Transcript

Recording	Welcome. You're listening to a recording of the society 4.0 symposium 2019, where we explore the development, maintenance, loss, and restoration of trust in the digital age. This is the panel discussion on law and justice, which took place on the Swinburne University of Technology campus, and was introduced by Associate Professor Diane Sivasubramaniam
Diane	We're going to jump right into our first theme of the day, which is justice. We have Ryan Young, who is the director of the national security college futures hub, at the ANU. Ryan recently completed a report in collaboration with the AFP about how crime is evolving in the digital age, what crime will look like in 2030, and how the police force will have to look to deal with that crime. He's also done some fascinating work lately on shifting public attitudes to privacy and the implications of that shift. Nicole Batch is protections manager in the migration support programs of the Australian Red Cross, and she'll be talking to us about issues around trust and justice in relation to asylum seekers and refugees, and how emerging technologies play into humanitarian action. Bob Bolia is from defence science and technology. He is the research leader for aerospace systems effectiveness and the lead for the defence science and technology strategic research initiative on trusted autonomous systems. We also have a few special guests in the audience who might make comments as the panel discussion evolves. We have Michelle [01:34 ?Righters] from RMIT, who's the director of the bridge of hope innocence initiative. Marilyn McMahon from Deakin law school, and Jennifer Beaudry from psychology sciences at Swinburne. And comments today are going to be facilitated by Lynne Haultain who is formally an ABC radio journalist, including some time hosting the law report on radio national and Lynne is currently the executive director of the Victoria law foundation. I'm so excited to hear what this panel have to say! Would you please join me in welcoming the panel (applause)

Lynne	Thank you Diane and good morning everybody, I'm Lynne. Great to be with you. Um, I'm very pleased that our special commentators are in the front row, saves me having to find you in the crowd! Thank you all for joining us. I'm going to ask you all to just briefly respond to the comments that Diane has just made, by way of locating her thinking in your worlds. Nic, do you want to start?
Nicole	Yeah I think it's, there's a lot of really interesting threads for us to pick up on I think, when we talk about a belief in a just world, the majority of my work is done is a migration sphere, and I guess we can, we live with the realisation that it's not a just world for people globally, that things are not distributed equally, and how things are rationalised and decided procedurally are quite complex and messy, and very difficult for some people. I guess for the Red Cross our focus is on the most vulnerable people that suffer as a result of that and how we can support them. So there's a few things that we can touch on in relation to that but it's quite a minefield of areas to reflect on here
Lynne	Yeah, it's going to be an interesting conversation, we could go in 15 million different directions!
Ryan	Absolutely. I thought it was interesting looking at the kind of procedural justice notion Diane was talking about, thinking about the legal and personal aspects to that. In the legal sense, procedural justice is designed in a sense to get better justice outcomes. Whereas the procedural personal psychological thing seems to be far more about being treated with respect. And those two things are often at odds with each other. You get a witness statement from the police, you know the personal procedural justice is you want to be believed, you want to be taken seriously. But in terms of the legal procedural justice, the police have to be sceptical about everything they hear in order to try and get better outcomes in the end. So I think there's an interesting tension there that may well be relevant in this discussion
Bob	Yeah I think in the defence context Diane talked about things like public trust in institutions. And I think in Australia, the Australian defence force has quite a high level of public trust. But in order to maintain that I think it's pretty important that the people see it as a just institution. When you talk about introducing autonomous systems and other modern technologies into the battlefield, I think that becomes an issue. I think military conflict is governed by international humanitarian law and the laws around conflict, which requires things like distinction and proportionality judgements, and it's going to be interesting to see how we can evolve autonomous systems that are able to comply with that
Lynne	We heard earlier the concept of trust, and then we moved to justice, and threads about political philosophy also sort of flow into that, you start with the social contract and the notion that it's a deal basically between the individual and the state. We accept these constraints because its broadly in our interests. But that notion of trust and I think the intertwine between those two concepts is undeniable. We saw some evidence interestingly around levels of trust around science, but when it comes to those sorts of really high tech capacities and technologies that we're beginning to see play out in all the domains that you guys work in, do you explore that in your work Robert, how well it goes down? About

	whether or not people are trusting of military and defence type applications? Is that relevant?
Bob	Yeah definitely is relevant. We have a lot of work in trust and autonomous systems. And part of the reason for that is in the military you're making life and death decisions and you don't want to leave that to a system that you don't understand. So there's trust in the sense of, we talk about explainable AI and the problem is in machinable learning systems, things like convolutional neural networks, what you get is a classification, a decision. Is this a target, is it not a target? But if you cant explain to the operator how it arrived at that decision, there's a chance that the operator wont trust it
Lynne	And therefore will do what?
Bob	Well we try to design systems that will allow some element of traceability in them, or at least systems that have a sufficient reliability that the operator can trust them. But we're exploring at a more basic level how this plays out in basic research with human subjects, where we vary the availability of autonomy and see how they respond, so we're looking at what sort of things lead to trustworthy systems
Lynne	Ryan, you've done a lot of work on trust and in particular in institutions and how people perceive the relevant or relative trustworthiness. Where are you at now with that thinking? Because I think all the sort of trust barometers suggest it's all plummeting and we don't believe government and we don't believe very many people beyond health
Ryan	Um I think, I mean the big picture story is that trust in institutions is plummeting, but the actual story is a bit more nuanced and complicated than that. For example, people – we did some research looking at trust in terms of privacy and data. And trust in government is actually pretty high, kind of around 60-70% trust government with their data. It's not as high as health, interest and the banks is still up there. Social media companies were way way way down the bottom, around 10% of people actually trust them with their data. But then that's really interesting because there isn't a mass movement to get off Facebook, despite the fact we don't trust them with our data. So I think partly the story is people are a bit more nuanced and distinguishing in how they trust. Banks are an interesting commission, we just had the royal commission and no one trusts banks, except everyone trusts banks with their personal information with their bank account with their money. And I think that's partly because banks treat you differently. Recently I saw Commonwealth bank, their systems went down, and so what did they do in response? Apparently I've got some free money in my bank account, 50 bucks or something for everyone that was affected by this – apparently, I saw it on the news. They really try, they almost recognise that they will fail but they recognise, they do something better out of it. I mean governments tend to be not very good at doing that sort of thing, so I think there's interesting nuances. Social media, people don't trust them, but I think that they feel like they have more control over the information they give to social media, as opposed to what they give to the tax office, so I think its different

Lynne	Some of this is about ignorance, we don't know what we don't know about some, like social media are up to. Some of it is about trade off, the fact of the social contract or the commercial contract in this instance, we're prepared to put on our GPS tracking for Google because it helps with maps. We're prepared to give Facebook certain information because that means we get sent info about whatever holiday we want to take
Ryan	Absolutely, but also Google tells you that you can go and get your entire, all the data that Google has on you, you can go and get it. So that means at least Google's policy is to be kind of open and clear (laughter) – I'm not saying they are!
Lynne	And then yesterday they get, well they're under investigation by the ACCC
Ryan	Absolutely. What's interesting is how they maintain and build that trust, there's a bit more of a two way relationship with them than with a lot of others. I think what's really interesting is dealing with government agencies, for example the classic types, police for example, government agencies, universities, we assume people trust us if we're a government agency. That's been true for a long time, we take that for granted. I think banks, people think they cant trust them, so they're working hard to try and make sure people do trust them, so there's an interesting difference in the way that works
Lynne	I'm not sure that the people in your world Nic, recognise the trust in government or institutions
Nicole	Yeah you're absolutely Lynne, I think we're dealing with very different parts of the world and different communities in the world. Certainly people we are dealing with in the humanitarian sector have usually had their trust broken by the government or by other things happening in the world that means they cant trust those that we might be able to here in Australia. And I think one of the things the humanitarian sector does is we have to rely on trust and people, we have to be upfront about what we can do, what we cant do, and everyone has to make sure we look after people's information very carefully and do no harm with that. I think the emergence of digital technology and digital identity gives us a really interesting look into this challenge. I work in the area of trying to find family members who have gone missing, so family members are looking for each other, having digital identities and data sets available to us really changes the game for us. But we need to make sure that people continue to trust the Red Cross as a safe place to store their information. We do a lot of work around our code of conduct and how we behave and our systems, along with having states trust us. We have to exchange data globally, not every state has a regulatory system that looks after data protection in the way vulnerable people need it. So there's a whole lot of layers that we're working through to make sure we can continue to be trusted by people. We can give them what they need to try and help look after their safety and dignity and so what they're asking of us, and work with states to make sure that we can continue to do that as well
Lynne	I mean the Red Cross is a fascinating example, because for the entirety of it's history it's had to walk that line, around looking around of the micro or the individual as well as negotiating with state, some of whom have been extremely um, critical and

	unaccepting of the Red Cross's role. So it's a diplomatic line that you walk as a matter of course.
Nicole	Yeah that's right, and I think the humanitarian space that we can really negotiate is really fascinating. I think one of the examples of that that's really pertinent is our work in monitoring the conditions of immigration detention. We've had continual access to places of immigration detention in Australia for 28 years, and we have confidential dialogue with government about what we see in detention. So we have trust from the authorities to do that work. I was asked recently if we have trust from the people in detention to talk to us, and how do they know they can trust us? And my answer to that is people keep talking to us, and we're very clear about what we cant do, and they tell us things they want us to know and we're very clear to act on that. I think it's an example of showing where some accountability mechanisms do make people behave better. If we weren't there, what else might be happening?
Lynne	I'm really interested, because I think as per industrial revolution 4.0 that we are in this state of extraordinary flux around the lines of accountability and trust in institutions. And the blurring of that division between the institutional and the commercial, we are confused about the relationships we have to have. In the past, institutions have been the agencies where we've felt the need to impart our information, but now we do it as a matter of course. With commercial and social media being the classic case. So the lines are blurring, and our comprehension of what's fair and reasonable in that relationship is really messy now. Ryan, have you got thoughts on that? And the responsibilities – I don't know what's fair to expect from Facebook or Google or Twitter or anyone else any longer and I really, I think that effects our relationships with major retailers and banks as well. How much information we're giving them, what are they using it for, and whether or not that's reasonable
Ryan	I mean I think yes, the point that it's messy is really really relevant. Particularly the international element of it too, in terms of we're used to dealing with a framework and regulations which are Australian, and we can kind of trust the Australian regulations, you know, most of these commercial operators are based somewhere else. Different systems, different laws, different regulations, may or may not have the same safeguards. So it's a whole lot more complex and messy. I agree people don't quite understand what that works. We in our research looking at data and privacy talked about, I think what people are looking for out of what they do with their data. And one of those things was the idea of clarity. The organisations that tell people clearly in ways they can understand what they do with the data gained the most trust. Whether or not they're telling the truth is a different question. But I think that's a really interesting dynamic, that a lot of big tech companies do really well, they have a really nice statement of what you can expect from them. Another aspect is I think people do want that procedural justice that Diane was talking about, they want to be treated with respect, they want to be treated with care and respect and be listened to. I think people in general understand that you cant control your data anymore, as long as they feel treated with care and respect – one interesting thing we discovered was that injustice system, if you give your data to someone you're kind of implicitly agreeing you can use it for the same types of things you signed up for. If they take that data and do something very different,

there's often, people turn into monkeys, throwing… so Google ran into that when they were in Gmail. They started scanning peoples emails so they could target ads to people. From Google's point of view, they're just delivering a better advertising service that's actually relevant to people. They pulled it because there was such an outcry over it, because people were taking, you know, Google is reading my email to sell me ads, that's very different and very - so it was that visceral reaction to the injustice there I thought was really quite interesting connected back to the injustice. In terms of, I mean I think people are looking for leads in this space, they're not quite sure how to deal with it, not even sure what's relevant to Australians and overseas, particular when our media shows a lot of what's happening overseas as well

Lynne	Robert, do you use Alexa or Siri?
Bob	No, I never do (laughter)
Lynne	Why not?
Bob	I don't know, I'm kind of a luddite when it comes to technology. I use my phone for – I don't really talk to any devices. I use my phone for data, I almost never use it as a phone
Lynne	And is there a philosophical position in that?
Bob	No, not really (laughter)
Lynne	So you're not concerned about being survielled?
Bob	Ah, I probably should be concerned but I'm not, I don't really think about that much
Lynne	So what about, I mean Ryan mentioned global conglomerate military complex, industrial complex and it's various manifestations. How does that play in your world, and what kind of national constraints or limitations are there on activity and in the defence field, or has it become globalised without us really realising?
Bob	Well for us defence is largely globalised because we don't have that much of a defence industry in Australia. So in terms of major air force platforms, major naval platforms – I mean, we do build ships in Australia, but we don't build fighter jets and things like that, so we tend to buy them from United States and Europe, so that's all very globalised, and that is a significant concern to us, not necessarily having sovereign access to our data
Lynne	And by concern to us, you mean who?
Bob	The Australian defence force
Lynne	And the Australian people
Bob	And the Australian people
Lynne	When they think about it!

Bob	Of course. But you also bought up earlier the issue of accountability and I think that's quite an interesting one, because if you think about a situation in which for example a civilian was accidentally targeted by a system that has a high degree of autonomy in it, the question becomes who to blame for that, and people will want someone to blame, want someone to be punished in some way, to be held responsible. And if you hold responsible the soldier or sailor who made the system, the commander, the programmer, the defence contractor that built the system? And I don't think there's any kind of policy around these complex issues at this stage and I think that's going to have to be developed. But there's also going to have to be an understanding about what the public will expect and accept in those circumstances
Lynne	So it brings to mind, I wish I could remember the name of the film, but the film about the drone operator in some bunker in a desert in Arizona, responsible for drone attacks in the Middle East or wherever it was. I mean that sort of distance between operator and tech is growing and growing isn't it?
Bob	It is growing. Although there's not really any autonomy in their systems, it just a teleoperated system. So it keeps the individual out of harms way that's actually flying the way, although it's not always the case that it keeps them out of emotional harm's way. Because a lot of the research on killing suggests the reasons get things like post traumatic stress syndrome in war, it's not because they're afraid of being killed, it's because of the act of killing itself
Lynne	So what's the research around how to create systems or chains of responsibility that addresses that? Is there one?
Bob	I think it's still early days actually, there's not a lot in that at this stage. I think one of the things you see in films, you get the impression from Youtube videos and things like that that killer robots are a thing, or that they're just a year or two away, a lot of the impressive gains that have been made that you see in the media are in areas like machine learning. These are problems that computers are very good at solving when given a lot of data. It can classify and tell the difference between a dog and a cat for example, or even tell your cat from another cat. But it's not good at reasoning, there's no actual intelligence in the sense that you'd think of artificial intelligence. Kind of drones, not drone but air vehicles that can take off then design their own program, target and attack people are decades away
Lynne	And yet we're constantly told stories that US military drones for example, or surveillance capacity target specific individuals in towns for example, and goes after them. That there is a level of high intelligence
Bob	No but there's not any actually. It's a human looking at a video, it's not the machine
Lynne	But the machines deliver the strike
Bob	Yeah, the machines deliver the strike
Lynne	So we zoom in and out of macro and micro here and the very specific individual, and then the mass of surveillance type experience. And for Nic, the whole notion of identity and who gets spotted doing what where is really life and death

Nicole	Absolutely, that's right. And I guess it brings to mind for me the potential benefit that some technology – we can use aerial drones ton monitor and see what's going on. It does make me think also of the sense of justice one might take after an event. If we look at atrocities like mass killings and mass graves, there's been satellite technology used for example to determine where mass graves are, in the Vulcans back in the 90s. those graves, you can treat them as a crime scene to prosecute the perpetrators, and you can approach them with a humanitarian framework to try to identify individuals so the families know the fate of their relatives. So there's multiple things going on, if we had humanitarian drones at that point, would it mean that people had behaved differently, or would it mean they adapt and find other ways to do things that they were going to do?
Lynne	What's the difference between a humanitarian drone and any other kind? Is it one with a red cross on it? (laughter) They're surveillance devices, yeah?
Nicole	Yeah and I guess what you do with that information and what you put that information into. So can we get food more quickly to people who need it because we can see where people are moving? The same information might be used for a military purpose. So it really depends how you're using it, and the rules around this are really being developed. I think the consequences really still need to be thought through, there's a lot of thinking about this going on, and not a lot of answers yet. A bit of testing going on but this is high risk, you don't want to get this wrong because it's big stakes to make errors on when talking about this kind of thing
Lynne	So the tech is really where we're headed obviously, and we'll draw in some of our other guests in a moment on their particular areas of focus and interest. But it cuts both ways is I suppose exactly the circumstances that you've described, it can be used for good purposes or it can be used for evil intent. And once again as a layperson in suburban Melbourne I have no way of gauging which sources of power and technology are using it for good or evil. So in terms of judgement, I've got no idea, so I'm in the hands of much bigger powers in terms of my comprehension of goodies and baddies. From a journalist point of view, that's the way the world gets carved up, and in justice I think that's also the way we're framed to think, that there are goodies and baddies. I was fascinated with Diane's thesis around if we cant attribute blame and we cant make things better, we just blame the victims. We wind up saying ah well, the Iraqis were on the wrong place at the wrong time, and the Kurds, they didn't help us with Normandy so they get what they get! (laughter) I mean the absurdity around that sort of framing just becomes increasingly apparent to me. Ryan, have you got thoughts about how we deal with tech and which side, I mean obviously it serves all purposes good and bad, but I suppose our challenge to comprehend what sort of impact it's having
Ryan	Big question. I think, I think – one thought is we default into dividing them all into goodies and baddies, but we cant even do that on an organisational level. There's different parts of different organisations using things for different purposes. For some people, police is a classic example. There's always police, hopefully they're on the whole, but there's often rotten apples and that type of thing. For certain people in society, the police are the baddies, they want to not deal with them. So I think part of managing these things is one, we need to be clearer and explain what the

technology is, what it can be used for. Two, I think people generally believe there are safeguards built into government agencies, but they don't know what they are, they don't know how they work. Government agencies tend to just say you can trust us, we adhere to the privacy act

Lynne	And then you get robo death

Ryan	Exactly, exactly, and that's because there's that sense that I think organisations, including government agencies, need to do a better job of saying this is what we can do. This is what we will do. These are the common checks and balances. This is where you can find out more information if you want. Um, and this is why. And some of the checks and balances people think why are they doing this, but there's good reasons for it. Something I keep trying to remind police officers for example of, there's the standard line you get from police and security that journalists get all the time 'we cannot comment on operational matters' 'we cant comment on security matters'. But there's actually general principals behind why you cant do that. Operational matters you don't want to leak information, or there's investigations you cant comment on because if they go public, you then cant prosecute in a court of law. So if the police say 'we cant comment on operational matters because' the one sentence principal 'we cant comment on ongoing investigations so that we don't jeopardise our chances of prosecution in a court of law'. It just helps people to understand how the system works as opposed to 'trust us, we're the police and we'll do the right thing'

Lynne	I mean I think that you're right and the Australian context is fascinatingly different from other law and order environments or military environments where we say as little as possible. I suppose I'm torn, I mean I think they should add that extra sentence and say because… that's entirely reasonable. But then I think, do people really want to know? Is this an issue for the majority of people fretting about whether or not they make the mortgage this week, or about housing. In the competition of needs, it's copping a fairly low priority, yet it has this profound impact on the way we understand our democracy, our rule of law, the sort of general health of society

Ryan	One comment there, I think right now they probably don't want to know, but there will probably be some point in their lives where it really does matter and really is important

Lynne	Like when?

Ryan	Well in the police example, a relative is arrested or they come in contact with the justice system, or they're a victim of some offence. If they, if police explain how it works at that point, they're emotionally invested and it's too late. There needs to be a sense of ongoing communication in a simple way. That's part of the background of people's lives, I think for things to sink in and for them to understand, they need that explanation and why we do things in certain ways, and what safeguards there are. I think also it's important because if our government agencies in this example, but if they cant explain it simply, they may not have it clear in their heads, and I think that's part of it there. If someone had been forced to sit down in those circumstances and explain to someone who might be effected,

what would actually play out in practice? I think there's some red flags going up. But there isn't a culture in Australia of explaining simply, clearly, to that kind of ordinary person. We all get caught up in our professional worlds where there's terms we understand, we know how it works, but for someone outside -

Lynne
So it doesn't matter until it really really matters, and we zoom from the macro to the micro and suddenly we're in the frame and our trust in the system is brought to the fore. I'd really like to draw in Michelle and Marilyn on this and their work on tech in the crime context, because once again it cutes both ways in the terms of the value of technology in this context. It's both a force for good and potentially a force for appalling maltreatment

Female
I think that, and this is really interesting for me because I teach overwhelming to straight criminal law and criminal procedure. So this is very much a reframing of issues that arise there. There are a couple of things that occur to me. The first is that new technologies we're talking about are simply mechanisms of crimes to be committed in new ways. And that's not particularly challenging, it's just a tool. I guess where I see real significance is in the development of new crimes that can only, or are predominately committed by cyber means. And the impact that has on criminal law generally, which I think is really to raise the profile of psychological harm. The big thing about crimes which are perpetrated by the internet for example is that they don't involve physical presence, which has always been the paradigm for assault, things of that nature. So we've got a range of offences which are now emerging liabilities for things that wouldn't have existed, say 15 years ago. There's an interesting case this week in the United States of a young woman who encouraged her boyfriend to kill himself. She was present when he did it, but Michelle Carter, a case that goes back a couple of years, wasn't. she was convicted of manslaughter. Now it would be very very hard to get a conviction like that, maybe going back 20 years ago, where someone might have done it by telephone. I think the immediacy of the internet underpins this sort of analysis liability, but it's a really interesting reframing about how we approach criminal liability, when we've got the conduct occurring not immediately in the presence of the victim, but being transmitted by some other means. So I think that's a really interesting implication

Lynne
Yes, and that goes to Robert's comments earlier too. Bianca, your work around sexting I think is in direct value here, or has direct value here. Can you tell us a little about that?

Bianca
Yeah I was actually thinking, so which category does this fall into, is it a new crime or is it actually an old crime? Because I used consider it a new crime, really, but I was talking to a colleague and he said, we used to track photos years ago, so is it really new? But to me the big issue, the things that Ryan was mentioning earlier, I was really curious, he said when we sign up for something we implicitly agree that our information can be used. To me, the main issue – you know, all the work we've done around sexting is the issue of consent. When you send a nude photo of yourself to someone else, are you consenting or are you not consenting? Legally, the law has done terribly with this! And really doesn't have an answer. Picking up on another topic, the sort of international laws versus national laws, even in Australia we don't agree whether it's a crime or not. So you know –

Lynne	State to state?
Bianca	Yeah. So in Victoria we now have sexting laws, where the distribution of nudes and even the threat to distribute is a criminal offense, but some states don't have it, so it's fascinating how even within the Australian context we don't agree on how to deal with it legally or morally you know – fascinating
Lynne	You wanted to add here Ryan?
Ryan	Yeah I think sexting is an interesting example of what I was talking about before in terms of the Gmail example. You share it and you implicitly agree to share it for a certain purpose. As soon as someone takes it and uses it for a different purpose, then it's a significant injustice. There's blurred lines and misinterpretations of what you agreed to in the first place, but I think you know, I think I guess my feeling there's strong reactions is, you share it with a particular person for a personal purpose, and someone does someone different. Sorry to hog the microphone, also I think the other aspect of the online cyber area for police is it makes it – parts of it makes their job easier, but parts of it makes their job hugely harder, particularly where – if you want to raid anyone's house to get the evidence. Now you've probably got a few different devices with terabytes of data, you're probably wanting to get data from internationally so other jurisdictions, so it slows down a lot of ordinary prosecutions. But because it all happened online, people think everything online happens fast so why cant you act quickly?
Lynne	So expectations get raised. I mean relationships are essentially messy, now we've created this extra dimension or at least expanded the range of it through online means, and enter into a legal framework as well, so it's layer upon layer. Jennifer, you've done some work around facial recognition which is also a fascinating subject because it has those dual dimensions, both around safety but also around personal persecution
Jennifer	Right. So I'm particularly an eye witness researcher. So I'm interested in how people react when they see a crime, and then what the police can do to get better information from those witnesses and then how that evidence should be used in court. And facial recognition has a really interesting component to this that we still don't really understand. So there's a possibility that facial recognition will eliminate the need for eyewitnesses completely, but simultaneously we have to trust in that evidence. So it's machine learning ultimately, but currently how it's being used is paired with other individuals. So the machine makes some decisions for them and then the human makes the ultimate decision as to whether the person is or is not that individual. And that's how it's being used with passport people for example, but there are questions around how that will move forward in the future, and ultimately, who do we go to to get information about the accuracy rates of this technology? Because currently it's being developed by companies, and so we have that commercialisation effect we were talking about where you have to trust in the company's decisions or the company statements about the accuracy of the technology, but their profit margin depends on their claims about accuracy. And so it presents this interesting tension that I'm not sure how we're going to solve

Lynne	Now tell me if this is absolutely fiction, but I heard this extraordinary snippet of information, that China had decided it was happy to bankroll CCTV coverage of I think it was Bulawayo or a large African city, because it wanted to improve it's capacity in terms of facial recognition of black faces. It had recognised that was a deficiency in the system, and that was the way to overcome that, was to factor – increase the volume of black faces
Jennifer	I don't actually know, I haven't heard about that
Lynne	You haven't heard about that? So I still don't know if it's true or not! But I suppose, and this is how we tend to think about these things, it tends to chime with our attitudes to a sort of global creeping presence by one state actor or another, it also chimes with this notion that surveillance is used for nefarious purposes. So it reinforces our bias, whether or not that's the case it struck me as plausible at least. Robert, that whole notion of the algorithm as being something in which we have been geared to trust, that the information that comes out of that database that Ryan referred to, the facial recognition tech that Jennifer was describing – how trusting should we be of that sort of machine learning? You said earlier that it was actually in it's fairly early stages of development
Bob	Well machine learning is actually fairly advanced, I was talking about the wider AI, and so yeah the question is not – it's probably not as much about the algorithm. I think we talk about algorithmic transparency and things like that, but I think no matter what we're not going to be able to really explain the algorithm to every soldier that needs to use it. I think it's more about making the systems work better by making the data better. The example of racial bias is a good one, and I mean I gave a talk in Canberra last month and I was talking about AI. I gave an example, I was talking about biases and I used an example on my phone, you can go into Google photos and type in any word and search. I typed in cat and there were 82 photos. Most of them were my cat, but there was also my parent's cat, there was a statue of a cat, and there was a picture of the front cover of the novel [43:43 inaudible] that has a black cat on the front. So they were all cats. So I thought, let's try something else, because I went hiking in Yosemite in the summer and I saw a bear. So I typed in bear, because I have a photo of a bear on my phone, and the bear didn't come up at all. There was a statue of a panda from Melbourne airport that came up but also a rock wallaby and various other creatures from the zoo that weren't bears. But that's because the internet is mostly made up of pictures of cats (laughter). So it's exactly the same kind of thing you see with racial biases, we need to make sure that the data is processed in a way that those biases are not there
Lynne	So how does that happen, is that more data?
Bob	No it's not necessarily more data, I think you have to kind of pre-process the data to level it out somehow, I'm not an expert in that area. I know there is work in the area though
Lynne	I can imagine. What this is all leading to is where judgement happens, and for example in the Netherlands, where they decided they would move their entire family law legal system online. That failed. They pulled the pin on that after a number of years of effort and one analysis I've read about that, which puts it in

extremely simplistic terms – the closer you get to judgement, the more human involvement you need in order to have trust. So that brings us right back to this whole notion of whether there is a social contract without a notion of trust. So can you see a time when for example, in the military context, human engagement, human judgement around whether or not to pull the trigger is eliminated completely?

Bob   Probably not. I think there will always have to be some level of meaningful human control. On the other hand I don't see increased use of AI and autonomy as a bad thing. On the one hand it could be seen – if you could introduce ethical norms and rules of behaviour into the system and have it be able to interpret things, then computers are better at recognising some things than humans, especially in cluttered scenes

Lynne   And probably more consistent

Bob   And more consistent. For example if you have a sensor with some AI built into it, it could recognise there was a red cross in the scene, that a human operator might miss. But also machines probably wouldn't wilfully commit war crimes, and humans do it all the time

Lynne   Yeah, I mean that was certainly in my mind as you were speaking as well, that it's all fine and well to assign good decision making to humans at that point in the process, but often we see bad actions, and we have a few of those in prominent positions of power at the moment around the world, that we probably wouldn't ascribe huge amounts of trust to

Bob   I'm not sure who you mean (laughter)

Lynne   But Ryan that notion of getting to judgement, is that something that's very considered, for example in the policing world, that it's important that there is a human dimension in there?

Ryan   Yes definitely. Interesting example doing some work with the AFP, they invited an international criminal futurist to talk by Skype, he wrote a book called future crime by a future cop. And he was going on about all these wonderful sensors and technology and autonomous and it will be great, because the police will then – there's an autonomous car, the police can have the autonomous car drive the criminals in and they can lock them ion the car and drive them to the police station. One of the police officers in the room then asked this guy, 'what does that mean for the trust between police and society? Because that human element of how can you trust.' Sadly this guy went, that's a really interesting question and I've never thought about it (laughter). But I think police experience it day to day in the front line, going and talking to someone who's house has been broken in, how they talk to people in the streets makes a massive difference to how people respond and how they trust them. That personal interaction makes a massive difference to how they trust and how people relate to them. So I think they've got that frontline experience, so that they understand what needs to happen. I think the other aspect I that machine's programs are in black and white with how they make decisions.

	Human's, we at least feel like we need to have some nuances, someone can at least express they understand nuances, machines aren't very good at that
Lynne	Black box, it doesn't necessarily deliver justice for all the human emotions we heard about earlier. So Nic, when it comes to the personal experience of you pass, you fail, in terms of your immigration status, your future, where is tech in that?
Nicole	Yeah I have heard some disturbing planning around some of the things being automated in terms of visa processing. Some of it might be fine to get through a lot that are pretty straightforward, but when it comes to things, cases that require a bit more judgement, there's a lot more to be looked at before we can be comfortable with that. I think the other thing that it makes me think about in terms of the judgement that's required is in our searching for missing people, we really need the human element when it comes to determining if we have a match for someone. We can look at large sets of data and algorithms can help us know we've narrowed the field, but we still really need people involved to check on naming conventions, spelling variations, identification from the family member that yes, that is my missing daughter, not somebody else who looks very much like her. Facial recognition technology is always something we're exploring, but again has some dilemmas about it in terms of the data sets that are available. I think all of that still requires human assessment, analysis and engagement with the person that's concerned in this. So I cant imagine that part changing, no matter how much we increase our reach or speed up processes. I think human assessment is always going to be a part of the way we work. Certainly a lot of things we do relies on a person being willing to trust a person to deal them really difficult, distressing information. That's not something you can just upload on a computer and it's done. So I think it will continue, but hopefully we can get smarter and faster in helping people by using technology, but balance that with the human touch, which cant be replaced.
Lynne	I think that smarter and faster is critical, because if you think of the capacity of tech to really scoop huge numbers of people into it's floor, then having to process that, unless that has a dimension of automation around it as well, we're asking for a world of trouble. Let's open it up, who would like to make a comment or a question? Any takers? Laurie, fancy that!
Laurie	Fascinating discussion. I'm interested to know, in terms of the growing number of platforms we all sign onto online, what's the research looking like in terms of the way informed consent operates? Because we heard about sexting and other things where people are suddenly imbedded in these types of systems, they probably don't have the right to be forgotten, but what kind of thinking is there about trust in these platforms and the 500 pages of stuff you'd trawl through if you actually read the terms and conditions? Are any companies making, taking initiatives to try and make that whole process more straightforward and transparent?
Nicole	I can say certainly within the Red Cross we're trying to do that, to make sure we explain to people in plain language what we're doing with their information and what they can expect, what they can do to take it off any of our databases if they want that. But it is very difficult to know once we're using it and passing it on to a third party that we might be needing to engage with to ensure they can also do

	that. I think that's where some of the rub is, to make sure we can be accountable for what else happens to it
Ryan	I think all the major tech companies grapple with this, and they've got fundamental tension between their business model and maintaining the trust so that customers keep giving them the data that drives their business model. Some of them, ones like Microsoft are actually starting to come out with manifestos about how they treat people. Interestingly Microsoft are trying to position themselves as [53:36 inaudible] I think the real interesting stuff is happening at the dynamic end where people are trying to use a logical approach, rather than you giving your data to someone else, you own your data in different technological solutions, so you have control over the data and you can choose to share it with someone for a certain period of time, which you can turn off and on. I think – lots of different people are experimenting with that. How far that will go and whether it will gain widespread acceptance, people are trying to grapple with
Lynne	Bob, is there collection of data about people in the military context? It sounds like a totally naïve question. But if there is, there is no consent given, is there?
Bob	Ah no, I think the consent is given when you sign up, to do whatever
Lynne	To be a citizen?
Bob	To be a citizen. No but there's not nearly as much data as you would think I think, there's kind of annual fitness reports and things like that, but it's not like we have people implanted and continuously monitored or anything. But that is something, people talk about that in the future, to be able to do that and monitor people's health, their mental and physical workload when they're on the battlefield. So there's lots of ethical issues around that kind of thing
Nicole	We do it with footballers
Bob	Definitely, and that's one of the things people look to in the sporting world
Lynne	Yes, fascinating. Any other questions or comments people would like to make? Bianca?
Bianca	I just wanted to mention for example, if a young person makes a complaint to the commissioner about cyber bullying, the commissioner actually requires that the complaint needs to be made to the platform first. So the platforms in essence – you cant even make the complaint without saying you have notified the platform first
Lynne	So that's very much in the consumer context. You make your complaint to your supplier of your lemon car before you take it to consumer affairs Victoria for example. Rather than being a social construct
Bianca	Exactly, so it's really interesting. I think on the other hand, it's really interesting with regards to the trust and the platform. Like you don't have any other way around. If you have a complaint, you need to approach, you cant go around it. You cant file a complaint to the safety commissioner without having done that, so the platform comes first! And um, I think the other thing is – Facebook specifically,

they're very keen on increasing their level of trust so they run events. I was recently invited to be a speaker about how to keep young children safe online. So they're trying to enhance their image in terms of what are they doing, but then you have people going, well it took you three days to take this stuff off, it was up for three days. So I think its really difficult

Lynne   So was that event face to face? It's actually in a room?

Bianca   Yes, it was in Geelong, so I went to the Geelong arts centre yes, with various other groups as well. It was a face to face event sponsored by Facebook

Lynne   I just find it intriguing that the tech outfits are very conscious that they need personal face to face interactions in order to build trust

Bianca   Absolutely. Unfortunately and this was actually interesting, I asked can it be live streamed and they said no (laughter)

Bob   The morning tea is not as good!

Lynne   That's a good point. Speaking of which, we should probably halt because I'm sure there are refreshments to be had and another panel to prepare for. Before we do that, can I ask you to thank our panellists very much? (applause)

Recording   We thank you for listening. This was a recording of the symposium 4.0 2019, organised by the social innovation research group, Swinburne university. For more information, search Swinburne social innovation

[END OF TRANSCRIPT]