools available for making that sort of decision and it would the Chief Executive of MOPAC that would make that decision.

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): Again, we would follow the same criteria. In terms of notifying the individual, it is the level of risk that that presents to an individual, informing them so that they can take appropriate steps to protect themselves. In terms of who would make that decision, we would, in a breach of that nature, create a gold group and it would be the senior officer responsible for that gold group on the advice of myself or my team from the data protection side. The Senior Information Risk Owner, which is at Assistant Commissioner level, would be the route for which a notification would go to the ICO staff as well.

Tom Middleton (Head of Finance and Governance, Greater London Authority): Very similar to the others. The ICO guidance is very helpful and we take the decision via the Director of Resources here, who is our senior lead.

Keith Prince AM: Just quickly to the Information Commissioner, it was interesting that Richard said there is no legal obligation to notify people. What is your advice though on that sort of thing?

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): The good news is that the law is changing, so there will be a mandatory duty to report significant risks. Breaches that could result in significant risk to the rights of individuals will be mandatory as of 25 May 2018 and so all public bodies will be required to report to the ICO and also, if there is a high risk to individuals, notification to those affected individuals. There will be a requirement and also a time limit, so the ICO needs to be informed within 72 hours of a breach. There is a very strong public policy purpose behind that provision. It is not about punishing organisations or playing 'gotcha'; it is really about the public knowing that a regulator has their back and the regulator can take action. If my office feels that notification should have been made to individuals and it was not, then we have sanctions and powers to take action. This is a whole new regime that is coming into force in 2018.

Keith Prince AM: You say there is a time limit by which the organisation must notify you; 72 hours I think you said. Is there equally a time limit by which they have a duty to inform the victim?

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): The duty to inform the victim is "within a reasonable time period". That is why the devil is in the details.

Keith Prince AM: You can make a lot of money out of that word, 'reasonable'.

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): Yes, but in some cases, there can be a breach - and maybe there are examples here that the organisations can give you - where they know there has been a breach, but they are not clear which data has been lost and whether or not it is recoverable, etc. Within 72 hours, there may not be all of the information necessary to carry out notification, but if there is, then as soon as practicable would be our advice. We are going to be issuing new guidance about the thresholds for notifying individuals and reporting to our office.

Keith Prince AM: Will we be given some kind of a guideline then as to what you believe 'reasonable' to mean because 'reasonable' is not definitive? As I said, lawyers make a lot of money out of the word 'reasonable', whereas if you could give them some guidance, "In this instance of X number of days, that instance of Y number of days". Obviously, I appreciate that a lot of the Oyster paperwork that was lost, you would not know who was on a piece of paper, would you? You would not.

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): You might not. That is part of the problem, but we will be issuing guidance. It needs to be pan-European guidance, because it is coming out of the GDPR and so we have to get agreement among all of my counterparts across Europe. The guideline on data breach notification will be coming out in December. On top of that, the ICO will give more detail to organisations, because it seems to be one of the areas of the new law that is requiring a lot of clarification. My message is: tell it all, tell it fast, tell the truth, get it out there and identify people, because it really is about also our ability to collect trends and to be able to give advice to all organisations across sectors about how to protect themselves, because these are the 10 top risks that you are going to face. There is a really good public policy, a reason for this provision in the GDPR.

Keith Prince AM: Thank you very much indeed.

Len Duvall AM (Chair): Shall we move on to the future of personal data then and legislation? Over to Peter Whittle.

Peter Whittle AM: It is a question for Elizabeth [Denham], thank you. You have already touched on some things, but can you say how will Brexit and the introduction of the GDPR affect how personal data should be processed?

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): GDPR, as I said, is probably the gold standard regulation around the world right now and there are going to be lots of countries that are going to imitate it, which is a good thing. We have waited a long time for new data protection legislation and I would say it has taken much too long because it is a generation behind the beginning of the internet. The law is strong. The GDPR will have direct effect in the UK. The Government has committed and now has the Bill that brings in the implementation of that regulation into UK law.

Peter Whittle AM: That was in the Queen's Speech most recently, right?

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): Exactly. Now the Bill has been introduced in Parliament, so as well as the Law Enforcement Directive, which I know that the law enforcement community was waiting with bated breath for that, so there is going to be a comprehensive law that brings in these standards into UK law. That is a very good thing.

Your question is: how does Brexit impact that? We are going to have those standards, which are essentially equivalent to the European Union (EU) standards, in our national law. That is a good thing, but we may lose the ability to participate in the pan-European system, which is something that I think would have been a positive thing for the UK, especially around international policing, crime and anti-terrorism. The closer we are to Europe in that sense the better it is, but our laws will be essentially equivalent to the EU and the highest gold standard around the world, which is very positive.

Peter Whittle AM: Thank you for that. Could I ask Richard [Bevins] and Paul [Wylie] what plans you have got in place, if any, to implement the GDPR?

Richard Bevins (Head of Information Governance, Transport for London): We have got plans. We have been closely following the drafting and the debate around the GDPR ever since the off, really. We are well-prepared in terms of knowing what we have got to do. The Bill will fill in those gaps that we still have, the questions that we still had about how some of the details in the GDPR will be implemented in the UK, for instance. We have had long enough to identify that there is quite a lot to do to be ready for May next year

and now we are working through our plans to do that very practically on the ground, changing privacy notices that customers are exposed to, identifying all the things that need to be updated on our website, the contractual changes that we need to make with our outsource suppliers, mapping where we hold personal data in the organisation and making sure we fulfil all of the accountability requirements that are in the GDPR and that are perhaps the single biggest element that is changing for it. Yes, we have a programme of work and we are working through it.

Peter Whittle AM: You are up to speed. Is it pretty much the same for you, Paul [Wylie]?

Paul Wylie (Director of Strategy, Mayor's Office for Policing and Crime): It is, in terms of the operation of MOPAC as an organisation. What I would touch on also is MOPAC's role as an oversight body of the MPS. We are approaching that from three levels, official, formal and then almost an assurance. At an official level, I sit on the MPS's Risk and Assurance Board, of which information governance is one of the risks. At a formal level, the Deputy Mayor has a regular Oversight Board with the MPS, at which this is a topic of discussion, of course. Thirdly, at an audit level, both of our organisations and the whole GLA is subject to the Directorate of Audit and Assurance and they produce reports to the Independent Audit Panel, again which will be scrutinising our progress towards this.

Peter Whittle AM: Thank you. Tom [Middleton], is it the same story for you? I was also wondering whether the Mayor has commissioned any work on any changes there might be between the flow of information between the GLA and the EU, for example.

Tom Middleton (Head of Finance and Governance, Greater London Authority): We are very much in the same position as the others. We have done a comprehensive survey of all the personal data we hold and what steps we need to take to comply with the GDPR as it is coming in. Paul [Wylie] mentioned audit, and with your other hat on, it strikes me it might make sense that you would want to ask our friends in audit to have a look at that and reassure you that we are doing what we say we are doing, so that is probably something we should add to the work programme.

In terms of GLA data flow with the EU, I am not particularly aware of what that might be, but --

Peter Whittle AM: Should there be more work done by the Mayor on this?

Tom Middleton (Head of Finance and Governance, Greater London Authority): Not that I am aware of, but people can suggest things, and please do so.

Peter Whittle AM: There has been no work commissioned on the impact, as it were, of our leaving the EU on the flow of data?

Tom Middleton (Head of Finance and Governance, Greater London Authority): I am not aware of anything. I am not quite aware what the angle would be on that.

Peter Whittle AM: Thank you very much.

Sian Berry AM: It seems to me like the GDPR is an opportunity to review all our practices and spot and find any gaps there might be. I have got a few questions about new technologies that are coming in. It seems to me like partly we are doing new tech, sometimes we are doing it right from the start, and I have been asking questions about data and body-worn video, because that has just come into the MPS. The police now have a camera on them, a lot of data is being recorded. It is not so much the crime recording, what happens when

there are crimes aspect that I have been worried about, it is more what happens to data that you do not need to keep, how long do you keep it for and all those kinds of things. For body-worn video, the answers have come back quite reassuringly that it automatically deletes after 30 days unless it is flagged - or 31 days, sorry - and we are reasonably content with the policies that have been done for body-worn video.

The other thing that has been in the news and caught the eye of people in terms of data has been facial recognition technology. From what the Biometrics Commissioner said today, if I can ask the Information Commissioner, it seems to fall a bit between you, the Biometric Commissioner and the CCTV Commissioner, who all have sort of overlapping interests in facial recognition. Is this why it is difficult to know what the policy is for facial recognition, because there is nobody making it? Can you maybe fill us in on what your thoughts are on this?

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): There are a lot of commissioners working in this space. It is a crowded space.

Sian Berry AM: Yes. Do you speak to each other?

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): We do speak to each other. Yes, is that not a wonderful thing? In fact, I am meeting with the CCTV Commissioner next week. I have met with the Biometrics Commissioner and I share his concerns that were expressed in his annual report. We had a meeting on that. Again, he has a very specific mandate. My remit is very broad: it is data protection across the public sector, across the private sector, across the third sector, and so we are not a technology-specific regulator, but at the end of the day we do regulate in this space, so if there was a complaint it would come to our office. The Biometrics Commissioner is writing reports and making recommendations and raising issues. That is the same with the CCTV Commissioner. The Camera Surveillance Commissioner does not have regulatory powers to take action, so it is more of raising awareness and critique of public policy. We work together, but we deal with all technologies across all sectors all the time and so we have a very broad remit, but I have deep respect for the work that the Biometrics Commissioner is doing and I agree with his concerns on facial recognition.

Sian Berry AM: OK, but ultimately you will be the one who might put the guidelines out. If we come to any conclusions here, we might write to you. That is really useful to know.

Could I ask the MPS about this therefore? It has been announced twice now in two years in a row that it is going to be used at Notting Hill, but we have quite little information about what information is being kept. I have put in about 20 written mayoral questions about this on various aspects.

Can you tell us roughly what sort of a data protection approach you are taking to the information captured and what sort of approach you are taking to the database? Every time I ask about the database it seems to be the same size, which does not make a lot of sense to me. Are you planning any consultation or publishing any guidelines about how you are using it?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): The trial - and it is still a trial - has been used at the two more recent Notting Hill Carnivals. A small subset of data has been used as that piece to monitor, which is people coming through the gates and that is of wanted individuals and those with bail conditions not to enter the carnival area. That sample is drawn from a wider database - I imagine that is the one you are referring to - and the size of it was 2.9 million records of our custody images. That is the source. The images on the facial recognition database are used for the carnival. That is just kept at the moment for three months for analysis purposes, for the purpose of the trial, but it will be 31 days, the same as

body-worn video, if and when it is used and it moves into operational service, as at the moment it is just a trial. The reason it is a trial still is that we have not been able to deploy elsewhere in any meaningful way and there are certain conditions under which that camera system works at the moment and finding the right place to trial it further as part of the trial. The intention is that that concludes the end of this year.

Sian Berry AM: All the images are kept, even if they are not matched, but only for three months?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): It is the reads, yes, just to prove the technology.

Sian Berry AM: That is useful information.

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): Yes, and those images are not used for any other purpose at the moment.

Sian Berry AM: They are not put on to the database or anything like that?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): No.

Sian Berry AM: The database comes from custody images still?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): Yes.

Sian Berry AM: That is useful to know. In terms of drones, also in the news, and helicopter footage, if I bundle those two in, it appears to me that the helicopter footage which is kept by the Police Aviation Service, which is a central service, the policy on how long they keep it for seems to come from each individual force that they are capturing the data on behalf of. It appears they are keeping all the MPS images for seven years and that that might be one of those policies that has been overlooked, that you have not put a policy together for removing those images.

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): I am not sighted or aware of that.

Sian Berry AM: This is what we heard and we have checked that --

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): Yes, I will verify, yes.

Sian Berry AM: That seems to me like there is a gap because there is no way you need to keep that information for seven years.

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): No. I will say no, but with the caveat that I will need to verify it, yes.

Sian Berry AM: Except if it is flagged as needed for evidence, yes.

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): That stuff is very much the statute of limitations periods and things like that, so it is a legal hold, which on individual cases I can imagine that is right, but not on all material gathered.

Sian Berry AM: That is right. It seems like there may be no policy.

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): I will review that one and get back to you.

Sian Berry AM: On drones, because this is new technology, presumably you are taking a more robust approach to planning for data protection?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): Yes, and that is going through a privacy impact assessment process at the moment. It is an eight-week trial, which has just started, and we are initially using the same measures as body-worn video, so it will be 31 days, unless it is operationally necessary for criminal proceedings.

Sian Berry AM: Are you planning any public consultation on any of these new technologies?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): That will be a part of it.

Len Duvall AM (Chair): We will move on from that point. Will you also be providing the Police and Crime Committee the evaluation of trials? Is that MOPAC's role in the oversight arrangements or is that the MPS's role? Either of you, can you make a note and can we just agree that action?

Bob Farley (Head of Information Law and Security, Metropolitan Police Service): We will come back to you, yes.

Len Duvall AM (Chair): Thank you very much.

Sian Berry AM: Thank you. Can I ask TfL whether there have been any requests, any consideration of using facial recognition on any of TfL's cameras or on the network at all?

Richard Bevins (Head of Information Governance, Transport for London): We have no plans to use any facial recognition in connection with any service.

Sian Berry AM: If there was, you would tell the public before this happened?

Richard Bevins (Head of Information Governance, Transport for London): If there was, we would start from very first principles and make sure that we did a really good data protection impact assessment on it. Part of that would be telling the public and consulting with the public.

Sian Berry AM: Just briefly, because I know we have not asked the campaigners anything for a while, is there anything you would want to add on new technologies or the facial recognition issue particularly?

Renate Samson (Chief Executive, Big Brother Watch): Thank you. First of all, we have just published a report about using body-worn video by police forces across the country. We raised extreme concern about the fact that not one police force nor the Crown Prosecution Service (CPS) could tell us how often footage from body-worn videos have been used to secure or otherwise a conviction. We think that is a huge problem if you are going to use this technology. There have already been plenty of questions asked by police forces within their own trials about whether the technology is proving to do all the things that we have been promised. You

should publish not just body-worn video, but how often CCTV or any other surveillance camera footage is used in convicting an individual. That would be helpful to see for transparency purposes, which I know is one of the reasons why you have rolled out body-worn video. The same goes also for local authorities using body-worn video. It would be very helpful to actually be able to see how, why, when. Local authorities retain body-worn video footage for much longer than the 31 days in some cases, so that is worth looking at further. We have two reports on the Big Brother Watch website you can look at about that.

With regards to facial recognition technology, we are profoundly concerned about what is going on and we have just released a campaign called FaceOff, calling for - just as the Biometrics Commissioner called for in his report yesterday - the automatic deletion of innocent people, that is unconvicted people's custody images and subsequent facial biometrics that have been made, of which we now know, thanks to yesterday's annual report of the Biometrics Commissioner, is over 16.5 million images. If you are innocent, you should not be held on a database. Your deoxyribonucleic acid (DNA) and your fingerprints are automatically deleted, thanks to the Protection of Freedoms Act, but the Government, which was required to respond to the retention of custody images, took five years to respond to the High Court and then came back saying, "They are quite helpful. We do not think your face is that sensitive. We suggest that people write and request removal and it is at the police's discretion as to whether that is going to happen further". We think that that is unacceptable and we would like to see the Home Office policy change, legislation change so that automatic deletion of innocent people's photos now becomes law.

With regards to the use of the trial of technology at Notting Hill, I just put on the record that Big Brother Watch was consulted about that, with one meeting last year. We have had no further consultation with the MPS. We saw no findings of the trial last year. We were not told in advance of this year's trial and we certainly object to any indication in the press that we signed off on this or gave our approval. It is not for an organisation such as Big Brother Watch to do that; it is for Parliament.

The final point is that the Home Office have promised for almost five years the publication of its biometric strategy. We are waiting still. That has not happened. We therefore do not have any oversight, legislation, regulation or scrutiny of any of the biometric technologies, namely facial recognition going ahead, yet we do know that the Home Office are offering investment of over £5 million for the creation of facial recognition technologies by police forces across the country. We think this needs to be addressed urgently.

Sian Berry AM: Thank you.

Javier Ruiz (Policy Director, Open Rights Group): Chairman, there is little to add. You will find that pretty much most civil liberties and technology groups in the UK right now would agree with the analysis and actually are preparing to mobilise. We did run a small campaign at the time of Notting Hill Carnival ourselves.

In terms of what else could be said is that actually apart from being a really expensive technology and it is something that has public expenditure, it is something that should be submitted to some evidence that it works. The evidence from the United States (US) is actually that it is quite mixed and it would be important to understand actually how much of this works. Particularly there are concerns around racial discrimination, both in the over-representation of ethnic minorities in police databases, not actually on the capacity of the technology to identify non-white faces. Those things definitely should be addressed. In the concept, US researchers are describing the widespread use of facial recognition as compared to a line-up, where every single person that walks down the street is now put in the line-up, you walk in and one person in the line is the potential criminal and everyone else is innocent. The understanding is that now as we walk down the street, we are going to be in a perpetual line-up and we find that deeply disturbing.

The other area of technology where we also have some concerns would be road pricing. I do not know if you were planning to discuss it here, but pretty much everyone right now shares the concerns both about the traffic pollution, the amount of traffic on the streets. We looked at the *London Stalling* report from the Assembly and what they found is that there is very little detail on how it could work and very little detail particularly when it comes to privacy and civil liberties, which is actually literally one line at the bottom saying that they did not think it should be looked at. This is one of the areas where if you can make it work, it would be amazing to make it work without tracking every single car in London. It is going to be incredibly difficult and the privacy and civil liberties concerns should be a much, much larger part of any report or work on this area. There are some ideas being proposed, like the extensive use or more sophisticated use of ANPR with differential pricing and things like that. It would not involve tracking every single car through Global Positioning System (GPS), but ultimately it seems that the end game would be individual tracking and I think that of course would be quite difficult to make compatible with civil liberties. It may work at some point, but it is going to be hard.

Sian Berry AM: Yes. Like I say, as a former transport campaigner, I am aware the last time road pricing was talked about, this was one of the key public objections, it is one of the key risks to doing it. With GDPR in place, potentially it is very difficult to make those things match up. TfL, do you have anything to say how you are planning to do that?

Richard Bevins (Head of Information Governance, Transport for London): Yes, if I could come in there, we are very conscious that my team will need a lot of privacy input into thinking as it develops around road pricing. The fact that privacy is a huge concern around road pricing schemes as they have operated in the past is very well recognised and accepted within TfL. We will need to work through what the GDPR means and look at it in a different way and be very open about how we develop our thinking on that.

Javier Ruiz (Policy Director, Open Rights Group): If I may say, for us, in a case like this, you need to go beyond policies. With all due respect, the MPS, we find it very hard to believe that once that data is created it will not be accessed for other purposes other than tracking. You will need to really to bake into the technology systems that would make it almost irreversible. That will come at a cost, of course, because then someone will say, "Here is the terrorist that did this and we were not able to catch them because the data was encrypted", but the decision will have to be that at some point you are going to have a loss of utility on the data if you want to protect privacy. To say that you are going to go ahead and promise people you are going to protect the data from other secondary uses, five years down the line, no one working in this sector will believe that the protections will remain in place.

Dr Onkar Sahota AM: This is sort of summing up on what we have heard this afternoon. These questions are directed to Big Brother Watch, also the Commissioner and also to the Open Rights Group. Is there anything that you have heard this afternoon that concerns you or that you feel that you are glad you heard it?

Renate Samson (Chief Executive, Big Brother Watch): I just come back to the point that we do not understand what data is, really. We think we do, but we do not. Talk about general data, as I have already said, more often than not now means personal data or data that can be used to identify people in some way or their movements. I am very pleased with the work that has been done by TfL in relation to the wi-fi scheme and the genuine attempt to bake in privacy, privacy by design, as Elizabeth Denham mentioned, and the approach to informing to the public. It is a good start and it is a start that I would really recommend that everybody take something from, particularly with regards to the Data for London strategy. It is the absolute, from my view, polar opposite of the Data for London strategy, which is, frankly, incredibly poor and merely tips its hat at the idea of privacy and it has no mention of security. Overall, I think has been a really helpful

session. I hope you listen to what everybody has said and certainly inform yourselves more about the GDPR and the impact and the positive impact that data protection has on all UK citizens before and after Brexit.

Dr Onkar Sahota AM: Thank you. Javier [Ruiz]?

Javier Ruiz (Policy Director, Open Rights Group): Yes, it has been very useful. It also helped to understand a lot more how TfL and MPS work and their processes. For us, the things that we would say, going back to some of the points I made before, we would stress the need to go beyond strict data protection, particularly for a public body or for scrutiny, and elected Members of the Assembly to look at the wider ethical issues around data, what are the impacts of the policies and how data plays there, rather than just looking at strictly whether data protection is breached or not, important as that is. We are looking at the impact of data in society. Nowadays it goes beyond strict breaches or the negative aspects and we would look at ethics that go beyond the principle of doing no harm, but actually using data in a positive way to actually do good, rather than just do not do bad things.

The second thing is that we find again, going back to what Renate was saying, there is data protection and GDPR has got this principle of data protection by design. One strong element there is minimisation, data minimisation, and we talk about the minimum viable data. In many cases what we find is that the opposite approach is taken, they say, "Let us see how much data we can get and later on we will see what can be done with it". We think that the principle should be the opposite - and actually, the law says that the principle should be the opposite - and you should say, "Do we really need this data? If we do not need it, let us not use it".

The final point, going back again to the data strategy, we also found it quite poor that strategy theme 4 around public acceptance contained almost no real actions but was all relying on external support for data protection, whether it is then Digital Catapult or the Royal Society. We think London needs a much stronger force for privacy and they need a data protection officer, but not just a person or a tick-box exercise to comply with GDPR, but to start embedding privacy and data protection into the processes in a much stronger way than what is there.

Dr Onkar Sahota AM: Thank you. Commissioner?

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): I can echo some of those thoughts. Data protection is not a tick-box exercise. If GDPR is read properly, then it is about three things. It is about transparency and that connects you with the trust that citizens have in your organisation. It is about more control for individuals so that they can take back agency when it comes to the use of personal information. Lastly - and one of my colleagues said this around the table - the biggest change in the GDPR is around accountability and what that means is there has to be structure and roles and responsibility and tracking your data, knowing where your data is, privacy by design, mandatory data protection impact assessments and mandatory recording.

All this is about gaining the trust of citizens and customers in organisations that process their data. This used to be, this discussion that we are having today, 10 years ago, a back-room issue. Today it is a frontpage, frontline issue, and if you want to - put the law aside - have the social licence to continue to use data, then you have to demonstrate that to citizens, because it is really easy to lose trust with shiny new technologies and the growing appetite for big data. The GDPR and the focus that it provides means that this is a chance to change the culture in the organisation and get this right. That is going to give you the ability to say you have got the trust and say what you are going to do, do what you say and then be prepared to demonstrate it. That is really what the GDPR is all about.

Thank you very much for inviting me to the discussion today. I really enjoyed it.

Dr Onkar Sahota AM: What opportunities and risks should the Assembly be aware of over the next few years? What sort of things can we, as scrutiny, elected officials, be aware of on behalf of Londoners?

Elizabeth Denham (Information Commissioner, Information Commissioner's Office): First off, somebody mentioned who is the data protection officer. There will need to be a data protection officer and you have to make sure that that person is in place. What is the governance for data protection in organisations that you oversee, and this Committee in particular? What about data protection audits? Is there a plan for them? Are you going to see them? You want to see the progress that is being made on data protection implementation, because at the end of the day, it is all about the citizen. That is what it is about and that is your role as legislators.

Javier Ruiz (Policy Director, Open Rights Group): Yes, just to make a couple of additions. I agree with Elizabeth [Denham]. There is also in the UK the Digital Economy Act, which will create new powers for data-sharing that will obviously give an opportunity, as it was designed to minimise some of the friction involving creating new data-sharing agreements. Some of the functions of the MPS will be completely outside of the digital economy, but when it comes to public services, it will easier to create some data-sharing agreements to share data. Now, obviously that also creates risks and something that we would want to understand a bit more is how the new powers will work with some areas of the GDPR which forces any legislation that allows data-sharing to be a lot more detailed than it was until now. We think that again it is an opportunity, but it is also a risk for any new data agreements. Even if it looks that it is easier to put them in place right now, they still need to have safeguards, they still need to be limited, proportionate. We would also say time limited, so that will be an important thing.

In terms of technologies, you have covered some of the discussion, but I think everything we have seen now will continue to accelerate. Something that we are seeing with concern, for example, is some of the centralisation of data. We have looked at how Camden has built this citizen index, where basically they built one single database, where every single organisation from all the residents is put in one single system. That raises concerns, both from the point of view of security, but also from the point of view of privacy more broadly, despite the assurances as to the limitations they have in terms of access control. We think that any idea about centralising data and building big data systems will create new risks and they should be examined quite carefully.

Dr Onkar Sahota AM: Renate [Samson]?

Renate Samson (Chief Executive, Big Brother Watch): To reiterate something I have said repeatedly, we have to understand that protecting the citizen is not just protecting our physical wellbeing, it is protecting our data, be that by installing and properly not breaking or undermining encryption, ensuring that policing for the 21st century is not a case of investing lots of money in technology that actually is not proven to be of any great value. Do not forget, we were promised that CCTV would remove crime from our streets. It has not done that. It has become a tool to investigate crime that has already happened, and whilst that brings great value, do not make promises that do not stand up. If the promises change, be open and honest about them.

Also, we need to be very aware that big data is not the solution to everybody's problem. Good data is very helpful. Accurate data and minimal data often will help you provide greater solutions than hoovering up everything. In summary, really that is a case of, as Elizabeth [Denham] said, protecting the citizen and that means protecting citizens' data.

Dr Onkar Sahota AM: Thank you. All right, I will hand it back to the Chair.

Len Duvall AM (Chair): Thank you very much. Can I thank you all for the way that you have answered the questions? We need to deliberate on what you have said, but there are a couple of things that we need to decide now as a course of action. Caroline Pidgeon [MBE AM] is attending this meeting, but also we have Keith Prince [AM] from the Transport Committee. It is quite clear we should keep some scrutiny focus on this issue in relation to TfL and the same should be for policing and crime at some stage if we are going to keep the process there that people are on top of. Can we give some thinking about that, about how best we do it? We of course have rightly focused on our responsibilities in the GLA Group, but it does say to me there is a whole other world out there from the private sector onwards that we should use our scrutiny voice to help and support not just the people that want to do the right thing, but anyone who thinks they are doing the wrong thing about that.

Maybe the Economy [Committee] should try to look at how do we influence some of the business interest, the collective groups, the Chamber, London First. How do we make sure, and much that there is legislation out there and that message is wider, we just need to keep the focus, because I was very much taken by what you said, Elizabeth [Denham]. Ten years ago this would have been a private conversation and very much a tick-box, "We have to do this", or whatever. It actually goes to the heart of citizenship and the rights of citizens and how we operate within our society and what we want. As public organisations, we will make mistakes. I like to think we would not abuse or seek to undermine those legislations and we want to minimise those mistakes, where possible, and guard against those issues. We will only get that right if we get some of the commissioning right and some of the thinking about what we are trying to achieve with the data that we hold. It is fundamentally the relationship with our citizens.

If we could, under a power, I would suggest that the London boroughs should be having one of these meetings about their own areas but, alas, we do not have that. Certainly, we should encourage and share this information because we should promote our work within London boroughs to say, "If you have a scrutiny plan and you think there are some issues that you are not quite sure about, this is one worth looking at locally in your area with the NHS trust", and all the rest of it. We should do that. I feel we are going to have a letter to the Mayor at some stage around this. I do not think we need another session, but we do need to think about how we try to build this into some routine scrutiny.

Sian Berry AM: Just to suggest that we also send what we write to the new Chief Digital Officer for London, who possibly has not been recruited on the basis of keeping an eye on this area, but may be somebody we could ask to look at it.

Len Duvall AM (Chair): Of course it is a Mayor's creature and I am all in favour, as people know, of the Mayor's policies and decisions. It is wider than that individual.

Sian Berry AM: No, it is.

Len Duvall AM (Chair): It is something that we ought to look at and I am looking for the Head of Paid Service around some of those issues about how professional officers act appropriately and take their responsibilities seriously, rather than one. We will look at that and see what the role is.

Sian Berry AM: I definitely say write to the Mayor.

Len Duvall AM (Chair): I am not sure if that role is envisaged as what we would envisage it as. The Mayor has a different version for that job, but let us look at that and examine that further and see if we can continue to make a difference. Yes, we will look at that. Thank you again. Once again, thank you very much for the way you have answered the questions.

Tom Middleton (Head of Finance and Governance, Greater London Authority): There is a role for audit as well, as the Commissioner said.

Len Duvall AM (Chair): That is very good. We will try to draw that together as we look at what you have said to us as well. Thank you.

This page is intentionally left blank