Speech: Speech to the annual data privacy conference

I'm delighted to be speaking at this event hosted by Taylor Wessing today. From the very start of my Commission as an independent regulator this law firm has been a good friend to my offices particularly in supporting my knowledge and understanding of the world of data protection and its application to video surveillance camera systems. Indeed you hosted my first ever webinar regarding surveillance camera systems. I thank you for that enduring friendship and acknowledge the calibre of your offices.

In the context of regulating surveillance camera systems am going to tell you a little about my role and regulatory interests, provide a synopsis of my views as to the regulatory framework and discuss a new paradigm.

I am mindful that I am amongst a host of data protection experts today, however what I really want to talk to you about is a subject which I consider to be the key issue occupying my regulatory focus, namely the growing capabilities and appetite for use of increasingly intrusive technologies integrated with surveillance camera systems in society. Of course data protection is a significant element of this subject but it is a much broader consideration than data protection alone.

For over six months now I have been endeavouring to energise engagement, discussion and debate on this matter with, amongst others, the Home Office, Government Ministers, the National Police Chief's Council, police forces, civil libertarians, the public and indeed fellow regulators. It is a matter which is gathering momentum in the public consciousness and I will continue to encourage debate and engagement as I believe that doing so will be a catalyst for change in support of public interest. The public interest which demands clear legislation, transparency in governance and approach and a coherent and effective regulatory framework in which they can have confidence.

Let me use the example of Automated Facial Recognition, or AFR as it is referred to, as an illustration. When I launched my National Surveillance Camera Strategy just over a year ago I engaged with a broad spectrum of stakeholders including police, public and privacy campaigners to better understand the divergence of opinion around its use. In the case of Liberty the message I received was; "…we are deeply concerned by the lack of progress on securing any form of independent oversight of the use of AFR -particularly used by LE (Law Enforcement Agencies).

I agree.

Then consider the view of the eminent David Anderson QC, formerly the Government's independent reviewer of counter terrorism legislation who said; "either you think technology has presented us with strong powers that the government should use with equally strong safeguards or you believe this

technology is so scary we should pretend its not there. And I firmly believe in the first category not because I say government is to be trusted but instead because in a mature democracy such as this one we're capable of constructing safeguards that are good enough for the benefits to outweigh the disadvantages.

I agree.

David has a sharp mind -let me tell you about a programmed use of AFR in China called 'Sharp Eyes' as an insight as to where the use of intrusive surveillance technologies can lead. Sharp Eyes -Xue Liang – Chongqing -the future?

This is a capability developing in China which connects security cameras with AFR that scans roads, shopping malls and transport hubs. It can connect to private and compound cameras and buildings and integrate then into one nationwide surveillance platform. This capability is backed up with a police cloud scooping up information of citizens, be it criminal, medical, commercial, socio -demographic upheaval and political unrest. Indeed the police commander Chongqing said; " With AFR we can recognise strangers, analyse their entry and exit points, see who spends the night there and how many times'.

As you may know I have a background in strategic leadership in the field of counter terror-ism. I consider this to be a nightmare scenario where the will of a totalitarian state continues its intrusive evolution through technology, seemingly unhindered by any regard to the will of the people or mechanisms to keep things in check.

That of course is China -it will not happen here will it? But could it? Only last month I wrote to Chief Constable Sarah Thornton, chair of the National Police Chief's Council formally bringing to her attention my concerns regarding discussions in police circles about bringing together public space video surveillance camera systems and integrating them for police use. There are aspects of these proposals which for me resonate with 'Operation Cham-pion' – a police initiative to erect a ring of ANPR cameras around a predominantly Muslim community under the guise of 'Crime Prevention' -when the larger intent was to support counter terrorism policing. The public outcry which followed in that particular case ensured that the cameras were never switched on.

But first, my role.

I thought it might be useful if I give you a little background about my role as Surveillance Camera Commissioner. It was created under the Protection of Freedoms Act 2012. I was appointed by the Home Secretary but am independent from Government. My commission was extended for a further term of three years as recently as last March. I'm entrusted to ensure that surveillance camera systems are used to support and protect communities – not spy on them. My primary focus is the overt use of surveillance cameras in public places by relevant authorities as defined in the legislation, in England and Wales by statutory mandate and indeed this extends to any organization operating such

systems in encouraging them to voluntarily adopt the Code which I oversee. The Code in question is the Surveillance Camera Code of Practice which is issued by the Secretary of State and contains 12 guiding principles which if followed will mean cameras are only ever used proportionately, transparently and effectively. Typically surveillance cameras falling within my purview include CCTV, ANPR, body worn cameras, drone and helicopter mounted cameras, dashboard cameras and analytic systems, reference systems, automatic facial systems etc.

It is very important that I make it clear that in publishing the Secretary of State's Code, the use of evolving technologies in society was foreseen by Government and indeed the use of facial recognition systems explicitly referenced within its pages. Those of you familiar with the content of the Code will of course know that the Code sets out that such technologies will be regulated by it and paragraph 3.2.3 makes it clear that the use of such systems must be validated, and that I am a source of advice on validation. You will understand therefore my enduring determination and commitment to ensure that this is debate which remains energized and to which I will remain central.

My statutory role is three fold, namely to encourage compliance with the code, review the operation of the code and in reviewing the impact of the Code, to advise on any amendments to how it should develop. Indeed I have recently made recommendations with regards to ANPR. My Annual Report was laid before Parliament only a few weeks ago. Chapter 5 of the SC Code describes how I may regulate.

Relevant Authorities are my key focus and they are essentially police, local authorities, Po-lice and Crime Commissioner's, National Crime Agency and non designated police forces. They all have 'a duty to have regard to the Code'.

The Code also touches on obligations of operators of surveillance camera systems under the provisions of the Data Protection Act and significantly paragraph 2.2 of the Secretary of State's Code provides that increasingly intrusive technologies when used as part of a surveillance camera system must be regulated by the Code. The guiding principles within the Code also specifically refer to areas where I must engage with new technology.

You may be forgiven for asking why AFR is considered as a video surveillance system at all when it is in fact merely a biometric algorithm. The answer lies in Section 29(6) Protection of Freedoms Act 2012 which defines the surveillance camera systems of my focus as being CCTV, ANPR, any other system for recording or viewing visual images for surveillance purposes, any systems for storing, receiving, transmitting, processing or checking images or information obtained by those systems, and, wait for it, any other systems associated with, or otherwise connected with those systems. Integrated technologies!

My journey with technology thus far reaches back to 2014 when AFR was a little more than a mere pixel in the eye of the motherboard. In 2015 when 'Slipknot and Muse ' should have been making headlines for their musical calibre at the Download Festival it was Leicestershire Police who instead

grabbed the headlines due to public concerns about their use of AFR at this event. Why? Well concerns included an absence of clarity as to the legal basis for its use, limited transparency and civil engagement, the credentials of the equipment being used, the database of images involved, where was regulatory over-sight and who said it was ok to use it and on what basis?

The Metropolitan Police made use of AFR at the Notting Hill Carnival in 2016. This too attracted concerns because the results of the deployment were not published, and concerns were raised regarding engagement, legality, reliability of equipment being used, the image database, evaluation and governance. They repeated this exercise in 2017 and whilst concerns remain, they reached out to regulators for guidance and completed my Self Assessment tool and a DPIA issued by the ICO.

South Wales Police employ AFR and have used it at major sporting events. They have worked hard to engage stakeholders, the Home Office, regulators and the public and have ensured strategic governance and independent consultation.

Let me make it clear, I think that the police are genuinely doing their best with AFR in what I consider to be an absence of a sufficiently robust legal and regulatory framework. It is inescapable that AFR capabilities can be an aid to public safety particularly from terrorist threats in crowded or highly populated places. It is inevitable therefore that there is an appetite particularly within law enforcement to exploit these capabilities, an appetite which is doubtlessly borne out of a sense of duty and determination to keep us safe. Many of those technologies such as Automated Facial Recognition already exist in society for our convenience and therefore the public will have something of an expectation that those technologies are so used by agents of the state, but only in circumstances which are lawful, ethical proportionate and transparent. But by the same measure the public also need to be safe from disproportionate and illegitimate state intrusion. The challenge is arriving at a balance and for that to happen there need to be a clear framework of legitimacy and transparency which guides the state, holds it to account where necessary and delivers confidence and security amongst the public. I don’t believe we are there yet. I don’t believe that GDPR and new data protection legislation in isolation takes us there either.

Let’s now consider areas outside of the state. In 2015 a survey conducted by the Computer Services Group found that 25% of retailers use AFR including 59% of fashion retailers. There was a total absence of signage, a priority data protection consideration.

A review of 28 High Street Retailers found that only John Lewis, Waitrose and Monsoon declared that their use of CCTV was for ‘more than crime purposes’.

Demonstrating compliance with legislation which governs the use of surveillance camera systems is a good place to start when it comes to engendering the trust and confidence of the public you are looking at through your cameras. The Surveillance Camera Code of Practice provides a whole system approach to standards of operation and the ICO Code for operators of surveillance camera systems ‘In the Picture’ enables compliance with data protection responsibilities. Is this enough where overt surveillance using

new technologies is concerned? I don't think so.

Let's look at another widely used technology, Automated Number Plate Recognition (ANPR), which in the context of effective governance and regulation has parallels with AFR. "The Face ain't dissimilar to the Number Plate".

ANPR is arguably the largest non- military data base in UK collecting up to 40million reads of innocent citizens number plates a day and upwards of 30 billion reads a year. It harnesses personal information and enables data mining of immense personal invasion across the UK. There is no statutory footing for ANPR although a legal framework sup-ports some of it. It is capable of providing misinformation as a result of irregular, cloned or defective plates and vulnerable to fraud. It has an error rate of 3 % in National Standards – 1.2 million reads a day!

I have led the regulatory debate on these issues with the police and Home Office for a number of years particularly in respect of the issue of data accuracy. The police response has been magnificent, culminating in asking me to establish and chair the National Independent ANPR Independent Advisory Group which comprises academics , privacy specialists , ICO, motor industry specialists etc.

Unlike ANPR, there are no national standards in place regarding AFR and central coordination within the NPCC is still evolving. The Home Office continues to fail to deliver a Bio-metric Strategy despite promises over last 4 years. A Home Office custody image policy has been produced which is arguably an improvement on the previous position but in my view still falls well short of fully respecting privacy rights.

So what have I been doing about this issue? I have written to the NPCC lead for surveillance camera systems, ACC Tim Jacques urging better strategic governance and suggesting that the College of Policing help design standards. I have written to all Chief Officers in England and Wales reminding them of their responsibilities and my role under PoFA, I have written to the Chair of the NPCC and to the Minister of Policing setting out my observations. I have met with other regulators and discussed areas of potential synergy, visited police trials in South Wales, the Metropolitan Police and the NEC, presented at numerous forums including the Police and Ethics Board in London and engaged with HMIC and the Crown Prosecution Service and even held a public engagement 'Question Time' event at the London School of Economics to engage public opinion and debate with a panel of experts from across the civil spectrum. In that regard, there is more to come.

Is the current and anticipated regulatory framework fit for the purpose of regulating technologically advanced surveillance camera systems in public? Well let's look at our regulatory fingers in the surveillance camera pie!

Can anyone tell me the collective noun for a group of regulators in that respect? How about 'a murder of regulators?' as you can be forgiven for thinking that is what we are doing to the subject matter at hand.

Firstly, the ICO – AFR relies on cameras and produces data – the ICO have a very clear strategic role in regulating the management and privacy of personal data- GDPR is coming over the horizon and Jonathan Bamford (ICO) has already talked about the new requirements – DPIA, Consent, Sensitive subject material It needs to be relevant and made relevant? The fine should help there! Data is the new oil and it will be interesting to see how the new requirements will be precisely policed? The ICO is developing fabulous guidance to help with what is an increasingly complex framework. It is only part of the regulatory picture however.

The Biometric Commissioner; One senses this title must have responsibility for this field, it makes good sense as Paul Wiles is the leading regulatory ambassador for ethical standards in the use of biometric capabilities –but in statute he bizarrely has no mandate where AFR is concerned. Paul has been and continues to be a strong advocate for a more ethical approach to the use of custody images and has like me, made repeated calls for the production of a government Biometric Strategy.

The Forensic Science Regulator very clearly sets and regulates the standards of digital forensics to ensure that the public interest is appropriately served by standards of evidential and procedural integrity in cases where judicial proceedings involve the use of digital images.

The Investigatory Powers Commissioners Office (IPCO), that very powerful and impressive UK privacy regulator in the field of data capture across a wide spectrum of covert techniques. Now in the covert domain the regulatory regime for covert surveillance is clear and unequivocal and in my view reassuring.

There is a clear basis in law for covert surveillance to be conducted provided by the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016. There is provisions for independent judicial oversight and approval, there is a clear regulatory framework within the relevant legislation which prescribes governance in so far as authorisation levels for covert surveillance activity is concerned and the key principles to be considered and recorded within specified timescales to ensure constant review. There is an inspection regime which scrutinises compliance in respect of every public authority which has powers vested in it to conduct covert surveillance which results in reports and recommendations being considered by senior officers and judicial figures alike. That is a regime which has stood the test of time – 17 years, and is necessary because of the degree of intrusion which covert surveillance causes and the use of technologies involved.

But arguably, overt surveillance is becoming increasingly intrusive on the privacy of citizens and in some cases more so than aspects of covert surveillance because of the evolving capabilities of emerging technologies. It may be AFR today but what about augmented reality, gait analysis, behavioural analysis, lip reading technology and whatever else may be around the corner?

Technology can enable OVERT surveillance camera systems to harvest an exceptionally detailed picture of your PRIVATE and personal information, in

some cases far better than a surveillance officer covertly following you to the supermarket. But my point is this; – there is a clear legal and regulatory framework to underpin covert surveillance. There is a more complex legal framework which underpins overt surveillance activity which includes Common Law, DPA, PofFA FoI, Counter Terrorism Act 2008 and others.

Whereas the new GDPR and DPA provisions and proposals will undoubtedly provide a more comprehensive basis in law for the management of personal data, overt surveillance is a wider legal consideration of which GDPR and DPA is an element but not the all. The academics and civil libertarians who sit on my advisory group would be happy to have the debate with anyone here who has a differing view. Fortunately my role is to apply balance.

A new paradigm

I made it clear in my recent Annual Report that I believe the current regulatory framework is not fit to manage the challenges emerging from new surveillance technologies in society. My role has drawn me through the camera lenses and in to the back office artificial intelligence systems in the preceding five years.

I launched a National Surveillance Camera Strategy in March last year- One strand of this strategy is that of Citizen Engagement and a programme of public engagement and de-bate has begun. I joined Big Brother Watch, the police, a member of the House of Lords, an academic and a Channel 4 correspondent on a panel to discuss these issues with an audience in a lively event at the London School of Economics.

How does society maximise the use of new technology without creating a creepy, oppressive breach of our fundamental freedoms? More importantly what is government doing about it, or at least, what's the plan? Is it right to say to our emergency services, don't de-ploy technology that can save lives as the government isn't ready yet, any more than it is to say you can be as intrusive as you like in deploying what are essentially biometric check points where your face is your ID card?

I do think regulators can work closer on these matters in bringing the debate to deliver tangible outcomes to benefit the public interest. Threats to society and threats to civil liber-ties are of equal magnitude these days and becoming increasingly complex. It is simply not satisfactory to expect law enforcement, emergency agencies and the public to 'just get on with it'. In the context of surveillance in society, voices who shout 'you should' or you shouldn't' resonate with equal conviction.

My view has consistently been that to establish a true balance regulators need to work closer together and Government needs to engage far better than has hitherto been the case. Most importantly there needs to be a constant heartbeat of constructive and mature challenge and debate from the citizens of this country who are ultimately on the other end of the camera lenses and its intrusive capabilities. The public voice is the lifeblood of change and progress to the greater good. We need to listen, to understand and to act sensibly and the 'we' includes government.