Justice and Home Affairs Committee

Uncorrected oral evidence: New technologies and the application of the law

Tuesday 7 September 2021

10 am

Watch the meeting

Members present: Baroness Hamwee (The Chair); Lord Blunkett; Baroness Chakrabarti; Lord Dholakia; Baroness Hallett; Lord Hunt of Wirral; Baroness Kennedy of The Shaws; Baroness Pidding; Baroness Primarolo; Lord Ricketts; Baroness Sanderson of Welton; Baroness Shackleton of Belgravia.

Evidence Session No. 3 | Virtual Proceeding | Questions 39 - 51

Witnesses

I: Professor Elizabeth Joh, Martin Luther King Jr. Professor of Law, University of California, Davis; Professor Colin Gavaghan, Chair of the Advisory Panel on emergent technologies at New Zealand Police and Director of the New Zealand Foundation Centre for Law and Policy in Emergent Technologies, University of Otago; Dr Rosamunde Elise Van Brakel, Co-Director at the Surveillance Studies Network, Associate Professor in Cybercrime at Tilburg University and Assistant Professor at the Vrije Universiteit Brussel.

Examination of witnesses

Professor Elizabeth Joh, Professor Colin Gavaghan and Dr Rosamunde Elise Van Brakel.

Q39 **The Chair:** Good morning, everyone, and particularly good morning to our witnesses who are joining us by video link from overseas, from California, New Zealand and Brussels. We are particularly grateful to them for taking part in this meeting, giving us the benefit of their experience and being prepared to do so at such antisocial hours of the day for two of you.

The meeting is being broadcast and a transcript will be provided. Our witnesses will have an opportunity to see that and correct anything if it needs correcting. If we do not have the opportunity to cover ground that our witnesses would like to cover, because we are time-limited, we would be delighted to hear from you with further written comments. We all have questions. We will have about six minutes for each of our prepared questions and then, I hope, an opportunity at the end for any further questions.

I will ask the witnesses, when I come to each of you first, to introduce yourselves very briefly. Off we go with the first question, which is an easy ball. Can you each tell us how advanced technologies are being used for the application of law in your respective countries, give some specific examples and tell us of any benefits the technologies have brought?

Professor Elizabeth Joh: Good morning. I am a professor of law at the University of California at Davis School of Law. My research has focused on how new technologies have changed and are influencing ordinary law enforcement in the United States, so my remarks this morning will be focused on that particular area of new technologies.

With respect to this question, there are a number of ways in which new technologies are being used in the United States with respect to ordinary law enforcement. One can think of automatic licence plate readers, facial recognition technologies, risk assessment programmes, social media monitoring and prediction tools, all of which have drawn intense scrutiny and criticism.

Theoretically, since you have asked me about the benefits, there are enormous potential benefits such as increasing the capability of the police in ways that would not be possible without automation and new technologies in terms of the speed of analysis, pattern recognition and those sorts of things.

One paradigmatic example of a new technology that has provided benefits in the United States comes to mind: the use of police body-worn cameras. Body-worn cameras have been used in the US for some time, but the big explosion of body-worn camera adoption in the US came about because of a particular incident in 2014, a fatal shooting of a civilian named Michael Brown by a police officer in Ferguson, Missouri. Because of the intense national and international attention to that shooting, and because there was a dispute about what exactly happened, as a result of the investigations into that civilian fatal shooting there were calls

throughout the country for some kind of technology, including body cameras, for increased accountability. In the United States, body cameras have been adopted very widely and have been embraced by a number of different sectors of society, including police reform advocates, police leaders, et cetera.

In this sense there have been good and bad things. For police body-worn cameras there has been more accountability, so, to the extent that accountability was the goal, that has been realised to a certain degree. We have seen exposures of certain instances of excessive force or questionable police behaviour.

The American experience has been also decidedly mixed with respect to this one technology. We have seen more accountability, but there has also been insufficient forethought given to regulation. Body cameras have been a primary example of the questions that come about when there is a new technology capable of increasing power and capabilities without a public debate about what the right sort of regulation is.

The Chair: We will come to some of these issues in a few minutes, Professor Joh. I suggest to members of the committee who may not have seen it that we have had a blog piece from you on this, which is really interesting, with the disbenefits as well as the benefits.

Professor Colin Gavaghan: Kia ora from Aotearoa. I am a professor of law and emerging technologies at the University of Otago, down at the bottom of the South Island of New Zealand. I am also the chair of the New Zealand Police Expert Panel on Emergent Technologies and a member of the Digital Council for Aotearoa, an advisory body to the Government on matters digital.

I would characterise New Zealand's status in this regard as being probably a fast follower rather than an early adopter of new technologies. Our use of technologies in this context has probably been a bit more limited, certainly than in the United States. Until recently we did not have a good idea of what was happening at all. Only in 2018 did we make a first attempt at getting a snapshot of what was happening.

I can draw attention to a few uses, broadly speaking within the criminal justice context. Police are currently trialling a predictive policing algorithm to identify likely crime hotspots. It is widely deployed in the United States with a view to informing procurement decisions, so deploying officers to areas where it is reckoned that there is likely to be crime.

A tool that has been in use for some time is called YORST, an acronym standing for youth offending risk screening tool. This is a prediction algorithm using a decision tree system that is supposed to predict the likelihood of young people getting back into trouble, recidivating. It draws on variables, including their education, living situation and the parents' offending history. It is supposed to categorise them as being at high, medium or low risk of recidivism with a view to informing interventions by youth aid officers. The idea is not supposed to be punitive but to

develop a plan to divert them from that path. There is probably a bit more to be said about that. We have a similar thing with a slightly different purpose for family violence, again predicting the risk of recurrence with a view to informing response and potentially a safety plan.

The other things I will quickly mention are an anti-money laundering tool, which looks at suspicious financial activity with a view to estimating the likelihood of something nefarious going on. Another one, interestingly, evaluates tip-offs about terrorist activity to the national intelligence body with a view to making assessments of their credibility and whether they ought to be followed up.

That is a cross-section of what is happening. There are quite a lot of trials either under way or shortly about to be so, but not so much in the way of active use cases at the moment.

The Chair: Thank you—all very controversial. Our equivalent in the youth area is the gangs matrix in London.

Dr Rosamunde Van Brakel: Good morning and thank you for the invitation. I am associate professor, cybercrime, at the Tilburg Institute for Law Technology and Society, and assistant professor at the Law, Science, Technology and Society Research Group at the Vrije Universiteit in Brussels. In addition, I am a co-director of the Surveillance Studies Network, and in 2019 I established a research chair in surveillance studies at the university in Brussels.

I have been conducting research on the social and ethical consequences of new technologies since 2006. More recently, I have focused on the governance of new technologies, specifically in Belgium, looking at how oversight of the police use of algorithmic technologies is organised.

Belgium is an interesting case, especially if you compare it to the United States, because it is quite behind in implementing advanced technologies. This only started to change from 2015 or 2016, when there were a lot of press releases about the launch of iPolice. This is one of the two main projects which the federal police in Belgium have been focusing on. In Belgium, the federal and local police forces are integrated because of the political structures in Belgium. This is quite a complicated structure. iPolice aims to make communication between all police forces more efficient and easy, and to have all databases communicate with each other and make it more efficient to make analyses and discover patterns in the information.

A second project is more recent and is called mass storage and analytic solutions for evidence. This aims to have a storage of output from investigatory tools, such as output from smart video surveillance, and use artificial intelligence for complex analysis.

Apart from these two main projects of the federal police, in Belgium the local police zones have been implementing advanced technologies quite a lot. This has

accelerated since the Covid pandemic. Many cities in Belgium have started to use smart video surveillance to assess how busy it is in the street, for instance.

A police zone on the west coast of Belgium has been experimenting with predictive policing software since 2016. However, very few details are known about this, so I cannot go into further details to explain it. The former Minister for Home Affairs had a plan, which has now been implemented, to have an automatic number plate recognition camera shield in Belgium, with 3,500 cameras. This is almost finalised.

In general on the benefits of the technologies, I have spoken about smart video surveillance and predictive policing, but no systematic evaluations have been conducted, so it is very hard to say whether they have had real benefits. Of course, people will say that they see benefits in certain cases, but there is no scientific evidence here.

We do see benefits with the Focus app, however, which is a success for the Antwerp police. It won a prize for IT project of the year and the police are very enthusiastic about it. The app allows police officers to consult various databases in the field in a very simple and smooth manner, view debriefing items and follow up on incidents. This is something that they feel has made their work easier.

The Chair: No doubt it depends on where you are coming from whether you think that being spied on to see whether you are going to your second home on the coast against the local Covid laws is a benefit or a problem in human rights terms, and so on.

Q40 **Baroness Hallett:** How has the use of advanced technologies in the application of the law evolved over time in your respective countries? Is it a general increase, or are there any hints of brakes being put on the application of advanced technologies in the law?

Professor Colin Gavaghan: It is a little hard to say with any certainty, because it is only since 2018 that we have had an accurate picture of what is happening. I would say it is a little bit of one and a little bit of the other. There is certainly an appetite to upscale and capitalise on the benefits of efficiency and accuracy from some of these tools, but there is also a growing awareness of the missteps that could significantly erode public trust.

We have had a couple of near misses in that respect recently. Last year a police trial of a facial recognition algorithm attained a degree of notoriety. It proceeded without proper authorisation or supervision. The trial fell over at an early stage, because it was not working, for reasons we may come back to. It was not scoring very highly on identifying New Zealand faces. That happened before any real harm resulted from it, but the resulting media fall-out drew attention to the potential dangers of proceeding so casually.

There is an appetite to deploy this technology but also an appetite perhaps not so much for brakes but for proper scrutiny and evaluation processes to be put in place.

Professor Elizabeth Joh: As the American here I must rely on the terrible analogy that we are the wild west when it comes to these technologies, meaning that there has been outright experimentation in the United States with respect to many different kinds of technologies. This relates to the political structure of policing in the United States. There is no sense that the Federal Government directly controls local policing forces, literally tens of thousands of police forces, so they are virtually left to their own, based on whatever local state governance structures there are. We have seen the adoption of many kinds of technologies all around the United States on a case-by-case basis.

With respect to certain technologies, we have begun to see some criticism and push-back. For example, predictive policing tools were embraced by many police departments in the 2010s. In the United States you can see small movements towards a backlash. For example, one of the first cities—a small one in California—to adopt a predictive policing software tool also later became the first city in the United States to ban such predictive policing programmes last year after some experiences, realising it was not the tool it was promised to be. In Los Angeles, which has a significant police force, the department has stepped back from relying on some predictive programmes after third-party audits have revealed issues with how the programme works in terms of oversight, inconsistency in the use of the programmes and things of that nature.

Finally, with facial recognition there is a growing call for some sort of regulation. We see movements towards bans, but again these have been piecemeal. There has certainly not been national regulation of any sort. That is the picture in the United States. There is a proliferation of many different kinds of technologies and a growing public awareness that some things have to be done as a response.

Baroness Hallett: As a follow-up to that, when you say there is some stepping back, is that on the basis of reliability of the technology or ethics or both?

Professor Elizabeth Joh: Both. There have certainly been concerns about, for instance, racial bias in the data used in tools like facial recognition. With respect to predictive policing tools, there is a sense that it may not be as reliable or as effective as promised. Again, much of this depends on the particular technology and how much disclosure there has been with respect to how these tools are deployed. Again, much of this depends on the local political structure of how policing is regulated in the United States. There is no Home Office in the United States. Our President cannot make a snap judgment and change policing throughout the United States. That has been the main regulatory difficulty for us.

Dr Rosamunde Van Brakel: In Belgium, at the political level in the federal police, there is huge enthusiasm to innovate. They have a clear strategy that the police has to innovate and invest in new technology. Local police are also autonomous and there you see differences. There are some local police zones who have invested a lot in new technologies, but there are other local police zones that are more

hesitant and are not such big fans of investment in new technology. So you see a different attitude toward the technologies within the police.

Concerning civil society and the population, because there has been this increase in the use of new technologies to control Covid measures, and in general, in the context of the pandemic, the Belgian Government have made decisions that have been in conflict with the law, and a lot of people have started to question these new technologies; they feel that they are being controlled too much by the Government. As far as I can see, this grew with the Covid pandemic. Before the pandemic there was not that much resistance from the population.

Baroness Kennedy of The Shaws: What would you consider to be the best or worst-case scenario for the development of new technologies for the application of law in the coming years? What do you think would be the best way to develop new technologies in the coming years, while being respectful of civil liberties and the rights of individuals? How do you do that while balancing the interests of the state with the interests of the wider community and individual rights? It is the central issue so let us get to it fast.

The Chair: Who would like to tackle that big question?

Baroness Kennedy of The Shaws: It is the central issue, so let us get to it fast.

Dr Rosamunde Van Brakel: I would like to talk about what the best-case scenario would be in this case. I have been looking at how oversight bodies are organised in Belgium and how the regulation has evolved. At the moment, we have data protection regulation and there is an artificial intelligence regulation coming up in Europe.

The best-case scenario is that, when regulating these new technologies, there is broader attention than just data protection when assessing whether the police should implement new technologies. Some new processes need to be implemented *ex-ante*, so before investment in new technologies, making proportionality assessments, and taking into account not only whether the technology is legally compliant but how it will have an impact on society, democracy and the rights of citizens.

Another assessment point should be how the technology empowers the police. How will the technology help the police in fulfilling their societal goal? This question is not asked enough. I feel that the technology is being praised as going to solve everything and there is not enough reflection on how it will help the police.

I think the worst-case scenario will be that regulation is watered down whereby the rights of citizens, especially certain groups in society, will be the subject of these technologies in a disproportionate way.

Professor Elizabeth Joh: As far as a best-case scenario is concerned, I echo many of the previous comments. There should be some *ex-ante* measures set in place so

that any new technology, regardless of what it is, can be vetted before the public in an open and transparent manner.

With respect to new technologies, because they so often involve processes that are not familiar to the public, some ability to explain to the local community is of paramount importance. The police themselves may be unable to explain why a particular technology produces the results it does or how it produces the results, or to the extent that it has errors or bias. These things have to be explained by the police and explainable to the public, so a mechanism, whether it is through an oversight committee or detailed regulation, is essential for a best-case scenario with respect to new technologies.

In the United States, we are still far from that best-case scenario. We are moving towards a situation where we have virtually unchecked experimentation with many different kinds of technologies. Police departments are seemingly free to pilot or experiment with something new without a lot of oversight or regulation. Then we sometimes see investigative reporting, of legal cases arising out of something disastrous or with life-altering consequences for particular people, and then calls for regulation. So in a sense the process is the exact opposite of what I said about the best-case scenario.

Also, an increasing distrust of technology would be one of the consequences of this worst-case scenario. In particular, with respect to a growing movement for algorithmic accountability, which applies not just with law enforcement but throughout lots of sectors where new technologies are being used, we see two different orders of questions. On the one hand, the early stages of algorithmic accountability call for things like attention to racial bias, fairness and transparency.

Increasingly, there are those who might say that perhaps there are some applications of new technologies where they should not be used at all—the notion that there are some areas of policing where these new technologies should have a pause or a permanent ban. These big picture questions are also arising. These are part of what would inform the best and worst-case scenarios.

Professor Colin Gavaghan: I agree very much with the two previous speakers and I will try not to repeat too much of what they said.

In terms of the worst-case scenario, it could go one of a couple of ways. You could see the baking-in of historical bias and historical prejudice, and it not only being baked into future decisions but being rendered less visible under an ostensibly objective algorithmic process. On the other hand, we could see a collapse of public trust in these systems. We could see a lot of babies being thrown out with the bathwater. We could see potential gains not just in efficiency and accuracy, but perhaps also in transparency and fairness, being jettisoned because these kinds of technologies have not been introduced in the right way.

The best-case scenario is, I guess, the opposite of that. It is one in which decisions are potentially more transparent than at present. The relevant comparator here is

not some Dworkin's Hercules. It is not some putatively perfect human decision-maker. We know that human decision-makers are flawed in all kinds of ways, and there is real potential for improvement on that.

In terms of how we get there, I reiterate Professor Joh's comment that the first decision has to be, "Is this the right solution at all?" The fact that we have an algorithm or an EDM solution does not mean we have to use it, and it depends on the question we are trying to answer.

Another observation I would make at this point is if we are going to avoid the worst-case scenarios, we need to involve, at a very early stage in the process and in a meaningful way, members of those communities who are likely to be at the sharp end of these algorithms. It is all very well setting up committees with people like me—white, middle-class university professors—but I am not the kind of person who is likely to be profiled as a future risk, I do not think, accent notwithstanding. Even with the best will in the world, we might not spot some of these problems and some of these risks. Having them meaningfully involved at an early stage, and not just in a box-ticking exercise when it is *a fait accompli*, is hugely important. There are all kinds of mechanisms, from a regulatory point of view, that could be employed to do this, and I am sure we can talk more about these as we go on.

Finally, there is definitely a movement towards a full-life cycle auditing and compliance model that recognises that problems can creep in. Even with a good pre-deployment, assessment problems can come to light, or, in the case of more self-learning models, can creep into the system as we go. So the scrutiny has to be ongoing; it cannot be just a one-time for all-time snapshot.

The Chair: Indeed. Thank you very much. I am going to have to say the thing that I always hate saying, which is that we need to keep an eye on the time. That is not addressed to anybody in particular.

Q41 **Baroness Shackleton of Belgravia:** Good morning. To what extent is the use of advanced technologies for the application of the law debated in your respective countries, both by experts and by the general public? It is very interesting what Dr Van Brakel says in relation to a pandemic making people more aware of the technologies that are deployed—they may have considered themselves to be law-abiding, innocent citizens and then they are caught on facial recognition having a cup of coffee with more than one person—and recognising that one person's tool is the loss of another person's liberty. These are very important decisions, and we are interested to know in your respective countries at what level these decisions are debated and by whom.

The Chair: We will start with Dr Van Brakel, and then go to Professor Gavaghan, where things have been very different in New Zealand.

Dr Rosamunde Van Brakel: The public debate, as I said, has really kicked off with the pandemic. I would say that the debate at the moment is quite limited in the sense that it is mainly focused on privacy implications. From the citizens'

perspective, they are happy if technology is used if it is targeted, if it is in the context of anti-terrorism or organised crime. Now, with the pandemic, technologies are focusing on the whole population, and people are questioning the Government. We see that there is a clear loss of trust in the Government as a result.

At the higher levels, there are political debates within law enforcement. Also, what is interesting is that the current Minister of Home Affairs has launched an inquiry to see how law enforcement in general can be improved in Belgium. One of the aspects that is being debated is how new technologies will play a role in the new police of 2030. Here the debate, especially within the police, is a lot about how technology will make our work more efficient. There is more and more attention here, in thinking about data protection issues, on how the technology will be implemented. It is limited to that.

Data protection in Belgium is interpreted in a very narrow way. It gets very little attention. Also, because of a lack of expertise, very little attention is given to the more discriminatory effects of new technology in the general debate. This is very different from debates in the United States and in other countries. There is very little discussion about how these new technologies can have a discriminatory effect.

Professor Colin Gavaghan: As you say, Baroness Hamwee, our situation has been rather different, although we are about two-and-a-half hours away from emerging from our latest lockdown, which is rather nice.

One thing that we have learned over the last year and a half is that there is generally and relatively a high degree of trust in New Zealand in the Government, not just this Government but Governments in general, and in the police. That obviously varies between communities but, comparative to my experience in the UK, it is very high here.

In terms of discussion of this particular technology, it has only recently come to light. I would say that it has happened partly in the shadow of revelations, particularly from the United States and other places, partly due to a few media splashes here, for example, about the discovery that Immigration New Zealand was using algorithms, which came as a surprise even to the Minister responsible. That has heightened the degree of awareness.

The main sides in the debate are much as you would expect, I suppose. Sceptics are concerned about non-transparent black boxes and entrenched bias. Proponents are concerned about greater efficiency and accuracy and about pointlessly onerous regulatory burdens being placed on them.

It is hard to characterise the general public mood, but the Digital Council conducted a series of workshops last year, particularly with traditionally excluded populations, to try to get a sense of how they felt about these technologies. We found that most participants were not intuitively hostile to the use of automated decision-making.

There are two things I would say quickly. One is that their level of trust tends to mirror the level of trust that they have in the government agency or department using them. If they think that they are generally treated poorly by a particular agency, they will expect that the EDM will just replicate that.

Secondly, there were a lot of questions going on about the purpose of the algorithm and what is being done with the outputs. For example, the young people we asked about the two algorithms we have that try to identify at-risk youth—at risk of criminality and of long-term unemployment—were not, as we thought, knee-jerk hostile to them. They could see potential benefits. They wanted to know the purpose of the output: "What is it going to be used for? Is it to provide me with additional support? Or is it to trigger greater surveillance or greater police attention?" I would say that they were less concerned about the technology than about the policy considerations and the assumptions lying behind it.

Q42 **Baroness Shackleton of Belgravia:** I have a supplementary question. You say that the Government influences people's trust, but we are harvesting data here, and what happens when that Government get overturned? It is a dangerous weapon for any successor if it was to misuse that data. Are they not concerned, or do they think so short-term?

Professor Colin Gavaghan: I think they are less concerned than I would like them to be. There are regular surveys that show that the New Zealand Government are highly trusted. That is a mixed blessing, because misplaced trust is obviously a very concerning thing. I am not saying that we should not particularly trust any of the Governments we have had since I have been here.

But I share your concern. There is a certain degree of naivety about the potential uses among the general populace. I think that is far less true among, for example, the Māori population, who have had far greater occasion to be concerned about actions of the Government. The general sense among the population is one of high trust—sometimes, perhaps, slightly misplaced trust—at least with a view to what might happen at some point in the future. I agree entirely with you about that.

Professor Elizabeth Joh: In the United States I would say that there is not a particularly high degree of trust in government on the part of many communities, and that also translates to law enforcement. There are those communities that, in particular historically, have been overpoliced or have experienced bad relationships of trust with their local law enforcement departments. That has carried over to the debate with new technologies.

On the other hand, there are certainly pressures on law enforcement to develop more capabilities, to be more efficient, and—one point that has not yet been raised here—to save money in human resources by adopting algorithmic programmes that might reduce the need for human officers and for human interventions. That certainly is one part of the debate.

Another point that needs to be addressed is the influence of the private sector in two ways. Number one, it is the private sector for the most part that has developed the actual technologies in the United States that are being used by law enforcement agencies throughout the United States. They obviously have an enormous stake in making sure that these technologies are adopted. They provide often enormous incentives to these departments to take up these technologies, either for free or on a vastly reduced basis.

The other aspect of the private sector using some of the very same technologies is not part of the policing debate per se but adds to the general level of confusion and policy debate insofar as who is collecting this information and for what purpose.

The Chair: We have a question for our witnesses about procurement and the private sector later, so perhaps the other two can come in then on that issue.

Q43 **Baroness Pidding:** What do you view as the most appropriate sphere of government at which to regulate the use of advanced technologies for the application of the law at local, national, regional, or global level? Who do you think should be held accountable for the use of such technologies and through what mechanisms?

The Chair: Professor Joh, do you want to go first? I suppose the United States is very different from the other countries that we are talking about, and indeed from ours.

Professor Elizabeth Joh: I would be happy to. Ideally, the most appropriate level of government would be at the national level, in my opinion—a nationwide set of solutions to set both the policy expectations and the regulatory mechanisms for new technologies. Unfortunately, in the American experience that has not been the case. The national Government have been quite slow to react. There have certainly been calls and some legal proposals for regulating certain aspects of technology, such as facial recognition or the use of algorithms, in a limited context. But those have not yet become enacted laws.

What we have seen is regulation in the US at a hyper-local level. We have seen city governments that have decided that their own departments must be regulated. There has been some movement to have this kind of accountability but again at a hyper-local level, not at the state or county level but at the smallest, most local level of government, with some success. Of course, if we are looking at the United States as a whole, the dozens of cities that are trying to attempt these kinds of enforcement and regulatory mechanisms are hardly the example that another nation ought to follow, because it is happening at such a small scale.

Baroness Pidding: Dr Van Brakel, you have already referred to the political division—perhaps that is too inflammatory a word—in Belgium. What can we learn, if anything, from what you can say?

Dr Rosamunde Van Brakel: Yes, Belgium is a specific case here, especially if you start talking about regulation. I think sector-specific regulations could be very helpful, especially if we are looking at the use of advanced technologies in the public sector, such as in law enforcement. What we are seeing, especially with the

general data protection regulation at a European level, is that this is very much focused on collecting data online or data collection in the private sector.

There are very few concrete guidelines for how public sector organisations should implement data protection measures, because the use of these technologies has very different implications in different sectors. Surveillance technology is used in the context of organised crime and in the context of child protection, and these are very different contexts. I do not think that a general regulation can capture the specificities here. Ideally, you will have a combination of different levels of regulation that go from the more general to the specific.

Finally, what is specifically very much missing in Belgium is soft law and guidelines. It is very unclear, especially in public sector organisations and government agencies, how they are supposed to implement these regulations. There are still a lot of questions, and I think more specific guidelines would be very helpful.

Professor Colin Gavaghan: New Zealand is a very simple country from this point of view, in that we have no devolution to speak of and any lawmaking at hard-law level will come down from Wellington. It is as simple as that. Nor are we party to anything like the EU, although we are, to a significant extent, rule takers as well as rule makers. The fact that so many of our companies trade into the EU has meant that ensuring compliance with the GDPR has been an important consideration, as it is likely to be with any new AI rule.

In terms of what level I think would be ideal, it is very hard to say at this stage. As Professor Joh says, I have seen anything from city level to Europe-wide level. I have no strong view as to which is the best way to do it, other than perhaps to say that there is a case to be made for nationally responsive regulation. For example, the New Zealand Government have obligations to our indigenous population under the Treaty of Waitangi, and considerations like Māori data sovereignty have been a growing issue. I suspect that is very much a horses for courses thing.

In terms of soft law, we have a piecemeal approach across government. A few government agencies are doing a pretty good job in putting self-regulatory mechanisms in place. It would appear that others are a bit slower to get off the blocks in that sense. Moves are underfoot to try to bring about some sort of consistency across the state sector in that regard. That is where we stand at the moment.

The Chair: Thank you very much.

Q44 **Lord Blunkett:** My question about transparency mechanisms has already been fairly thrashed to death. I want to try to ask a very simple question to all three of you. By the way, Professor Joh, my youngest son is coming as a student to California in two-weeks' time. I will frighten him to death by telling him that there will be seminars at 3 am that he will have to attend.

My question is very simple. Professor Joh, you mentioned the withdrawal of particular predictive mechanisms at one of the smaller police forces. Has there been

a reliance in all three of your jurisdictions on people taking legal action when particular mechanisms, such as predictive technology or algorithms, have been used in a court case that they have been involved in or in a class action?

The Chair: Are you stumped?

Professor Elizabeth Joh: This is a wonderful question. I think what we are beginning to see is limited, individual cases where individuals who are being criminally prosecuted are raising questions about a particular technology that has been used against them and trying to find out something about how that technology is being used. We do see some of these cases; they have not yet been resolved at a high level, for example by the United States Supreme Court. However, I think most American legal experts working in this area would agree that the United States Supreme Court will eventually look at how some of these new technologies ought to be reconciled with the traditional manner in which American federal constitutional law has regulated ordinary law enforcement.

We see some attempts—not class actions but other types of lawsuits—with respect to state and national public-disclosure laws. For example, media organisations have attempted to find out the details of a particular technology. Despite the fact that there is broad use of this, as of yet there have not been too many significant or major legal cases in the United States opining as to the desirability and the nature of legal regulation with respect to these kinds of technologies.

As for anticipatory regulation, there has been some, again at the very local level. We are at a bit of a mismatch. A mass proliferation of lots of different kinds of technologies, and slow responses on the part of individuals or local governments.

I have one last point. Part of this—and this is just a guess of my own—is that it is often very difficult for individual criminal defendants even to know what types of technologies might have been used in their particular case. Of course, that adds to the difficulty of raising challenges to a particular technology when you are not even sure what combination of licence plate reader data, facial recognition technology or predictive policing software might have led to the identification of you as a particular suspect. That gets to some of the transparency questions that are being raised here this morning.

The Chair: On that last point, you would not have been able to hear, but it provoked a lot of, “Yes” and, “That’s right”, and nods from around the room. We have different legal systems, but that is a common factor. Do either of the other witnesses want to add to that or have we have covered it? No, it does not look like it. Lord Ricketts next.

Q45 **Lord Ricketts:** Thank you very much indeed for a very interesting discussion. We have talked about decisions taken on regulation in particular. Professor Joh, you have talked about the hyper-local level at which these decisions are taken. We are also interested in procurement of the systems and whether the procurement decisions are also being taken at local level and dispersed differently around

different countries. How can we be sure that the authorities that are doing the procurement are competent, that they understand what they are procuring, that there are arrangements in place so that the handling of the data they receive is going to be transparent, and who even owns the data? In a world of deregulated and disseminated decision-making, how do you ensure that these procurement decisions are being made well? Again, can we start with Professor Joh, since probably the US is further ahead than other countries on this?

Professor Elizabeth Joh: That is an excellent question. In the United States, I think the short answer to your question is that we do not know how these things are happening or whether they are competent decision-makers. Again, there are some movements around the edges to try to respond to this but, for the most part, these products, these new technologies, tend to be made and developed within the private sector. If you are a local police department accountable to your local city council or the local mayor, you may be approached by a company that says, "We would like to offer you a deeply discounted product. Would you like to pilot it? We would like to offer you something for free".

Perhaps the most notable example in the United States was a few years ago when the largest manufacturer of police body-worn cameras made a big splash in the United States by offering a year of free body-worn cameras to any police department in the United States that wanted them. Of course, it would be the rare police department that would not be tempted by that offer, given the financial constraints that any government agency has, particularly at the local level. We saw mass adoption; a lot of adoption ensued as a result of that offer.

Of course, no free offer is ever truly free, and those body cameras came with an obligation to be a part of the data and ecosystem of that large body-camera manufacturer, which included being obligated to use the company's software and to store that data with the company's servers. After the year of free body cameras, the analogy one might use here is using a shaver and a razor blade or a printer and a cartridge. It did not matter to the company so much that the cameras were free. After a year, many of these police departments presumably felt obligated to keep going, because they had produced so much body-camera video that was now part of this data ecosystem. That just happened, without necessarily a lot of oversight or thinking ahead of time at all on the part of local governments or police departments. To me, that is a perfect example that perhaps there is not a lot of foresight going on.

Lord Ricketts: There was no competitiveness in that tender and probably no clarity about who owns the data at the end of the contract. It has many risks, I would think. Is there a New Zealand experience here in what is good practice on procurement of these systems?

Professor Colin Gavaghan: There perhaps is. In 2018, Statistics New Zealand, which is a department of government, commissioned a kind of stocktake of what was happening across the public sector, which was the first snapshot we ever got. What they found was that a lot of the algorithms used in government were being

developed in-house within those government departments. Where they were purchased from external vendors, they tended to be bespoke products that were developed for a particular purpose, rather than off-the-shelf. By far the most common practice was what they called a mixed model of procurement, which involved contracting external expertise into an internal development process rather than buying a ready-made product from those developers.

I think that has been quite a good model for us. An example of what can go wrong with the off-the-shelf model was what we saw with the police facial recognition technology trial last year, where the algorithm simply was no use at recognising Māori or Pacific Island faces, probably because the dataset that it had been trained on did not contain many such faces.

There are also concerns about compliance with our privacy and discrimination laws, and such like. I have had a chance to speak to the private sector consultants that the Government work with, and the ones that our Government have been using have been very committed to openness. In fact, if anything, it has been the government departments that have pushed for a little bit more downlow about how exactly certain things are happening.

So far, I would say that it has been a fairly happy story, but some of these questions persist about who is evaluating these tools for accuracy and what happens to the data at the end of the life cycle of the project. Those things are probably as true here as they are anywhere. The fact that most of the development is taking place at least partially in-house should, in theory, give us a bit more control over these variables.

Lord Ricketts: Dr Van Brakel, do you want to add to that, briefly?

Dr Rosamunde Van Brakel: In Belgium, it is very unclear how procurement is done. There is no transparency about the rules and whether the police have to abide by certain steps in procurement. It is all very unclear and there is no public information to be found about how decisions are made. What I would like to raise here is that a very important factor for the people who are involved in these procurements is having the expertise to understand what technology companies are telling them and what the companies are promising the technology will do. That is a very important factor: the expertise of the people involved in the procurement process.

Another factor I see happening across Europe, and in Belgium, is that the police are opting not to buy technology from American companies but are developing the technology themselves. For example, the police in Amsterdam hired a data miner to create predictive policing software, so it was developed by the police. In Belgium, the Government are financing a professor at the University of Ghent to develop a predictive policing algorithm. I see there is a movement towards trying to develop these technologies and there could be some best practices, especially if it is being done in an open-sourced way so that scrutiny of the algorithm is possible, but I cannot give you a concrete example where this has happened.

Q46 **Lord Dholakia:** We have heard that human operators must understand the limitations of technology—as well as its opportunities—to avoid relying excessively on it or misinterpreting interest outputs. Have you come across examples from your respective jurisdictions in which human machine interaction has been particularly problematic or particularly successful? What would help me most is to understand how relevant the technology is when there is a considerable deteriorating relationship between the police and the community in some of the jurisdictions that you represent?

The Chair: Can we start with Professor Gavaghan, because he has referred to this already?

Professor Colin Gavaghan: I am not aware of any evidence of either good or bad examples specifically in New Zealand. We still do not have a very rich set of data on that point. There are certainly efforts under way in government to mitigate the dangers of algorithm bias and so on. The early initiative in the form of the algorithm charter, which is a quasi-voluntary document for government agencies to sign up to, serves to try to remind decision-makers of the danger of becoming too differential to an algorithmic decision where a human is supposed to be exercising meaningful scrutiny.

That is going to be one of the tricky things. There is the danger of what we might call a regulatory placebo, if we simply think that having a human in the loop—there is a lot of excitement about that term—is a guarantee of meaningful scrutiny. Whether a human will be able to exercise meaningful scrutiny very much depends on the capacity and awareness of the human in the loop. That is a very general observation. I cannot honestly say that I have any specific findings from this jurisdiction.

The Chair: I was thinking about your reference to the Māori population, but we can perhaps come back to that in a minute or two.

Professor Elizabeth Joh: I have an anecdote that may not seem obvious here—I will explain it in a moment—about where the human machine interface can go badly wrong. The story is that last year there was widespread reporting on what is likely to be one of the first wrongful arrests based on facial recognition technology. This occurred in a relatively ordinary criminal case in the state of Michigan.

A man was incorrectly identified and arrested by facial recognition technology. In this case, there was an image from the store's security camera in a case of shoplifting. That image was then fed into a facial recognition programme relied upon by the state and local police. It just so happened that this algorithm provided by a private company was among those identified in a federal study as tending to identify black and Asian faces erroneously at a far higher rate than white faces.

Where is the human interface, the interaction? In this kind of situation, the programme spits out a number of possible leads and they are supposed to be investigative leads. One might imagine that the next step would be that the local

police would then use their traditional or conventional techniques to follow up on this automated result. It appears from the reporting on the case that, rather than continue, there was simply just human trust that one of the pictures must be right. One of the pictures was simply put in a photo line-up and provided to the security manager in this private store. The man was identified this way and wrongfully arrested as a result, a mistake which the police later admitted.

That is a perfect example of the overreliance on machine decision-making. It seems quite ordinary, but there was really no human follow up other than at the tail end seeing some human beings participating in some way. One can think of how this gets magnified in hundreds or thousands of examples, in all kinds of cases, where there is a sense in which there is a hit from automatic number recognition or from facial recognition technology and that leads directly to an investigative stop of a person on the street or of a car. This one Detroit example, in Michigan, has been particularly relevant for a question like this.

Dr Rosamunde Van Brakel: I do not have any cases in Belgium that I can say anything about. There is no evidence. As I said before, no systematic evaluations are taking place. As my New Zealand colleague also said, there is too little data to make good assessments in this regard.

However, in my research and speaking to police officers in the context of predictive policing, I have noticed that there is a lot of resistance from police officers on the ground about having to follow what the algorithm says to do. They feel that their instinctive, gut feeling about going to a certain neighbourhood, their expertise, is being ignored. In some cases, they have stopped using it, because so many police officers did not like to use it in that respect.

What you see happening is that in cases where they still feel it is useful, the human factor becomes more important again and there is more discretion. What you see with the danger of overreliance on technologies is that the discretion of the police officer starts to disappear. I think that is an interesting aspect here.

The Chair: The cultures in different societies and different police forces is a new factor. Thank you.

Q47 **Baroness Chakrabarti:** You have now all touched on the question of societal bias, but I want to give you a final opportunity to develop it a bit further. Professor Gavaghan talked about the dangers of baking bias into algorithms, and Professor Joh gave the story about facial recognition just now. I am interested in the murky territory between what might be seen as acceptable profiling or risk assessment on the one hand and things that we think of as unacceptable baking in of bias on the other.

It is widely accepted that insurance companies should be able to take age and health status into account for setting premiums or deciding whether someone should be insured, but we would not accept health and age as determinative or even highly probative of your guilt in a criminal courtroom.

Given that so much of this technology is about a range of stages in the policing and intelligence field before you even get to a courtroom, is there a way to delineate between acceptable and unacceptable bias/risk assessment/profiling?

Dr Rosamunde Van Brakel: In the context of critics of policing, for example, the data that is often used is arrests data, and it has become very clear that this data is biased, especially as a result of ethnic profiling by the police. As long as this data has this societal bias baked in, the software will always be biased.

The first step here is not a technological question, it is a question about how policing and social practices are already discriminatory or are already biased. I do not think you can solve this issue by tweaking the technology or trying to find AI to spot bias. You can solve it only if you solve the issues that are already there within policing. Here it is essential that the practices in which technology is embedded are taken up in this assessment where biases occur.

In addition, profiling is inherently biased and discriminatory. That is an essential part of how risk assessments and profiling work. The only way to use these technologies in a democratic and race-respecting way is to start with your policy stating this very clearly: "We know it is discriminatory. Is there a context where it is proportional to use it?" Then you make sure that the safeguards are in place in a lifecycle way; you make sure that there are safeguards before deciding to use it during the implementation and afterwards.

As I have said before, in Belgium no systematic evaluations take place, so we cannot say whether the technology is working, whether its use is proportionate, or even whether it is violating people's rights. Also, traditional evaluations have always focused on how effective the prediction is. I feel that these evaluations need to be expanded to include impacts on society and communities and, as has been said before, also to get the affected communities involved in the policy decisions about implementing the technologies.

Professor Elizabeth Joh: I know that time is of the essence here, so I will be quick. I agree with everything that has just been said. I do not think there is a contrast between insurance and policing, particularly for some communities. I will just speak for the American experience. In fact, we are seeing across the board that for many people it is a nightmare that the lifecycle of their data lives is separate from them. They have created it, but they have no control over it and whether it will be used to see whether they have creditworthiness for a loan, whether they are going to be stopped by the police, whether theirs is the appropriate resumé that rises to the top of the pile.

We are looking at one sector of society in which risk assessment is particularly problematic because of the liberty concerns, but those concerns are also now being echoed throughout the social sphere. So instead of thinking about this in terms of policing versus risk assessment, I would pose that question somewhat differently and think about how this is just one instance of a society-wide problem.

Professor Colin Gavaghan: I will also try to keep this brief. Yes, actuarial justice is just a fact of life, whether it is bail considerations, parole, preventive detention or anything else. The problems to which this give rise are not novel to EDM systems or algorithms. There is a danger, though, of dirty data; there is a danger that historical bias will be replicated to reinforce.

I will just give two quick examples of things that have been done in New Zealand. One has worked quite well and the other perhaps less so. We have an algorithm that is supposed to predict future offending called RoC*RoI. In an attempt to try to break the cycle of repeating bias, the ethnicity variable, which used to form a part of that algorithm, was set to zero. Effectively, it was removed from the algorithm. What was discovered at that point was that it made no difference whatsoever.

That was initially acclaimed as being a good thing, because clearly ethnicity had not been playing an important part. However, there is entirely another way to look at that, which is that other variables stand as very close proxies for ethnicity, whether that be geographical area or whatever else. In attempts to clean the data, we have to be quite careful that it is cleaning not just the completely obviously things but those that act as proxies for them.

A better example, perhaps, is the trial of the predictive policing tool in New Zealand, the deployment to crime hotspots, which is obviously very prone to self-fulfilling prophecies and feedback loops. If you send lots of cops to an area, you will find lots of crime. A way to break that loop, which is identified in the USA and has been used here, is to feedback into the algorithm only reported rather than detected crime—a crime reported by other people, not that found by the police officers.

The hope there is that, in doing that, it will break the cycle whereby identifying an area as a crime hotspot means that it is more likely that they will find evidence that supports the conclusion that it is a crime hotspot and we get locked into this permanent feedback loop. There is some quite good thinking going on about that in New Zealand and elsewhere.

Q48 **Lord Hunt of Wirral:** We have had some very valuable insights into the uses of technologies in other jurisdictions. If I may, I will just turn the spotlight upon us here and ask Professor Joh whether, seen from California, there is anything particularly noteworthy about the way advanced technologies have been used, or perhaps not used, for the application of the law in England and Wales.

Professor Elizabeth Joh: From my limited experience and observation, one of the things to note is just how early surveillance became ubiquitous in England and Wales, and how the public have become inured to that. It has been fascinating in this morning's discussion to hear about public mistrust, public questions and things of that nature.

Another part of this is thinking about the extent to which the public simply becomes inured many of the uses of these technologies. I do not have a ready analysis for that other than to say that, with regard to surveillance cameras—the sorts of things

that have happened on a mass scale—one can look to England and Wales and see how quickly they have been deployed and become normalised. Certainly, that has been the case in the United States as well.

Lord Hunt of Wirral: Professor Gavaghan, the issue seen from New Zealand.

Professor Colin Gavaghan: We look very significantly to the UK. Our legal system is very strongly based on the English legal system, so we are always watching what is going on there. Obviously the recent Bridges case involving facial recognition technology used by south Wales constabulary has no direct application to our legal system, but it is certainly something we would look to learn from.

Regarding the overall regulatory terrain of this technology, I think we are quite envious of some of things that have been set up in the UK. We would love to have the resources and a team as big and competent as the Centre for Data Ethics and Innovation. We talk to them quite a lot. Some of the think tanks that have been established, like the Ada Lovelace Institute and the Alan Turing Institute, are very impressive.

We do look a lot to the UK for guidance and for information, but I think we are all probably at an early stage in this journey and what that settles to is not entirely clear to anybody yet. That is what I would say about it.

Lord Hunt of Wirral: Dr Van Brakel, the view from Brussels.

Dr Rosamunde Van Brakel: What is very interesting in the UK—I will give one example, because I have been looking at how oversight has been organised in Belgium but also beyond—is the establishment and development at the West Midlands Police of an interdisciplinary ethics committee on new technologies. That was established by the police themselves. That is a very interesting way forward and should be watched by several other countries to see whether this is a model that could be interesting to copy. I have said before that in Belgium the focus is very much on oversight of a narrow interpretation of data protection, and I feel that this ethics committee takes into account a much broader perspective in assessing what the police are doing and experimenting with.

The Chair: I should declare an interest in that the chair of that committee, Dr Oswald, is advising this committee. We are very glad to have her, not physically in the room but I know that she is watching.

Q49 **Baroness Primarolo:** Thank you very much. It has been an absolutely fascinating session so far, as well as incredibly challenging, and I am trying to bring my thoughts together. Could you identify, in each of your jurisdictions, lessons that are important for us to keep at the front of our minds as we are working on this inquiry with the development of technologies here in the UK? Chair, I would also like to come back and ask a specific question of Rosamunde after we have had the answer. It does not have to be one lesson, but are there some key points—you have touched on many—that we absolutely must stay focused on?

Professor Elizabeth Joh: I would like to use this opportunity to raise a point that has not yet been raised. In the United States, the one important lesson that I think we are slowly coming to terms with as an enormous problem is the blurred line between public and private. This Committee seems to be focused on the use of technologies by law enforcement and government agencies, for example, but the American experience has been one in which there is increasingly not much distinction between public and private.

There is formally, as a matter of law, of course, but practically speaking that line is becoming disintegrated. In particular, in the United States, I am referring to the ability of government to buy outright what they cannot easily access directly. For example, in the United States the Government may be required to seek a warrant or be required to adhere to other statutory or constitutional law restrictions before collecting information from persons or entities. This today can be easily circumvented by simply purchasing that very same data, or similar data, when the Government act as a customer in the private marketplace, thereby creating not just a loophole but enormous end run around the normal restrictions that we would expect of government.

That is true from just purchasing things like large blocks or tranches of mobile phone location data, licence plate data, accessing it through direct arrangements with private individuals who have their own security cameras with facial recognition technology, and simply making private arrangements.

There is an urgency in the United States to try to address this problem. I do not know how this will be addressed in other jurisdictions, but simply focusing on the Government in their traditional sense is a very limited view of how to think about the problem of new technologies.

Baroness Primarolo: Thank you. That would take us in the UK straight into the same debate that Belgium would be in, which is this whole question of data collection, whether it is private or public sector, and the interactions of the GDPR and the law enforcement directives, for example. That is quite difficult to break into in terms of the very important points you have made about privacy, discrimination, accountability and transparency.

Rosamunde, do you have some examples or thoughts of how we should proceed in that way, bearing in mind that a lot of the information comes from the private sector and it has been collected in all sorts of ways that we do not know?

Dr Rosamunde Van Brakel: Specifically concerning the data collection from the private sector, I feel that currently, at least in Europe and in Belgium, there is insufficient regulation with respect to private companies. There is very little control about what the private companies will be doing with the data. There is very little transparency. I feel that there is a lot of work to be done here and that the current proposal of the European AI regulation is not strict enough in that respect. It is still giving private companies too much power because of the self-regulation route that the regulation has taken.

Concerning the general question, there are lessons learned from Belgium that I would like to emphasise. One of the things that has come to light in Belgium with implementing the new technologies, especially when it comes to big data and using AI, is that there are a lot of very interesting ideas and potential for doing this for the police. However, there is very little expertise on how to turn all this data into actionable knowledge that they can use for their work. On the one hand, there are not enough people who have this expertise involved in these decisions and, secondly, there is not enough reflection about how the technologies will fit into the police work. There is a lot of enthusiasm and hope that these technologies will do a lot of good, but there needs to be much more reflection on what impacts they will have on police and especially on society.

Baroness Primarolo: Finally, briefly, Colin, did you want to add any lessons?

Professor Colin Gavaghan: Maybe just the notion that there are certain regulatory tensions at play in this area that might be hard to avoid. On the one hand, we are concerned about the misuse of data, but sometimes that has been set off against considerations of accuracy.

If I can go back to the facial recognition algorithm that the police were trialling last year, which did not work well with Māori and Pacific faces, the next question became how we address that gap. Attention turned to the possibility of where we would find a good data resource of Māori faces—perhaps the driving licence database or the passport database. That is problematic, because people do not give up their pictures in order to train a police database. We have this inherent tension: how do we make the algorithm better without tapping into private data that was not intended for that purpose? Some of these tensions are going to be very hard to avoid altogether. There are going to be some hard choices to make.

Q50 **Baroness Sanderson of Welton:** Thank you very much, everyone. I have a couple of very quick questions for Professor Gavaghan. You mentioned earlier all sorts of mechanisms that would enable those that are likely to be most affected by this technology to get involved and that it not be a tick-box exercise. Could you give us a couple of examples of those? It might be quite useful to know how you do that? Presumably bringing people on board very early on would be one answer.

Secondly, very quickly, we have been told that you are scaling back in New Zealand on the use of DNA technologies because the costs are outweighing the benefits. I am interested to know if there is anything you can tell us on that.

Professor Colin Gavaghan: First one first, you are absolutely right: it is very important to have people from those communities involved at an early stage. What we are seeing in New Zealand and in other jurisdictions is an initial triaging of algorithms into high need or low risk or something like that, some kind of classification of that nature. The degree of regulatory scrutiny they receive will depend on that initial classification. This is where I think having scrutiny by the people likely to be most diversely affected by them at that stage is pretty critical.

The danger is that, otherwise, people like me will evaluate them as low risk and they will not receive the degree of scrutiny that is required by that. That is certainly one thing I would say. Evaluation is not just for compliance with legal and ethical standards but simply for accuracy. We have found some quite alarming statistics and not only for the algorithms that have been evaluated. For those that it is even proposed are evaluated, it is something like one in five. That process is going to be very important.

If we are going to be serious about involving marginalised communities, there will have to be an investment in developing capacity and skills in those communities. We have a fairly small number of Māori data scientists in New Zealand who are stretched very thinly because the demands being put on their time are astonishing, and there is recognition that we need to start investing in that capacity fairly early.

There has to be an ongoing scrutiny. It cannot be a one time for all time, because these problems can creep back in.

Regarding our use of DNA evidence, I am afraid my knowledge is not very much greater than your own in that regard. I have heard much the same, but I do not have a great deal to add to that, I am afraid, sorry.

Baroness Sanderson of Welton: No, thank you, that was very useful.

Q51 **Baroness Kennedy of The Shaws:** This is one that I am sure can be answered by Professor Joh. You mentioned in an aside that some technologies should not be used at all. Is there anything on the horizon that you see as falling into that category that we should be alert to?

Professor Elizabeth Joh: I do not have anything in particular that is on the near horizon. I do think of it as a question that should be asked in every instance. If we were to hypothesise about the middle distance, we would want to be cautious about any automation in policing that would be combined with real action with robotics—anything that would involve some sort of automated decision-making, perhaps with a drone carrying out some assessment or some on-the-ground robotic system to do that.

There, you have an instance in which real questions ought to be asked about whether such use of new technology, even if there were some human interface at the end, is worth it given the cost, the errors, and even dangerous literal fatal errors in the United States where police have used firearms. Civilian fatalities are a large issue in the United States. Those are the kinds of things I am speaking of.

I cannot think of anything in particular right now. In the US, there are some calls. In my very own state, for example, there is a temporary ban on facial recognition technology. I do not think that is likely to be long-lived, so it does not qualify as one of those technologies that will not be used at all. Rather, we are in the process of thinking about how to deploy those technologies in a way that makes more sense.

The Chair: Thank you very much. Many thanks to all of you. It has been suggested

that I should ask you—I am not going to, though—what worries you so much that it keeps you up at night. Well, we have been keeping you up at night.

I will, if I may, ask you after this meeting if you could let us have any thoughts that you might have on the transparency issue of how information can be made available to the public in a comprehensive, explicable fashion. It is something that is exercising all of us in this room in Westminster as well as you.

Let me end this part of the evidence by thanking you very much. If there is anything more than that you would like to come back to us on, please do. We are very grateful, indeed. Thank you for staying up.