Biometrics and Surveillance Camera Commissioner speech at NPCC CCTV Conference March 2022

CCTV

One of the ironies of surveillance is that it's such a fast-moving area it's hard to keep an eye on.

A year into my appointment I thought it might be helpful to highlight 4 themes from year, each is followed by a surveillance question for you:

Biometric Surveillance is not just data protection

David Fuller was convicted of two counts of murder at Maidstone Crown Court last December. Fuller reportedly videoed himself sexually abusing 100 corpses over a period of decades, from very young children to elderly women, retaining the images in his home.

DNA played a key role in the investigation but that's not why I've put him up here. Had he conducted a DPIA and followed policies for capturing and retaining sensitive personal data Fuller would have been 100% compliant with the letter of the law – because our DP only protects the living.

Fuller's conduct was just about the most egregious and intrusive imaginable, violating elemental levels of human dignity and respect. The trial judge told him: "Your actions go against everything that is right and humane". Indeed – but they don't go against GDPR.

There were calls for mandatory installation of CCTV in hospital mortuaries – but any DPIA would be the same and cameras wouldn't even be covered by the Surveillance Camera Code as they're not in public space and not operated by a 'relevant authority' (currently limited to the police and local authorities).

Biometric surveillance is not just data protection. If people think they're being watched or having their conversations listened to by the state and therefore decide not to speak, not to protest, not to meet up in public, not to travel – that effect on their fundamental human rights is profound but it's nothing to do with data protection.

What do Fuller's grotesqueries tell us about wider Human Rights? Well again the case raises some interesting questions – Art 3 ECHR for example creates an absolute right to be protected from inhumane and degrading treatment – including by the police. But again it only extends to the living – last year also saw a case of police officers taking photos of murder victims – hideous professional conduct issues yes, but a Human Rights Impact Assessment would have produced similar results to a DPIA.

Surveillance question – how far do your CCTV polices and practices assume that everything that matters is covered by data protection compliance?

Legitimate and accountable surveillance is about what's legally permissible yes, but increasingly it's about what's acceptable – to us as citizens and communities. In my view the point at which legality and acceptability converge is ethics – where we find the second key surveillance concept to dominate last year.

Xinjiang Surveillance

Most of our public bodies have ethics committees, ethics champions – the Policing Minister asked the House of Lords in January "aren't we the national ethics committee?" Some organisations even have strap lines about putting ethics at the heart of everything they do. In policing we know ethics is at the centre of the National Decision-Making Model and, according to the College of Policing, that means it's at the heart of all policing decisions – including presumably procurement.

These facilities spread across the Xinjiang Province in Northern China are designed, built and operated to deal with one group of people: Uyghur Muslims. In order to carry out their functions they rely heavily on surveillance, state-of-the-art surveillance, designed and sold by state-run surveillance companies.

Last December, giving the judgment of the Uyghur Tribunal, Sir Geoffrey Nice QC found that "Hundreds of thousands of Uyghurs – with some estimates well in excess of a million – have been detained and subjected to acts of unconscionable cruelty, depravity and inhumanity. Sometimes up to 50 have been detained in a cell of 22 square metres, observed at every moment by CCTV."

The judgment went on "Many of those detained have been tortured – detained men and women have been raped – one detainee was gang raped by policemen in front of an audience of a hundred people all forced to watch [while others] were raped by men paying to be allowed into the detention centre for the purpose."

Not everyone agrees with me, but I think this raises some ethical questions. Let's pause and look at a few.

You wouldn't employ an individual surveillance operator who had designed, built and worked in one of these appalling places so why would you employ a company that designed, built and operated them?

How much public money is it ethical to contribute to the design, building and operation of these facilities? How much tax revenue should we hand to the surveillance companies that are owned and controlled by the same State which the Tribunal found to have been directly responsible for genocide using their

surveillance technology to perpetrate it? How is partnering with such companies and enriching their owners “putting ethics at the heart of everything we do”?

Many public authorities have bought and installed surveillance systems from such companies – largely, it seems to me, on the basis that the cameras offer “value for money”. Well, I suppose it’s an exchange of values for money – but that isn’t quite the same thing and there are different ways of counting cost. I’d like to know from those authorities “how does this sit with the professional and personal ethics of your own officers and staff? Have you asked them?”

It’s interesting how our supermarkets have been very successful at driving improvements in animal welfare. By insisting suppliers meet minimum standards in relation to the humane treatment of animals the retail sector has made ethics a condition of entry to that market. Next time you’re in a supermarket you might want to look up and check whose camera system is monitoring your every moment – and then reflect on the ethics of having commercial contracts which properly include very high standards for the supplier’s treatment of free-range hens but absolutely nothing about human rights abuses. This seems somewhat asymmetrical.

And this isn’t about product boycotting – the bigger point here is that the systemic nature of our surveillance capability means people need to have trust and confidence in all of it – not just in the police or public bit, but in the whole ecosystem of surveillance. And that means we have to be more vigilant if we’re to maintain public trust for our own State surveillance. We need to be careful whose corporate company we keep. Lawful, ethical, publicly-acceptable surveillance needs a systemic approach – and a systemic approach means focusing on the integrity – of the surveillance systems and practice as a whole – and the standards of everything and everyone in it. Because, in a systemic setting, if you infect one part, you infect the whole.

Surveillance question – How far do your surveillance partners reflect your professional code of ethics and your own professional values?

The past year has shown as never before that what’s acceptable to the citizen matters – not just here but globally. And what’s acceptable to the citizen is changing – so too is your surveillance relationship. This has been understood by a celebrated son of this great city we’re in today, someone who’s arguably done more to promote discussion of contemporary public issues than most – of course I’m talking about Banksy.

Banksy

The headline behind this slide is “terminally ill dad arrested by 6 police officers for mooning at a speed camera.”

Darrell Meekcom, 55, reportedly protested against a speed camera in

Kidderminster last year. His wife and carer conducted her own surveillance and filmed officers wrestling the terminally ill man to the ground and handcuffing him. Footage of the incident went viral. Shortly afterwards this mural appeared in his home town.

Whether this was the real Banksy or one of his followers as rumoured doesn't matter – this story provides a powerful illustration of a few surveillance issues:

- Not all public space surveillance is welcomed – the COVID 19 pandemic provided some very good examples last year – the public reaction to it can be instant and enduring.

- The "surveillance relationship" between the police and the citizen means that the citizen is often surveilling you, sharing images at a speed and scale we'd never have imagined a decade ago.

- In addition, the police and public services are increasingly dependent on citizen-generated images from a whole range of devices and sources.

The first public communication from many police forces now is often an appeal, not 'for witnesses' but for surveillance images.

We now see the police needing not just images of the citizen but images from the citizen. This has profound implications for the 'surveillance relationship'. Investigations might use extracts from high street CCTV, but they also rely on image captures from dashcams, GoPros, ring doorbells and car parks. Increasingly the police are reliant on the product of an aggregated surveillance capability made up of hundreds of sources, most of them privately owned.

If one part of the system has been alienating the citizen with what are perceived to be unethical partners, untested technology, untrusted processes, mass retention of photos – or generally disproportionate intrusion into their lives they may be less inclined to assist when another part of the system needs their help.

And another aspect of this new surveillance relationship is to remember that citizen generated data may be unreliable, deliberately misleading or even maliciously intended.

Surveillance question – How would your surveillance relationship with the citizen be depicted by Banksy? You don't need to spraypaint it on a wall but at least think about it.

You can't do a surveillance conference without mentioning AI which brings me

to the 4th and final thing from my first year. The importance of transparency and explainability. AI in surveillance comes in many forms and excites a mixture of fascination and fear. There are many reports of genies getting out of their bottles, the rise of the machines and a dystopian future running out of control.

The lawful and ethical application of AI is much wider than a surveillance issue – if you want a brilliant summary and haven't already done so, maybe listen to the BBC Reith Lectures, also from last year.

But of all the use cases, novel applications and scare stories, just about the most terrifying thing I've come across in AI surveillance capability is this:

"Hello Barbie"

Forget Harpy and other 'loitering munitions' this is the most frightening thing I've seen in AI exploitation full stop.

An interactive doll produced for the English-speaking market, equipped with speech recognition systems and AI-based learning features, operating as an IoT device!

Mercifully this toy is no longer marketed owing to concerns about system and device security and you could run an entire conference on smart toys alone – but for now just think about the issues raised by having an interactive, AI-enabled doll connected to a developing child at one end and to the internet at the other. If you're struggling to see why that is so ghastly from a surveillance perspective read Nicole Perlroth's "This is How They Tell Me the World Ends".

Back to transparency and explainability. I have heard people say the AI in their surveillance tech is just "too complicated" to explain, and that even their designers and programmers don't really understand how it works. Well, if you're spending the public's money on it and you're abiding by your legal obligations to demonstrate that you've avoided bias – and discrimination – that won't do. If you're relying on automated decision-making that won't do, and if you're claiming ethics to be at the heart of your every decision, you'll need to prove ethical functioning of your AI.

Transparency and explainability are two keystones of public accountability – if your tech is too opaque or unintelligible for the citizen who's funding it – and purportedly benefiting from it, the problem isn't the citizen.

Surveillance question – How have you assured yourselves that all your AI-equipped, internet connected devices used for continuous and invasive monitoring, such as video surveillance are secure?

What about all your other data-intensive systems that collect mobility data

and drive behavioural information (GPS; Wi-Fi tracking devices; RFID technology; Intelligent Transport Systems and “event data recorder” devices)?

In summary – here’s what I’ve learned over the last year:

1. There’s a significant element of data protection and human rights engaged in biometric surveillance. But it’s not just data protection – any more than facial recognition is just photography or DNA sampling is just chemistry.

2. Be careful whose corporate company you keep – Conduct ethical pen tests as often – and sincerely – as your technical ones – and be as attentive to the ethical standards of your contractors as you are to your own.

3. Take care with your Surveillance Relationship with the citizen – you’re going to need each other. Remember – you’re only a part of a much larger system of surveillance capability – no one wants to be responsible for the weakest part of that ecosystem. Look after your bit.

4. Never connect dolls to the internet.