Biometrics and Surveillance Camera Commissioner speech at the National ANPR Conference 29 November 2021

Thank you for your kind invitation to this key event which addresses one of the most critical aspects of policing surveillance technology. I'm Fraser Sampson and I'm the – no longer quite so new – Surveillance Camera Commissioner having replaced Tony Porter in March. I'm also the Biometrics Commissioner having also replaced Paul Wiles in March. The government is planning to simplify the arrangements for oversight and regulation in this area and so to that extent at least I am the walking embodiment of simplification – 2 commissioners in one pair of shoes.

When considering the sprawling issues covered by these roles I usually look at them from 3 vantage points: the technological (what's possible) the legal (what's permissible) and the societal (what's acceptable). And while the technology often gets a lot of the 'look what they can do now' headlines I'm going to focus on the combined effect of the technological, legal and societal developments. Now these aren't discrete categories and they overlap in many areas – but they're helpful in framing some of the issues in what is a very fast moving and increasingly complex area.

Let's start with the law. Lawyers love a definition so how about this one:- "A critical system, the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life." You may recognise that as the government's definition of our Critical National Infrastructure.

Transport is of course one of the wider areas but does our ANPR capability meet the definition all by itself?
A "critical system"? In terms of Its contribution to overt and covert investigations, traffic monitoring, vehicle safety, safeguarding, disrupting organised crime, counter-terrorism ….. unarguable I think. Would the loss or compromise of the National ANPR system result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life?

The NASPLE Document (at 8.9.7.) makes provision for what it describes as "the unlikely event that connections to the National ANPR System are unavailable for more than 7 days". What would happen if the system itself was unavailable to the police for 7 hours or even 7 minutes? It would be like switching off the internet. It wouldn't just be an unlikely event – it would be unthinkable.

Perhaps wait until the end of the conference but I believe that each of the speakers from whom you will hear are witnesses whose evidence will corroborate my proposition that ANPR is now part of our CNI.

If it is part of our critical national infrastructure – and it is unquestionably part of our Critical Policing Infrastructure – shouldn't it have an express legal basis? The lawyers will know why it should but let's shift vantage points for a moment and look at ANPR from a citizen's perspective.

Wouldn't the person on – or even driving – the famous Clapham omnibus expect to be able to look up such an intrusive tool and its parameters in an act of Parliament with all the express enabling sections, limitations and safeguards which have been the product of democratic scrutiny?

Pity the poor motorist who begins a quest to find out who can look at their ANPR data and for what purposes. It's a perfectly reasonable Q for them to ask. But try to plot their journey through the GDPR and Law Enforcement Directive, the Data Protection Act, the Regulation of Investigatory Powers Act, the Protection of Freedoms Act – eventually arriving at the NASPLE document – consider their epic journey through our current regulatory landscape and the case for greater legal clarity and consolidation is made out from the citizen's perspective too. You could of course begin the journey at the NASPLE document but I fear many would never arrive at their destination.

The Societal perspective – what's acceptable to people whether it's legally permissible or not – is where the future of biometric surveillance is being shaped across the world. The evidence for that proposition is set out in my formal responses to recent government consultations and we ignore it at our peril.

ANPR is a well-established form of surveillance – The fact that it's established is important – because people have grown up with it and to an extent have so far – generally – trusted its use – or at least haven't been as worried about its misuse as some newer surveillance capability – In that respect ANPR is a bit like old school Closed Circuit TV – but there is nothing closed about our surveillance systems anymore – in fact their adaptability and scaleability is one of their strengths. Technological capability means that – like other forms of surveillance – ANPR can now do far more than it was originally designed to do. Increasingly it's able to capture non-vehicular data, monitoring people, their behaviour, associations, networks and habits – not just the driver but occupants. Which means it's increasingly difficult to separate its output from the mass of aggregated surveillance data. This is important both for the legal perspective and also the societal one.

In terms of the law, the revised Surveillance Camera Code provides – at 1.3 – "A surveillance camera system should only be used in a public place for the specific purpose or purposes it was established to address. It should not be used for other purposes that would not have justified its establishment in the first place." – that's an interesting test. – partly because people's attitudes and awareness have changed. When looking at increasing the functionality of ANPR in the future ask yourself whether this new purpose would have justified its establishment at the outset.

It goes on to provide that “Any proposed extension to the purposes for which a system was established and images and information are collected should be subject to consultation before any decision is taken. When using surveillance systems, you can only use the data for a new purpose if either this is compatible with your original purpose, you get consent from individuals, or you have a clear obligation or function set out in law”.

In terms of what’s acceptable, since this audience last met there have been some very specific policing issues arising from the exigencies of the COVID 19 pandemic. Aside from the relationships between communities and their police where there has been a blurring of law enforcement and health enforcement, the use of ANPR to identify potential breaches of lockdown arrangements has attracted criticism in some areas – how has that been received more broadly by our communities? We should probably find out. The exigencies of the COVID pandemic required temporary, emergency measures and it is critical to ensure that they were exactly that – temporary and used only to the extent necessary to counter the threat at the time. I’ve reported to Parliament on this in the very specific context of National Security Determinations but I think there’s a much wider need to assure ourselves that we’re not living – as if in a constant state of emergency. Temporary structures can become very convenient particularly when the demands of the day job are unrelenting and they can quickly become a permanent fixture – ask anyone who’s worked in a Portakabin.

But the risk of permanent and irreversible incursion by the state during times of emergency is well documented and one of our many challenges now will be to ensure that the balance between responsible intrusion, accountable regulation and societal expectation is resumed. I think this will be particularly important in retaining public support for the use of ANPR.

Aside from the emergency provisions, integrated surveillance solutions themselves bring their own challenges. Will people still be as accepting of ANPR once it can recognise the occupants of a moving vehicle, identifying their children, when and where they got their flu jabs, their passport and if they’ve paid their tax bill?

Integration can bring new ethical considerations too. I spoke recently at a security conference where a former intelligence officer asked why Hikvision routinely fitted ANPR capability in all of its CCTV cameras sold in the UK. I don’t know the answer and to be fair to them they weren’t present to answer my questions either. But Parliament has heard how their surveillance systems are facilitating human rights atrocities against Uyghur Muslims in Northern China. How comfortable would policing professionals be in teaming up with a company that is capable of doing that? How much of their money would your local communities like to see spent on contributing to the profits of those companies? The more intrusive your technological capability, the more careful you need to be about who you partner up with.

Back to the permissible and the acceptable – Proportionality is a key legal concept as we know and it’s a relative concept – the greater the anticipated harm the more room for intrusive tactics. When stacked up against the global threat of a pandemic, “local law enforcement tactics” can suddenly become

“proportionate” in a way previously only seen in high harm criminality such as terrorism or even national security. When measured in terms of the enormity of the overall global threat the citizen’s individual expectation of privacy can be easily overridden – but is that really a legitimate comparator?

If it is, how about the end of the world? Literally – that’s what climate change and the COP26 risks are ultimately about. Does that mean the State can use whatever methods it likes in the name of combatting climate change because nothing is comparable to the enormity of the overall threat? If so, using ANPR to enforce low emission zones is a breeze and the privacy of the individual citizen will be easily blown away.

In such a fast-moving and unpredictable area as biometrics and surveillance, identifying and balancing what is technologically possible with what is legally permissible and societally acceptable is as good a starting point as I can come up with.

In terms of the possible – Large volumes of valuable data can now be merged quickly and easily with datasets from a wide variety of other sources including surveillance camera systems – publicly and privately owned – with greater accuracy and specificity. The clear bright line beyond which this becomes Directed surveillance is perhaps becoming less clear and less bright than in the past but Technological developments in biometrics and surveillance have meant that our capability to prepare for, respond to and recover from global crises has increased beyond anything our forebears might have realistically imagined. Technological development means having fewer and larger aggregated databases which in turn means that – while they ought to reduce the likelihood of breaches – they potentially increase the impact of any such breach should it happen- and it probably will at some point

In terms of permissibility – The law should reflect the importance of this part of our Critical National Infrastructure. In the area of biometrics and surveillance the govt is committed to a strong legal framework and simplification. This area needs both strengthening and simplifying.

But the biggest risk to ANPR as I see it is societal – it’s that people withdraw their support for it. We are getting more used to surveillance and are installing our own personal systems – even ANPR – more readily and cheaply than ever before. But when it’s done by the State with all its apparatus of enforcement some feel wide scale surveillance is becoming highly questionable – especially as the Government doesn’t yet follow its own Surveillance Camera Code. Understanding public acceptability is a matter for your elected local policing bodies, knowing the views of your communities sits squarely in their job description – they are the voices and advocates of their communities in ensuring the style of policing fits with what is locally acceptable and we would do well to keep them at the centre of this critical discussion.

Look around at the regulatory framework within which we currently operate. GDPR, DPA, PoFA, … This wasn’t the product of some Eureka policy moment – it is largely the product of litigation and challenge, mainly by or on behalf of

the dissatisfied citizen, not just here but across the world. We've been sued into our current framework – surely it's better to design the next one in response to thoughtful and comprehensive consultation?

This is not just about ANPR – We need to be able to have confidence in the whole ecosystem of surveillance and be sure that what is technologically possible is only being done in a way that is both legally permissible and societally acceptable.

Thank you once again for your kind invitation and I hope you have a very productive conference.