Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Covid-19, Adverse Scrutiny and The Journey to Code: where next for biometric tech?

Stewart Room, DWF Law

Between leaving a Big Four accountancy firm on New Year’s Eve and joining DWF Law as head of data protection and cyber-security, I spent a month developing a new business plan – fine-tuning a number of ideas I’d been working on concerning the future of data protection and privacy. This time allowed me to confirm the business plan should focus on two core ideas: namely ‘Adverse Scrutiny’ and ‘The Journey to Code’.

Adverse Scrutiny refers to the circumstances when an organisation’s positions on data protection, privacy and cyber-security can come under challenge. The challenge can be both internal and external. And it can be benign, malign, self-serving, public spirited or neutral. For example, an internal auditor will provide an internal challenge, from a neutral perspective. A whistle-blower, also an insider, will act in the public spirit. A rogue employee, also an insider, will have malign intent. A statutory regulator will provide external challenge, from a neutral perspective. I’m sure you’ll see how this challenge works.

The Journey to Code borrows ideas from a very influential book, ‘Code and other laws of cyberspace’ by Professor Lawrence Lessig, and combines them with what I’ve learned about the root causes of operational and legal failure over the years, and what I know about the legal obligations for Privacy and Security by Design. The thrust of the point is that the trajectory of data protection and privacy is only going one way – towards a time and place when the outcomes required by the principles of data protection are actually coded-in to the technology systems and data themselves. This will be a journey of evolution by incremental steps, rather than an overnight revolution and there’s plenty of evidence of the journey having already begun – for example, in the AdTech space.

To bring these two ideas together, at DWF I convened a community called ‘The Tech and Data Leaders Forum’, which launched with a webinar in March. The title of this webinar was ‘Techlash’ – and its core focus was facial recognition.

Techlash and facial ID

So why is facial recognition seen as so threatening to privacy? It stems from the major changes brought by the coronavirus pandemic. The world before the Covid-19 lockdown now seems like a lifetime ago, and the psychological impact of what we are experiencing is likely to be huge. At a personal level, I’m already finding it hard to relate to many aspects of my former life. I struggle to remember why I got worked up by stupid things like office politics and office bullies, and why I neglected the things that really matter, like prioritising time with my family.

Yet there will be many constants that carry over from the pre-Covid world into whatever the new world brings. One of these will be Techlash – and in January 2020 the world’s biggest data protection and privacy story was about facial recognition.

This Techlash around facial ID was arguably one of the most acute forms that we had witnessed. A momentum for ‘bans’ was building up. People were protesting in public. Litigation was starting. And the reasons for their concerns were both obvious and legitimate: people feared mass surveillance, not just by law enforcement agencies but also in retail estates, and coded-in bias and inequality, such as reported by NIST, which found that some algorithms presented much greater false-positive risks for people of colour than compared to people who are white.

CovidTech

Covid-19 has birthed a new tech and data movement, namely CovidTech. CovidTech constitutes the largest and most profound period of agile development for tech and data involving the processing of personal data that the world has witnessed. There are many aspects to CovidTech, but broadly speaking it has two key concerns: epidemiology and lockdown exit strategies.

“CovidTech constitutes the largest period of agile development for tech and data involving the processing of personal data that the world has witnessed”

Most recently, the CovidTech agenda has turned to contact tracing apps, which are being spun up everywhere, some involving governments and public health authorities, others not – while Google and Apple have united to add unprecedented accelerant. Other big initiatives involve the use of communications data, supplied by telecoms companies.

Facial recognition forms part of CovidTech, though in some territories it has received less airtime than contact tracing. Even so, it’s been reported that buses in China are being outfitted with facial recognition systems that combine with thermometers. Russia is said to have redeployed its facial recognition technology to the cause. And apps in Poland and India are being
The country’s surveillance system. The worry is its Investigatory Powers Act, which establishes the UK gaining an adequacy decision is restricted data flows from the EU to third countries. EU data protection law, which allows unrestricted data flows from the EU to third countries that the EU deems are adequate for data protection purposes. Arguably, the biggest hurdle to the UK gaining an adequacy decision is its Investigatory Powers Act, which establishes the country’s surveillance system. The worry is that this could permit surveillance that is closer to the ‘mass’ end of the spectrum than the EU feels comfortable with.

In the same way, many people are uncomfortable with the risks that CovidTech, both facial recognition and contact tracing, is taking with civil liberties. There are far too many strands to the concerns to cover here, but some of the more interesting ones are:

- The technology involved is unproven and in the absence of enough virus investigators and testing facilities on the ground, it might not make a difference, meaning that the invasion of privacy cannot be objectively justified as being necessary.
- Claims that data used to combat Covid-19 will be anonymous, or pseudonymised, might prove to be untrue.
- We’re heading down a slippery slope, where invasions of data privacy can lead to much more substantive invasions, such as arrests and forced testing.
- We’re playing into the hands of the Big Tech companies, whose power stems from data insights, control and surveillance capitalism.
- Governments might be reluctant to rein back their new powers at the appropriate time, with the result that we might be subjected to unjustified surveillance for a period of time uncertainty or, worse still, perpetually.
- We don’t have any basis to objectively measure the downside of surveillance of the kind in question, meaning that we might be risking something even worse than Covid-19.

After 9/11, the War on Terror was waged against hidden enemies – which has some metaphorical resonance for now. But the better comparison is with the creation of the new mass surveillance system that whistleblower Edward Snowden exposed to such dramatic effect.

The instances of illegality Snowden exposed are too many to count, but some that are worth remembering include the EU’s Data Retention Directive and its Passenger Name Records Framework Decision, which were both found to be unlawful by the European Court of Justice. They were direct responses to 9/11. Another casualty was the Safe Harbour Decision, which was declared unlawful because of the mass surveillance system in the US exposed by Snowden.

The surveillance infrastructure built after 9/11 provides our warning. What we’ve learned is that even the most pressing needs after the most shocking events are subject to the Rule of Law, and that what appears necessary and expedient at one point in time may not do so later on. Everyone participating in CovidTech needs to be aware of this – not to create fear or to stymie sound developments, but to help improve them.

“After 9/11, what we’ve learned is that even the most pressing needs after the most shocking events are subject to the Rule of Law”

Can facial ID survive scrutiny?

Imagine the time after the Covid-19 crisis, when the lockdown is over, vaccines have been developed and herd immunities established. This future will likely include myriad political, judicial and public inquiries; countless episodes of public inquiries, and I expect CovidTech to suffer a Techlash to some degree.

9/11: the pendulum’s return

Have we been here before? In part, yes we have. After 9/11, the War on Terror was waged against hidden enemies – which has some metaphorical resonance for now. But the better comparison is with the creation of the new mass surveillance system that whistleblower Edward Snowden exposed to such dramatic effect.

The instances of illegality Snowden exposed are too many to count, but some that are worth remembering include the EU’s Data Retention Directive and its Passenger Name Records Framework Decision, which were both found to be unlawful by the European Court of Justice. They were direct responses to 9/11. Another casualty was the Safe Harbour Decision, which was declared unlawful because of the mass surveillance system in the US exposed by Snowden.

The surveillance infrastructure built after 9/11 provides our warning. What we’ve learned is that even the most pressing needs after the most shocking events are subject to the Rule of Law, and that what appears necessary and expedient at one point in time may not do so later on. Everyone participating in CovidTech needs to be aware of this – not to create fear or to stymie sound developments, but to help improve them.

“After 9/11, what we’ve learned is that even the most pressing needs after the most shocking events are subject to the Rule of Law”

Can facial ID survive scrutiny?

Imagine the time after the Covid-19 crisis, when the lockdown is over, vaccines have been developed and herd immunities established. This future will likely include myriad political, judicial and public inquiries; countless episodes of public inquiries, and I expect CovidTech to suffer a Techlash to some degree.

9/11: the pendulum’s return

Have we been here before? In part, yes we have. After 9/11, the War on Terror was waged against hidden enemies – which has some metaphorical resonance for now. But the better comparison is with the creation of the new mass surveillance system that whistleblower Edward Snowden exposed to such dramatic effect.

The instances of illegality Snowden exposed are too many to count, but some that are worth remembering include the EU’s Data Retention Directive and its Passenger Name Records Framework Decision, which were both found to be unlawful by the European Court of Justice. They were direct responses to 9/11. Another casualty was the Safe Harbour Decision, which was declared unlawful because of the mass surveillance system in the US exposed by Snowden.

The surveillance infrastructure built after 9/11 provides our warning. What we’ve learned is that even the most pressing needs after the most shocking events are subject to the Rule of Law, and that what appears necessary and expedient at one point in time may not do so later on. Everyone participating in CovidTech needs to be aware of this – not to create fear or to stymie sound developments, but to help improve them.

“After 9/11, what we’ve learned is that even the most pressing needs after the most shocking events are subject to the Rule of Law”

Can facial ID survive scrutiny?

Imagine the time after the Covid-19 crisis, when the lockdown is over, vaccines have been developed and herd immunities established. This future will likely include myriad political, judicial and public inquiries; countless episodes of public inquiries, and I expect CovidTech to suffer a Techlash to some degree.

9/11: the pendulum’s return

Have we been here before? In part, yes we have. After 9/11, the War on Terror was waged against hidden enemies – which has some metaphorical resonance for now. But the better comparison is with the creation of the new mass surveillance system that whistleblower Edward Snowden exposed to such dramatic effect.

The instances of illegality Snowden exposed are too many to count, but some that are worth remembering include the EU’s Data Retention Directive and its Passenger Name Records Framework Decision, which were both found to be unlawful by the European Court of Justice. They were direct responses to 9/11. Another casualty was the Safe Harbour Decision, which was declared unlawful because of the mass surveillance system in the US exposed by Snowden.

The surveillance infrastructure built after 9/11 provides our warning. What we’ve learned is that even the most pressing needs after the most shocking events are subject to the Rule of Law, and that what appears necessary and expedient at one point in time may not do so later on. Everyone participating in CovidTech needs to be aware of this – not to create fear or to stymie sound developments, but to help improve them.

“After 9/11, what we’ve learned is that even the most pressing needs after the most shocking events are subject to the Rule of Law”

Can facial ID survive scrutiny?

Imagine the time after the Covid-19 crisis, when the lockdown is over, vaccines have been developed and herd immunities established. This future will likely include myriad political, judicial and public inquiries; countless episodes of public inquiries, and I expect CovidTech to suffer a Techlash to some degree.

9/11: the pendulum’s return

Have we been here before? In part, yes we have. After 9/11, the War on Terror was waged against hidden enemies – which has some metaphorical resonance for now. But the better comparison is with the creation of the new mass surveillance system that whistleblower Edward Snowden exposed to such dramatic effect.

The instances of illegality Snowden exposed are too many to count, but some that are worth remembering include the EU’s Data Retention Directive and its Passenger Name Records Framework Decision, which were both found to be unlawful by the European Court of Justice. They were direct responses to 9/11. Another casualty was the Safe Harbour Decision, which was declared unlawful because of the mass surveillance system in the US exposed by Snowden.

The surveillance infrastructure built after 9/11 provides our warning. What we’ve learned is that even the most pressing needs after the most shocking events are subject to the Rule of Law, and that what appears necessary and expedient at one point in time may not do so later on. Everyone participating in CovidTech needs to be aware of this – not to create fear or to stymie sound developments, but to help improve them.

“After 9/11, what we’ve learned is that even the most pressing needs after the most shocking events are subject to the Rule of Law”

Can facial ID survive scrutiny?

Imagine the time after the Covid-19 crisis, when the lockdown is over, vaccines have been developed and herd immunities established. This future will likely include myriad political, judicial and public inquiries; countless episodes of public inquiries, and I expect CovidTech to suffer a Techlash to some degree.
of investigative journalism; and who knows how many regulatory investigations and court cases. Those processes will praise the good, such as the heroism of the key workers on the frontline, and they will criticise the bad. Somewhere along that spectrum will appear CovidTech, including facial recognition.

I expect CovidTech to suffer a Techlash to some degree. This isn’t a commentary on whether it’s good or bad, but a statement of likelihood that reflects the normal run of things. In my view, facial recognition operators might be in a different category to some of the other participants in CovidTech, due to the legacy they take with them into this new field. If they reflect on the recent past and are honest about what it meant for them, they might appreciate that they are at a heightened risk of suffering additional Techlash against them in the future.

This could be a starting point that will help them to make a positive contribution to the goals of CovidTech (reducing infections and speeding up the exit from lockdown) in a manner that is respectful of civil liberties. Or, at the very least, they might avoid a ‘pile-on’ that simply harms civil liberties with no Covid upside. Some ideas that I offer for discussion are:

• The use-case for facial recognition during the current crisis needs to be properly understood and reasoned. The idea of contact tracing is first and foremost an epidemiological one, so the use of facial recognition in this context needs to be supported by the consensus of expert opinion in this field and then backed by governments. Of course, epidemiology can be supported through law enforcement – for example, to detain people for testing purposes (as with the UK Coronavirus Act 2020), but we have not yet reached that point, or even started a public debate about this.

• National laws and systems need to be understood in detail. One of the claims made by data protection regulators and some lawyers is that the European Union’s GDPR privacy law will not stand in the way of data processing that is necessary and proportionate in the fight against Covid-19. This is true in a technical sense, in that the GDPR allows for data protection rules to be lowered in very serious situations such as pandemics – but this means nothing more than there’s a possibility that CovidTech could be lawful for data protection purposes. To make progress on the question of lawfulness, the details and nuances of national laws need to be understood. They differ from country to country and when considered against real use-cases, the law might not be as permissive as the initial claims suggest.

• If a lawful use-case for facial recognition is identified, the implementation plan should address the minutiae of data protection. The three pillars upon which data protection lawfulness rests are transparency & accountability; Privacy by Design; and regulatory clearance.

There is much detail here and it should not be overlooked. Where possible, the required outcomes of data protection, balanced against the needs of the use-case that is being supported, should be baked-in to the tech and data themselves, supported by other controls within the organisational and paper structures of the operator. In other words, CovidTech is, in my view, a compelling argument for the commencement of ‘The Journey to Code’.

Reputations cross borders, so participation in a mass surveillance scheme in one country might have longer-term reputational consequences in another country. One of the issues here is how much of tomorrow will your company trade for today?

About the author
Stewart Room is global head of data protection and cyber-security at DWF LLP. He is recognised as one of the UK’s leading lawyers working in the fields of data protection, privacy and security. A barrister and solicitor with nearly 30 years’ experience, Stewart has worked on many very large transformation projects, as well as having acted in many leading legal cases. He joined DWF, the LSE-listed legal business, in February 2020 as head of data protection and cyber-security, and prior to that held an equivalent position in a Big Four accountancy firm. He has written or contributed to many leading textbooks in these areas. He can be contacted at stewart.room@dwf.law.

In a summary of its work, Stanford recognised the inevitable jokes by saying: “There’s a new disease-detecting technology, and its No. 1 source of data is number one. And number two.”

The ‘precision health’ toilet can detect a range of disease markers in stools and urine, including those for colorectal and urologic cancers. Stanford said the device could particularly suit people who are genetically predisposed to conditions like irritable bowel syndrome, prostate cancer or kidney failure.

The researchers, led by Professor Sanjiv ‘Sam’ Gambhir, have completed a pilot study of the smart toilet using 21 participants. To create it, Gambhir fitted cameras and motion sensors inside an ordinary toilet. These capture urine and stool samples on video, which are then processed by algorithms that can distinguish normal ‘urodynamics’ (such as flow rate, stream time and total volume) and stool consistencies, from those that are unhealthy.

The toilet also uses uranalysis strips, or ‘dip-stick tests’, to measure the user’s white blood cell count, blood contamination and protein levels, which can point to diseases ranging from infections to bladder cancer or kidney failure. In its current form, Gambhir said the toilet measures 10 different biomarkers.

It automatically sends any data extracted to a secure, cloud-based system for storage. The intention is that when something questionable arises – like blood in the urine – a privacy-protected app would send an alert to the user’s healthcare team, allowing professionals to

Continued on page 12...