Penn State Journal of Law & International Affairs

Volume 7
Issue 3 *Symposium Issue*

April 2020

Autonomous Systems & Domestic Security

David Atkinson

Douglas Burig

Marc Canellas

Alan Wagner

ISSN: 2168-7951

Penn State
Journal of Law & International Affairs

2020 SYMPOSIUM ISSUE

AUTONOMOUS SYSTEMS & DOMESTIC SECURITY

Moderator: Anne Toomey McKenna
Panelists: David Atkinson, Douglas Burig, Marc Canellas, and Alan Wagner

Anne Toomey McKenna: We have had some general conversations today. In this panel, besides trying to make sure that we wake you up since you just ate lunch, we are going to really try to give some more specific examples. One of the things that I want you to understand is how exciting it is to have these experts here. They bring a different focus than some of what we have been hearing from today. We have a wide array of people today, but we are going to be focusing on autonomous systems in domestic society and autonomous systems from a domestic security perspective.

I am very excited to welcome here today, to Penn State, the panelists we have. First, sitting next to me, or right beside me, is Dr. David Atkinson. He is the head of systems and technology, and he is the chief research scientist for artificial intelligence (AI) at Continental Silicon Valley Research and Development Center. He oversees systems and technology projects for future transportation and mobility systems with a focus on intelligent

driver assistance, autonomous vehicles and smart cities. He has worked at the Florida Institute for Human and Machine Cognition, leading research projects and trustworthiness on autonomous robotic systems. He has previously worked for twenty years with NASA's Jet Propulsion Laboratory at Cal-Tech, and he was a founder of NASA's artificial intelligence program. Dr. Atkinson has made significant contributions; and he continues to, in the world of autonomous vehicles, be a pioneering thought leader. He has dual degrees from Yale University: a Master of Science degree and a Master of Philosophy degree. The focus of his degrees are computer science and artificial intelligence. So, we are very happy to have him here.

Anne Toomey McKenna: Sitting next to him is Professor Alan Wagner, Penn State's own. He is from our Department of Aerospace Engineering, and he is a Research Associate with our Rock Ethics Institute. He received his PhD from the Georgia Institute of Technology. Dr. Wagner researches and develops techniques that allow robots to interact with people in a variety of different social contexts. If you ever look at the Penn State News Day Today feed, he is in there, I feel like every week, for the fascinating work he is doing. That, or that he is a really good communications director. He is investigating deception, human robot trust and the conditions which encourage people or discourage people from trusting robots. He is also—this is I think, particularly fascinating considering—researching robots that can evaluate whether or not they should trust people.

Anne Toomey McKenna: Dr. Wagner's research has won numerous awards. His research on deception has had significant notoriety in the media. Not just Penn State, but the Wall Street Journal, New Scientist magazine, Journal of Science, and his work was described by Time Magazine as the thirteenth most important invention. Again, he holds numerous accolades and awards to his credit, and he holds a Master's degree in Computer Science from Boston University and an undergraduate degree in psychology from Northwestern University in addition to his PhD. Then, I'm going to jump over you for a second there.

Marc Canellas: I'm just the odd one out.

Anne Toomey McKenna: And so, we'll come back to that in a minute. Next, we have Major Douglas (Doug) Burig, who is a Major here with our Pennsylvania State Police. There are really very few Majors if you're unfamiliar with the ranking of that system. There are over six thousand officers employed with the Pennsylvania State Police, and only eleven of those are Majors. He is the overall director for the Pennsylvania State Police's Bureau of Criminal Investigation, and that falls under the umbrella of the Bureau of Criminal Investigation. His background: he has served for over two decades as an officer, including the Commander of the Analytical Intelligence section, as he brings up while talking with him at lunch. He worked his way up through the ranks. His experience in analytics and use of predictive abilities really bring us a lot of information here today. He has a BA in Political Science, and he holds a

Masters in Science degree in Administration of Justice and Homeland Security.

Anne Toomey McKenna: Then sitting in between, we have a 1L. We have Dr. Marc Canellas. While he is a JD student at NYU School of Law, he is also NYU's Jacobsen Leadership Program in Law and Business Scholar and Cybersecurity Service Scholar. His current legal tech research focuses on technological civil rights movements, the use of predictive policing, and biometrics including face recognition.

Again, Dr. Canellas, though while he may be a law student now, his CV is remarkable. He has a PhD in Aerospace and Cognitive Engineering from the Georgia Institute of Technology, where he studied human decision making and human machine interaction. His postdoctoral research at the Cognitive Engineering Center at the Georgia Institute of Technology's School of Aerospace Engineering involved mathematical computation and human subject studies towards developing decision support tools for military command. He's a voting member of the IEEE-USA Artificial Intelligence and Autonomous Systems Policy Committee. He has served as an IEEE Congressional Science and Technology Fellow in the United States House of Representatives where he was responsible for legislation, appropriations and media for aerospace, cyber security, privacy and surveillance science, technology, AI, robotics. His research has already been published in numerous journals, in media outlets, national security outlets, and he has won awards from the National Science Foundation and the Max Planck Institute for

Human Development in Berlin. He earned his BS in Mechanical Engineering from the University of Missouri, and his Masters of Science and PhD in Aerospace Engineering from Georgia Institute of Technology.

Anne Toomey McKenna: I already said today we are going to be talking about domestic systems, and what a range of people to have bring this to us. And we are going to get really specific about it. But I want to set the stage because we have had some theoretical discussions and we really want to break this down today in very concrete, real examples of how technology, law, autonomous systems, and what is really happening and what we think of this. We have challenges in this question about, what, really, from the domestic standpoint, is not a theoretical or a philosophical standpoint, but a domestic standpoint: what is the law? And we are talking about this. And so, there' are several problems that focus on this. One is definition-based, one is knowledge-based, and then there is reality-based.

We keep hearing these terms, "autonomous systems" today, and we have heard some very extreme examples from autonomous systems and weapons. We have heard just the potential. A lot of debate that has been very provocative and thought provoking. But when we say "autonomous systems" from a legal standpoint, what does that mean? Your phone is loaded with autonomous systems. Are we talking about Skynet? Are we talking about Alexa? What are we talking about when we talk about autonomous systems? Part of our problem and the challenges in this is

knowledge-based: do consumers, policymakers and lawyers even understand AI? Do they understand autonomous systems? And then, this other part is reality-based. Again, we keep hearing theoretical conversations. But AI and autonomous systems are pervasive now. They are what you do on a daily basis. We did hear some great examples about—I think it was General Dunlap—"I go the way it tells me to go." That is autonomous systems controlling your present-day behavior, designing and controlling how you interact with the world.

Anne Toomey McKenna: We continue to see, though, just the concept of autonomous systems and domestic society are not regulated in the way that the concepts of military use of autonomous systems may or may not be regulated. But that is where we tend to see the technological advances that are changing and shaping all of our lives.

When we look at this, we are going to talk about systems, both the design and the data that is collected. But then, how this data is actually aggregated? How it is used? How it is used by police? How it is used by researchers? And so, we're going to be trying to keep this concept of "private sector" in action and impact on these broader questions of civil liberty. Part of the problem when we talk about law and autonomous systems is: what laws regulate autonomous systems? What regulates AI? We have this crazy patchwork of laws and a sectoral approach in the US that makes it very challenging to explain this to someone not steeped in the technology or law in this area. And so I have highlighted the regulatory agencies in these giant bubbles. We are pulling

from multiple sources of law that may or may not influence, or control, or regulate autonomous systems. But I want to focus to give you an example on that regulatory agencies for a minute.

Anne Toomey McKenna: Autonomous systems in the US, again, are sector-based and state-based. When we talk about autonomous cars, like self-driving vehicles, well, we are talking about the National Highway Traffic Safety Administration that is producing regulation and mandates – legislative mandates that embed AI technology in every vehicle in the United States by federal law – and the goal is to get to the point of communication to vehicle to vehicle communication. If we want to talk about UAVs, which somebody will touch on today, it is the Federal Aviation Administration. If you want to talk about websites and online activity and algorithms that are controlling what you see or do not see on websites, that is the FTC, the Federal Trade Commission.

Just as a quick overview, we also have our federal laws and our state laws: part of the problem in this. Then before I turn it over to these, my esteemed colleagues here, this is really timely. Yesterday on the NPR driving up here, Ralph Nader is on this. So, in the most recent Boeing crash, Ralph Nader's grandniece was killed. It was a twenty-four-year-old woman, and Ralph Nader is a consumer advocate. This quote, though, I think really frames almost everything we've heard today in these panels, and what we heard last night from Paul. So, this is a harbinger talking about this crash, medical technology, autonomous

weapons, self-driving cars. "It's the arrogance of the algorithms, not augmenting human intelligence, but overriding it and replacing it." The significance of this Boeing disaster is that it can teach us some very important lessons about maintaining human intelligence, and not seeding it autonomous to systems that have no moral base and intuition.

Anne Toomey McKenna: With that, I am going to turn this over to David Atkinson. Again, he is one of the country's leading . . .

David Atkinson: Oh, stop.

Anne Toomey McKenna: Okay, sorry. He is really cool. But I just want to set the stage for us with an overview of AI supported autonomous systems, how they function in domestic society and their increasing use. I actually hope you can also just loop in that 5G point as that is changing.

David Atkinson: I will. Yes. Thank you very much.

Yeah, okay. Thank you very much, and sometimes it is hard to continue on a Friday afternoon after lunch, and I appreciate you being here. I realized part of my challenge is to stimulate you for the remaining part of the symposium, and we will see how many heads go down and give me some real-time feedback.

I published my first paper on autonomous robotics in 1984. In retrospect, it is a terrible paper. But it tells you that I have been thinking about this for a very long time, and my career has been devoted in various positions to autonomous systems in one form or another.

A very long time with NASA JPL and deep space exploration, working for the Air Force, doing my own research, and lots of other work for NASA, and now was time to go do something that would take all that interesting work that I was aware of, and that I could do, and infuse it into the Society for some social benefit.

David Atkinson: There were lots of different ways of doing that, and I chose automotive. Because if you look in the parking lot, every one of those cars has parts. My company, Continental, makes most of those parts. I think the only thing we don't make is a steering wheel, but you don't need that for that for an autonomous vehicle anyway. I'm going to keep this really reality-based.

I am prone to going off in technology speculation sometimes, and forward casting, vision casting. But my job here is to tell you what is. What is the current state of things? And I am going to talk to you about it from the point of view of commercial products. Not from what's running in the laboratory, but what is real today.

One exciting part of the job that I do is I get to go visit the companies that buy stuff from us: all the OEMs, FORD, GM. I am not going to name them all, but those companies that use the parts and so I can see what they are doing in the state of autonomous vehicles. I go visit startups, of which there are many in Silicon Valley, and see what they're doing. And so, I have accumulated this pretty nice overview, I think, that gives me a chance to share this information now with you.

David Atkinson: First thing to realize, you interact with intelligent systems every day, if you use a credit card, if you use a travel agent, if you—well, lots of things. Just trust me on this. They've been deployed since 1990s. Now, the important thing to remember is that there are lots of different aspects to artificial intelligence. And so, at different times in the history of AI, certain tools and techniques have become prominent, and other times faded. Parts of AI have—people will no longer even think of AI.

Object-oriented programming, which is a conventional part of programming languages, was originally invented by a researcher named Hewitt to support his work on agents and actors: the Actor Model. And other computer scientists said, "Oh, that is really interesting. I'm going to program my stuff in it. Doesn't have anything to do with AI." AI people want to know what intelligence is, so that was a programming language. We peel the onion off, threw that layer away, and we go to the next level. So AI, in a lot of ways, is advanced computer science. It's also mostly about algorithms, and not entirely.

Here's another thing to realize. Sometimes people equate Deep Learning and Connectionist learning – network-type learning – with AI. That is it, it was a relatively new development. Those are a relatively small part of the toolbox of artificial intelligence. It is working really well, surprisingly well, from my point of view. But it is not as mature as other areas. So, there is a large toolbox to draw on. I would refer to these Deep Learning techniques as "Connectionist" or data-driven.

David Atkinson: Then there is the alternative approach or complementary approach, which is semantic, conceptually-driven techniques that used to drive the portion of AI that was referred to as "expert systems" (an unfortunate name). I really want to be careful about not giving false expectations by giving things names like "deep" and "learning" and "expert." It is not that. It is computers.

So, intelligent systems may or may not be autonomous. They gain the ability to choose with autonomy, as I will show you in a minute. When they do, they can augment, multiply or replace human efforts. So we have in there the human augmentation model. We have the human multiplication, labor multiplication, and then replacement. Replacement, or substitution, is not the right way to think about it, and I will tell you more about that in a moment.

In conventional software, the programmer makes a decision on the sequence of how the program works. Maybe with some branching stuff, but it's well-defined in advance. One of the key features of AI software and particularly autonomy, is that you push that decision of what to do out to run-time because that's where you have a lot of uncertainty, and you do not know what the right sequence of things to do is. So, you make that choice from a limited number of predefined options. That is fine. It is still deterministic, but you do not decide until you actually have to.

David Atkinson: Autonomous machines perceive, interpret, decide, plan, and they act without the need for direct control. "Autonomy" is a word with a lot

of baggage these days, and we have already heard lots of definitions. So, I get to give you mine. It reflects the machines' relative independence and control authority, which means it has been delegated the ability to do something, to perceive some goal, to pursue some goal within some constraints subject to certain levels of monitoring. But it is always contextual, and it is always with respect to whoever owned that control authority before.

David Atkinson: I was asked the question, "Will this all be disruptive?" Oh, yeah. Oh, yeah. Was this super computer in my pocket disruptive? I can get to any knowledge in the world anytime. Yeah, it has changed the world in a lot of positive ways. So when we are talking about autonomous systems, now they can act in more sophisticated, increasingly intelligent ways. In fact, now have wheels and can go places, or have arms and robots. Okay, yeah, we are going to see massive disruption. Important to note, this is why substitution is not the right way to think about this either.

In almost all cases of the introduction of automation into an existing system, there are ripple effects. In any organization, there is workflow, there are communications, there are levels of responsibility. This gets touched by the introduction of automation. The introduction of autonomous systems with decision-making capability adds another level of disruption to it. So you have to consider autonomy in this larger systems context, and that is part of what causes the disruption.

David Atkinson: How am I doing? Fine? Okay. So what is the real story about autonomous vehicles. I am

telling you the truth, first-hand knowledge of emerging mobility companies, my experience. I really worked hard to make this true. So, there you go. Trust my authority.

David Atkinson: So the component capabilities for autonomy such as perception are maturing, and very rapidly, and they are driving incremental deployment of the elements of autonomous systems, such as driver assistance. And you could buy these today. In new cars, you can spend the money, and you can get lane-keeping, and you can get highway cruise control.

Around this subject of autonomous mobility, we see that the evolution of an ecosystem of companies now. There are lots of different stakeholders who can find value in this for different ways, but they have shared vision. And now these companies are partnering up. We see a multiplication of components suppliers, the services that are needed for, what five years ago, would have been a very absurd part of artificial intelligence, now with thousands of people working. And what is really important is that there is enabling infrastructure being put in place, a high-speed communication, 5G networks.

5G is fast enough, so now you can just start distributing computation from one computer to another effectively. And cloud computing is there, which means there is the potential for a lot of sharing in the information. Today, there are probably—I don't know the exact number, but oh, well—over one thousand autonomous vehicles on the street in the US, in Europe, and also in Asia.

David Atkinson: When you see pictures of these on the news, they show you the ones that really look weird, with the swirling LIDAR is on the top and the racks that go, "Oh, nobody would ever buy that car." It's like this is a test. Most autonomous vehicles look like ordinary cars. The ones I work with, and then Continental's Chrysler 300s, they are black. We have lots of them. I mean, so they might stick out that way. But otherwise, from the outside, they look like ordinary cars. And that's what you will buy when they are available.

Here are some examples and my forecasts, and in a couple of years, you can call me up and say, "You were smart." Or, "Boy, were you dumb." Driver Assistance, as I mentioned, you can buy that now. App-based are now rolling out, like Uber and Waymo, and they are moving very fast. They are in one or two cities now. But I know from being in the inside that they have very aggressive growth plans. In another year, you are going to go, "whoa."

Self-parking–this is the part I love. How much time do you spend parking? A lot. Looking for a parking space. How would you like to roll up to your destination, get out of the car, and say "go park yourself?" And the car goes off, and finds a parking spot and parks. Then when you are done, you come out, and you go, "Pick me up." And it comes, and it picks you up.

David Atkinson: And then it works. I am not saying it is perfect. I am not saying it is perfect yet. Parallel parking is hard for everybody, even for these cars. But it does work, and companies are buying this now. It is going to show up as an option in one or two years in cars you can buy.

David Atkinson: Trailer hitching. I do not know how many people pull a trailer. But trailer hitching is difficult, and parking a trailer is really difficult. Technology exists. It is in advanced development.

Long-haul trucking. These are those big trucks on the highways that go far, across the western states, straight shot. These autonomous trucks are very advanced right now. I have seen them perform in what I think were very difficult circumstances. They are hauling freight. They are in pilot use by companies right now. And we will see in the next two years growth in that to hundreds and then thousands of trucks. Right now, they have safety drivers, but there is no need. I have seen a bunch of demos with them. I have followed in chase cars. The safety driver never touches anything. Not from parking lot to parking lot. These are big, huge trucks and they work great.

David Atkinson: Now, that is a limited domain, and you can make a lot of assumptions. And the company that provides this has made a lot of assumptions, but it works. Here's something I want you to think about. This is getting into smart city now and tying into the infrastructure question, intelligent intersections and traffic control. So, this is a converging interest topic. The cities want to reduce congestion, they want to improve throughput, they want to get workers from outside in and inside out very quickly. And we have a technology now. We have a pilot installation in Walnut Creek of cameras and radars that get a complete 360-degree view of all the cars, pedestrians, and builds a model of the world. It watches where an incoming car may be coming and cannot see

a pedestrian, because there is a visibility problem. It sends a message to the car saying "There is a pedestrian you can't see." This uses the European DSRC communications, which we don't have in the US yet but it is the kind of technology that is coming. In fact, we have demonstrated the ability to automatically brake the car so it doesn't hit the pedestrian. This is important.

David Atkinson: Intersections for pedestrians are the most dangerous place to be. That is where a huge number of accidents occur. If we have just solved that part, then we have made a huge dent in the safety problem.

Anne Toomey McKenna: And I have to make a dent.

David Atkinson: Yes, I am going fast now. Okay, what about my car? Because it is such a complex environment, and you want to use it. And if you are saying, "I have taken a craftsman wrench and tried to pound a nail with it." That is not what the wrench was intended to do, but it works. People do this routinely. They use technology in ways that are not intended, but this is dangerous. So if you use this outside of the domain in which it was designed for, it is going to cause a problem.

David Atkinson: Now let's put this all together on the last slide. As AI increases in capability and controls more and more systems, and interacts, it will become an increasingly attractive target for bad actors. Unfortunately, autonomous systems based on artificial intelligence are vulnerable to unique new attacks. Not to cyber-attacks as we know them today, but new ones on various aspects

of the system. And it is quite a difficult, real situation. There are dozens of attacks demonstrated in the laboratory right now. Luckily, because it's not a big target, there are not too many out there on the road, actors have not spent time doing this. And there are no sufficient defenses today.

David Atkinson: One day someone will publish a new attack. Another day, the following week, there is a defense. It is an arms race. This is not my area, but it really makes me wonder how many companies, including automotive, are going to address these unique new challenges.

So what is the impact? Well, I mean, degradation of performance, failure, privacy breach. What if they hack and get a view of the camera inside your car? Yes, there are cameras inside your car for lots of reasons that we could talk about. Worst case: they subvert control. Now they are driving. This has been demonstrated already. Without the AI, we can already subvert vehicles. You could use it as a computing platform. You can use it as a stepping stone for other attacks just because it's connected to other cars and to the infrastructure. And worst case: mischief or physical attack.

David Atkinson: Last week, we saw Baltimore traffic grind to a halt because a gasoline tanker overturned at a critical intersection. That was, of course, human involved and not automation involved. But let's say it wasn't. Now, it took them twelve hours to fix that up. And a bad actor might now go to another intersection and crash another one, and then another one. Or you can imagine a truck driving up on a sidewalk in a

crowded city. There's lots of ways that this could go bad, and that is what needs attention. Thank you very much.

Anne Toomey McKenna: Thank you. Then we're going to hear now from Professor Wagner with some really fascinating stuff.

Alan Wagner: Thank you! Yeah. I think I will be much more brief. My name is Alan Wagner. I do technology of science engineering, and really trying to build these systems focusing on real world ecology, valid types of experimental systems and robots. And so, one example of one area that I'm very interested in is developing robots, and it is a robot here that we named Emergie.

It's an emergency evacuation robot. Maybe it might looks like something that you would want to pull the arms on like a slot machine. But, nevertheless, I am trying to have these things show up at your door. Even if you've never interacted with a robot before. It is seeing whether or not different types of people will follow these types of robots in high stress, high impact, high physical risk environments. We believe that there is a lot of value to doing this; ideally to reduce response time and have something that could work in schools, hospitals, any type of environment to get people out as quickly as possible.

Alan Wagner: We ran experiments doing this. They have talked about them all over, and we want to see whether or not people would follow these types of things. We found that basically, everybody will follow them. All the people we

tested, no matter even if we told them the robot was broken, they would follow it. And so, this sort of shows the automation bias, and the fact that people have a tendency to default to believing that the technology is right even when it's behaving in ways that you know it probably shouldn't.

Alan Wagner: In related conversations with the military, I have spoken with fighter pilots. When we talked to them about the possibility of using drones in warfare, and one of their concerns was, "What if this thing malfunctions? Will I have to put myself at risk to try to save it?" And these are sort of the things that come up in real world environments as well.

We are also doing some other work, but the goal of this project is develop robots that could interact and learn how to play a game from a child, and play the game the way the child wants them to and wants to teach the robot. Part of the advantage, again, is that the robot could actually adapt its behavior to the variations and local variations of the way the child wants to play. But it also provides a fertile ground for really human robot interaction questions such as having common ground, which is sort of a shared interactive experience, and involving methods for having the robot ask relevant questions that a child would understand. And then, using those answers to sort of build a structure of the game.

Alan Wagner: We are also looking at some ways for machine ethics frameworks, how can autonomous systems decide what is right and what is wrong using different frameworks such as utilitarianism, Kantianism, and having the

machine try to determine what the trade-off is when you have two frameworks trying to do different things. Autonomous driving, for example, which Dave was talking about.

Alan Wagner: For example, I moved here from Atlanta a couple years ago. And in Atlanta (downtown Atlanta), the speed limit is 55 miles an hour, but everyone drives at about 70 to 75 miles an hour. So it is an autonomous system. It has to sort of answer this question: should I follow the rules and drive the speed limit? Or should I do what might be safer for everyone and drive as fast as everyone else? This is a very challenging system, or a very challenging question for an autonomous system to answer, or the people that write the code for it.

If you are Google, or whatever company, you do not want to program in a code that says, "Break the speed limits," even if that may be what is safer in the long run. So, we are looking at architectures that may allow these types of systems to kind of consider a broader contextual framework.

Alan Wagner: Finally, an even more strange and extreme kind of project, we are looking at what happens when an autonomous system tries to enforce norms. What happens when an autonomous system actually punishes people, and physically punishes? We are looking at this. But we have an exoskeleton that we have built, and this exoskeleton is specifically built to a lock to prevent someone from doing something. Part of our hypothesis is that, people actually prefer to be punished by an autonomous machine than they would have human because these autonomous machines do not judge. They

don't emotionally make you feel bad. They just meter out the punishment. So this is one thing that we are looking at, and I think I will end with that.

Anne Toomey McKenna: How did legal counsel feel about exoskeletons that punish?

Alan Wagner: We have our own internal review. They are fully aware there . . .

Anne Toomey McKenna: Did internal review approve this? I just want to check the law.

Alan Wagner: Nobody will get hurt.

Anne Toomey McKenna: Thank you. Thank you.

Alan Wagner: My department head is here. I can see if she is frightened right now.

[From Audience]: I'm terrified.

Anne Toomey McKenna: Okay, her palms are sweating, but then no problem. No, so in terms of hearing those, that is really real research going on right now here at Penn State. And that is very cool to get. Just to see this actual research that is going and then in societal goals that you are attempting to use autonomous systems for, in emergency situations and rescue situations. And that adaptability piece is so fascinating.

Alan Wagner: Yes.

Anne Toomey McKenna: All of those human factors have to come in, so I think it is going to be really interesting now to turn it over to the Major and talk about this. But if you can just give us that hands-on understanding of how the Pennsylvania State Police are using AI and autonomous systems right now, and where you see its benefits and where you see its constitutional concerns.

Douglas Burig: Thanks. There is no question that artificial intelligence and autonomous systems are having a significant impact on what we are doing in law enforcement today. In my view, mostly a positive impact.

It is changing at a rate that I have not seen anywhere in my twenty-five-year career to this point. But I think the challenge for us is to continually innovate, to embrace these new technologies to see how they fit into our world. But also, respect and protect peoples' privacy, civil rights and civil liberties while we are doing it. I find that the change in technology is sometimes outpacing what the courts can help us decide, or any policy that is set or any laws that are passed to help govern this, which I know Marc on the end is going to talk about a little more.

Douglas Burig: Just one of the technologies I will talk about today, just to give you some real-world examples of how is this benefiting you. How is it helping to protect you and your families on a daily basis? But we are having a tremendous amount of success with facial recognition technology. The same type of technology I used to get through the encryption of my laptop this morning just by looking at it, that

you log into your phone or you tag your friends on Facebook with is solving crimes every single day.

Doug Burig: Fifty years ago, because we know offenders are largely recidivists, we would take bookings, arrest photos, and show them the victims of violent crime to go through them, to search through it, and pick out the person who committed that crime. Now, this intelligence, this artificial intelligence can comb through twenty million drivers' license photos and three million arrest photos in three or four seconds. I mean, just think about the power that it has today.

Just a couple of real-world examples, and these are recent. First of all, this is one of the caveats with facial recognition: it is not discriminative enough to be considered identification. It is not fingerprints. It is not DNA. There is a disclaimer when you log into the system that tells everybody that is using it that. So I don't want anyone to think that it is definitively the person when this query comes back. And we do not treat it that way. If we were to use that in evidence, as probable cause for a search warrant, it would become fruits from a poisonous tree, and we would have no foundation. So, we do not do that with this technology.

Douglas Burig: Also, it does not have to be a head on shot. The technology is now 2D. When I first started this, it had to be a pretty much a head-on shot. Now if the head turns the side, it can interpret with the data points and look on the other, and fill it in. Of course, it is a lot less accurate that way,

but just in the last couple of years, this has changed dramatically.

Douglas Burig: This is a case from four weeks ago. This is a homicide in the eastern part of Pennsylvania. It is still an ongoing case, so I cannot say a whole lot about it. But a young man was killed and a witness was able to give a nickname for the individual, and a possible spot on Instagram to look for them. That is all they had, and that is the actual photo that was given. Obviously, the center part of their face is blacked out.

How long would this have taken trying to get an image out in the greater Philadelphia area to identify this person? But our analyst sitting in her cubicle in Harrisburg, in thirty seconds was able to get a hit—what we would call a hit—on this image for this individual. So, that is an arrest booking photo from two years before.

Now, once they started layering in, and that is really what makes it valuable in law enforcement. We started layering in the other data sources that we have, look at the criminal history, and where does this person live. It became apparent very quickly that this was likely the suspect. This is transmitted to the investigators, and through the independent investigation, and eventually witness identification. This is the person, and he's currently awaiting trial for homicide.

Douglas Burig: This is another one. Unfortunately, a young woman was raped. This was North Central Pennsylvania. This is November of 2018. She did not know her attacker's name, only knew a nickname, and there had been some conversation back and forth on a social media platform. So this image was sent into our

analysts who ran it through, and that is an Instagram photo. Again, within about two minutes, they were able to identify this person or get what we would call a hit. A strong correlation that it is likely the individual.

Douglas Burig: It is interesting. When you see the returns come back, you will see both males and females because it is only looking at jaw angles, and distance between your eyes, and things like that. So, you will see both males and females come back. Sometimes you will see the person wearing the same clothing that they wore in their driver's license photo while committing the crime. Or there will be a very distinctive image. A tattoo that is visible on their neck where you don't have to be an expert or a scientist to figure out that that is probably the individual. Layer the other data sources onto it and get it out to the people that are doing the case.

How long, again, would it have taken to identify this person through social media or through banging on and just becoming part of the daily news cycle? So, this is something that, when I started law enforcement, we could only dream of.

Douglas Burig: On the national security side, this is a case the FBI was working on. An international terrorism suspect that had social media presence in both a foreign country and in the United States. They did not know who this individual was. The case is going for quite some time. The agent sent it in to us, and we were able to identify the main target and three accomplices. This is somebody that was planning with other terrorists to do harm to the

United States, yet it was in a Pennsylvania database that helped bring together this international terrorism case.

Douglas Burig: It also shows the value of sharing information, and working collectively with all of our partners. Something that we learned well before 9/11, but was certainly made increasingly apparent after that horrible event.

I just want to talk briefly about some of the protection. So we have access to all this information. We have your social security numbers. We have access to an incredible amount of data that we are entrusted with. So, how do we protect that? How do we ensure that it is not misused?

We are very cognizant every single day that one misuse of this type of technology can result in it being taken away, and we would not be able to get justice for other victims in future cases. So we are very, very cognizant of that. We don't wield this lightly. I hear analysts and our investigators talking constantly about how much can we collect on this? Should we share this? Who can we share this with? And that is where we want to be in law enforcement. But this includes the collection, the use, the analysis, retention, destruction, sharing, and dissemination of protected data on all fronts.

Douglas Burig: First of all, the training component. Nobody has access to the systems without extensive training, without non-disclosure agreements, without regular training. This includes both the state statutes, which for criminal justice information in our state is 9102, 9106 and Title 18. And the federal regulations 28 CFR, Part 23, which I just took my annual training on two

weeks ago. Even at my level, I still do it every year. I spend the three hours because I oversee the program. That is how seriously we take it.

Douglas Burig: Restricted access. All these systems are closed. I think you have heard from the panelists today, there is no system that can't be penetrated. However, I haven't seen it on UC systems that I am talking about today. They have to meet pretty rigorous FBI CJIS standards, which is criminal justice information sharing systems. So they are defended about as well as it possibly could be.

They also have really extensive audit trails. In our intelligence system, it is searchable to the keystroke. There are audits that are done by outside people that don't have a vested interest in the Pennsylvania State Police, as well as internal audit controls with mandatory numbers of inquiries that you would have to be at to look.

Do people abuse the systems or misuse them? Unfortunately, that has happened. But many of our people are not short timers. They are in this for a career, typically. And the penalties include suspension and termination, and I have seen both for misuse of UC system. So, we take this very seriously.

Douglas Burig: Also, with our privacy policy, we are very transparent. It is available on the state police website, and we have a privacy attorney embedded in our function with a top-secret security clearance who has a backdoor, all-access pass to everything that is going on. We often speak to her during different aspects of the collection or dissemination of information to get her insight, and she has the right legal

acumen to be able to do this. This is not somebody we call the privacy officer. It is a highly qualified individual, and I know our federal partners operate the same way.

Douglas Burig: But I hope that gives you a little better view, and we could talk endlessly about the other autonomous systems, UAVs, drones. The state police just got into that technology. Just purchased it. We took a little bit longer than other agencies to get to that point because we want to be very deliberate.

Just for example, the last helicopter we purchased was $8.5 million. The drones we bought this fall were $2,500. So, when you look at efficiencies and uses, and the capabilities are largely the same, especially if you are not in the medical transport business. This is something to think about. I don't think we will have a fleet of helicopters ten or fifteen years from now.

Anne Toomey McKenna: Maybe, can you give them some examples of how UAVs will economize what you need to do across this big state?

Douglas Burig: Sure. Right now, we wanted to be conservative when we started with this program. So, they are being used for accident reconstruction. So normally we would shut down a road, impede travel and commerce for four or six hours at a time. The drones are doing fly-overs. They are doing several million data points, and usually in about thirty minutes. From a lot of different angles, we get all of the measurements that we need and the road gets opened sooner. We are also using it for a crime scene reconstruction. We can get all the distance from the victim,

from shell casings, and capture everything—any weather in a matter of moments. We are also using them in the search and rescue aspect of things. Certainly, a lot quicker to get them up.

Douglas Burig: Also, in the special emergency response team, we already have an exigent circumstance around somebody's property for shots fired, for a barricaded gunman situation, and why risk tactical members to go up to the window and see if the person is lying in wait for those officers? Or if he took his own life a half hour ago, and they are flying up to these windows, sending information real-time and out to people on the scene that have to make decisions.

We saw in Georgia overnight; two police officers were shot trying to enter a house. A hostage situation. Three people were killed. I see a day where there will not be live police officers, and I think my panelists would probably agree, we will not be entering these situations. It will all be autonomous vehicles taking the risk.

Anne Toomey McKenna: Thank you very much, Major. We have really heard the broader concepts from Dr. Atkinson, and Professor Wagner's research, and I am excited to turn this back to someone who comes to us both from the technology standpoint with the experienced research you have done, and you are in the thick of law school.

Marc Canellas: Yeah. I mean, it is wonderful to follow Doug, especially someone who wants to go into

criminal law. But on the defense side and has a slightly different perspective.

Marc Canellas: Yeah. No, but this is exactly the type of conversations I think we need to be having. That there are cases where this technology has been used, is being used and actually has some real promise. I am going to have a slightly different take though.

I was trained in graduate school by Amy Pritchett, along with one of her students, my PhD advisor, Karen Feigh. And my training was essentially, as someone brought up the Boeing 737 MAX 8, our job was to make sure the Boeing 737 MAX 8 would never have happened. The interaction between the pilot and the autopilot should never have become a situation where it crashed into the ground. So that is a very stark reminder of me of why I went to law school, is to make sure bad things like that don't happen.

Coming from my background, I'm trying to combine all of this and talk about challenges and steps forward. The first one—and these are five general thoughts that I have that are hopefully somewhat provoking—give people some thought. The first is that "Our wars are all intertwined." The war on terror, war on drugs, war on crime. They share the same technology, tactics and failures.

Marc Canellas: I mean that to say that, especially at NYU where I am, there's the international law people, and then there's the criminal law people, and there's the IP and technology law people, and these are all together. There may be domains where they are applied, but the tactics are being shared, the technology is being

shared, and the failures translate as well. Even the metaphor, the war metaphor, translates as well.

Marc Canellas: And so, we must look at how these technologies are being deployed, outside of things like accidents and crime scene reconstruction. You have drones that were developed for the military but used to surveil Freddie Gray protests in Baltimore. You have stingrays which simulate cell towers that were developed for military purposes, then DHS licensed them out to police forces, and now they're being used for domestic criminal investigations.

You have advanced cyber and surveillance techniques developed for the military, but then unconstitutionally used against Muslim populations by the NYPD. So, there are ways that, not particularly-good-faith actors can use these technologies against populations. And so all the concerns about discrimination, disparate effects on minority populations, and criminalization of poverty, are influenced by the technology developed in the international scene. If you think about autonomous weapons abroad, I hope we think, at some point, about what happens when we arm drones— what happens when we arm robots in America? When you come face to face with one? I would prefer a police officer. That is my preference, but I think that's a conversation we have to have.

Marc Canellas: Second, "technology is not neutral." This is my sort of slightly Southern coming through. It ain't magic, and it certainly is not our savior. It's not neutral. So even normative technology

built with the best intentions can be used in bad ways by people acting in bad faith. Body cameras were supported by the NYPD and even the ACLU for use in New York City. The idea was that was going to bring accountability.

Marc Canellas: But they did not realize its other potential. There is a recent case just a few days ago, where the NYPD settled the suit, where they had edited videos to make it seem like they had the warrant before they entered someone's apartment when, actually, they had flipped the order of the video. So actually, they had entered, already left, got the warrant, re-entered, but edited the video to make it seem like it was the other way around. So, when you control the video of body cameras, if it's not governed correctly, if there's not enough safeguards in place, it can be used in bad ways.

Magic has already been talked about. Patrick and Mike talked about this earlier. This is advanced technology. It is. And it's certainly complicated and may have some emerging properties, but it's not magic. It's also not our savior, and I'll leave this to Noreen, the theologian, who will be talking in the next panel. We cannot think of technology as the only solution to our problems. That if only we could use AI to filter out things like extreme content, if only we had robots that could do all the dirty, dull law enforcement work, we would be better off.

Marc Canellas: The minute we call it magic or deem it a savior, and appeal to these higher powers where we are abdicating control and responsibility for our own actions and our own responsibilities

as people in a democratic society. And I think we have to hold that together.

Marc Canellas: Third, "law and policy are designed to be slow, methodical and backwards looking." I've used the word design there very deliberately. They were meant to be this way. When people founded it, that was the goal. When law was developed, precedence was the goal. And so . . . Huh?

Anne Toomey McKenna: You're good.

Marc Canellas: No, no. I want to make sure because the question and discussion is going to be the most interesting part. So, I hesitate to go down this direction when I have an immense privacy and a wiretapping scholar next to me.

But I think about the Carpenter case from 2018, which is, I think, a very useful example. Hopefully, I get the story right. Otherwise, I will get graded. Let's say you're arrested for robbery, and the critical information that was used to identify you, placing you at the scene, was gathered by police who accessed your physical location through phone records. You're convicted, but you're really upset. You're saying, "There's no way this can be constitutional." You think it violates your Fourth Amendment right against warrantless search against and seizure. So, you appeal. The problem is, laws are based on precedents.

Marc Canellas: For many years, there's been something called the third-party doctrine, where the minute you gave up your information to a third party, it was no longer yours to be protected against. But in 2018, the Carpenter decision said that

actually, there are certain ways that you are protected against this third-party doctrine. You may be very happy you won. But this has been going on for twenty plus years, the law is not proactive. Only when things go wrong, Only when there's been enough time to get it out into the general public that certain things are going on do we really see the law actually react. It is not proactive.

Marc Canellas: Maybe you say, "Oh, I'm going to go to Congress. Congress will listen to me." I have lots of thoughts about that, obviously, given my time there. But the problem is, Congress's primary job is also not to pass legislation. So, they're doing their job really well in some ways at the moment.

But their job, the first thing I was told when I worked there was, "Our job is not to pass good legislation. Our job is to stop bad legislation." The entire process is built around the battles, of people coming together, forcing laws into action only when everyone can agree that this is the right way to go. So, these are deliberate bodies, whether it be law or government, that are meant to go slowly.

As you think about the pace of technology, it is inherently outpacing law and government. We have to decide as people what we want to do about that. Whether it's the stories we tell ourselves. Whether it's the engineers coming together and saying, "We need to self-regulate and establish standards." Whether it's lawyers coming to the fore. Whether it's police agencies saying, "We're going to do this the right way, even though there's no law against it." So, we have to take control of it.

Marc Canellas: The fourth one's a little cryptic, "the oracle has been poisoned." This was when I worked on the Hill in 2017 to 2018. I worked a lot on election security. There were reports that the Russian Internet Research Agency, which helped do some of the cyber-attacks on our electronically-influenced campaigns, they called it "poisoning the oracle." What they meant was that elections are actually based on trust.

Elections are based on trust. It's not to convince the winner they won. The winner always thinks they won. It's to convince the losers that they lost. So it's about trust. It's about trusting the process, trusting that people got their vote counted correctly.

If you can convince people that their votes were not counted correctly. If you can convince people that there are nefarious actors, deep state, fake news, rigged elections—however you want to describe it—you can undermine, even if you did not hack. Even if you did not actually get in there and change any votes, you've already destabilized it.

Marc Canellas: And so, this idea of trust, which is why I know a lot of what Alan does. Trust is inherently critical to a lot of our general governing of our society. And you can poison the oracle if you can use things like deep fakes. So, you're recording video, you can create alternate video making the President or anyone you want say the things you want and have a video. That will spread like fire across the Internet. You look at India and Pakistan recently with their information warfare, and reality does not matter. If we live in a world where reality does

not matter, everything starts to break down. And AI is only going to increase that capability.

Marc Canellas: Adversarial AI is another one of those things where you can actually make an algorithm, by attacking the data that it's built upon, characterize things wrong. Characterize threats when there's not a threat, and characterize certain people as a threat when they are not. That's going to be a problem.

All of this to say the last point. I put it in bold for a reason. **"People are the beginning and the end of everything."** They are the only reason we care about things like autonomous weapons, things like autonomous vehicles. Yes, there's efficiency, there's money to be made. But we care about the people's lives that are at stake. We care when and how people are killed. We care about the safety of people. That's something we can't forget. That's what I learned from my lab down at Georgia Tech.

If you don't understand the humans involved, their lives, their needs, their wishes, these minority populations, these criminalized groups. If you do not understand and you don't go out to reach them, you will never succeed.

Marc Canellas: I just want to close and say, the hard questions are not going to be technology questions. The technology is sitting up here. The technologists sitting there are brilliant. They're going to continue to do amazing things, I have no doubt about that. The questions is: what do we want them to do?

I love this discussion of storytelling. What stories are we going to tell ourselves about the future we want? What are the norms we're

going to set? If we don't have that, then how can we possibly ask Congress or the law to reflect our will when we don't even know what our will is? And so, I think there are good ways to do it, but I implore you to start with the humans. Start with us. Thank you.

Anne Toomey McKenna: Alright, so we can take questions. But I am going to go ahead and just ask questions for the group. So, if you know you have a question that you want to ask, please feel free to get up and come to the mics.

I'm just finishing up and really setting the broader question. How do we handle this from a legislative and policy standpoint?

We see very different approaches, both with your Europe's EU's GDPR, General Data Protection Regulation, there's very different approach to data and use of data, including use of data by algorithms because it's all humans that are doing this and driving this.

Anne Toomey McKenna: In the U.S., how is that playing out? And what I tried to set that stage for, and I think you've gotten a little of this, is that we have this really kind of disjointed approach to managing autonomous systems because they fall in different categories. So, they're regulated by different institutions and agencies. So, these are some of the broader questions I know we think about. I see that we've some people up here.

Audience: Thank you for that very interesting discussion. My question has two parts, sorry about it. It's mostly directed to Marc because you talked

about *Carpenter*, but anybody can answer it. Do you think third party doctrine in this new era of technology still a viable doctrine? Or do you think we should throw it away?

Audience: The second part is, and probably anybody can answer this. Do you think our expectation of privacy decreases as the technology rolls? Or it stays the same, or even increases? Because we have signed a lot of privacy policies and so on.

Alan Wagner: I will defer to the leading scholar on things like that, and then I can address the second part.

Anne Toomey McKenna: Okay, so, I'll go with the first part. Just so everybody in the room who are non-lawyers understands that third-party doctrine states in law, that if you share something with someone else, you can't really claim that you have a reasonable expectation of privacy in it under the Fourth Amendment to the United States Constitution against unreasonable searches and seizures.

Anne Toomey McKenna: The problem with third-party doctrine is that it was passed in cases, precedents that occurred long before the Internet existed. And so that idea was, of course, if I'm sharing something with David sitting next to me, how can I say I have a right to privacy in it? As technology changes, the platforms evolve. Every single thing you do online, everything you do in our society is necessarily shared with a third party: the companies, the platforms that are operating these technologies.

So, in *Carpenter*, the Supreme Court very deliberately said, it is clear that we got

indicators in earlier cases, in USP Jones, Judge Sotomayor said it's clear the third-party doctrine is not working here. But very clearly in *Carpenter*, Chief Justice Roberts made it and, "Hey, this third-party doctrine is not working. We can't say just because we shared something with someone using technology that we no longer have a right to privacy."

Anne Toomey McKenna: Remember, the piece of that, though, that's important in all of these conversations is: there's a massive distinction in the application of law here. Private companies are not bound or restricted by the First Amendment or the Fourth Amendment. Only the United States, only federal law enforcement, only the government is restricted. So everything, that's the data aggregation that's occurring, that's part of our problem. We don't have parallel privacy standards or parallel privacy law to regulate what industry does versus what government does.

Marc Canellas: Yeah, and I would say to the question, I think it's our changing expectations of privacy. We have quite a range of demographics in the audience. I'm sure by generation we have different expectations of privacy. The one I always come back to is convenience.

Marc Canellas: If you can make something convenient where I don't have to pay, I'll give you all my data. You make it convenient for me to reach out and connect with family. Facebook sounds great, even when people know what's going on in the systems. All this stuff with Facebook and Twitter, whoever you want to pick out, people still use it, because how else am I supposed to

connect with all these people? So I think the amount of convenience and in that trade off, I think people are happy to give away that convenience. But I think it's also because they have a new expectation of privacy.

Marc Canellas: It's not that they don't know they're giving up the data to a third party. It's that I trust that you will be good with that data. I don't know what good means in that sense. But I think a lot of us when we're giving up data to some of these companies or even to our universities, where there have been lots of breaches, we're assuming that they're acting in good faith. And I think the key, as was just mentioned, is that, commercial companies don't have to have good faith necessarily. And that's the change.

Anne Toomey McKenna: I do think part of it, though, is that consumers do not understand the amount of data that is aggregated about them individually. That just millions of data points that are aggregated about each of us sitting in this room, whether we are users or not of the platforms, somebody we know is. Every person in this room has a genetic profile that's probably being captured by 23andMe, and the like, because somebody you know did it. It doesn't matter if you did it or not.

I think that part of it is a lack of understanding in terms of what really is being given over for the convenience.

Marc Canellas: Yeah.

Audience: I have a question that speaks to what a few of you talked about, which is—it has to do with

the atrophying of our skills based on our reliance on technology. David, you talked about the possibility of having a car that you could just tell to engage in parallel parking. Of course, parallel parking, which is notoriously difficult, requires all sorts of skills that we been a long-time honing, and a lot more time honing before we had power steering.

Audience: Before I could just look up phone numbers on my smartphone—or my phone is storing most of the numbers that I ever used—I had memorized hundreds of phone numbers and, actually, there are all sorts of therapies that require kids to memorize numbers and recite them backwards, and so on. So, we're losing the skills. Already they find that they have a grave difficulty having adequate surgeons and training surgeons because our fine motor skills are starting to atrophy so much.

Alan, you talked about people being willing to follow these emergency guided robots. Now, that reliance on technology then has a feedback loop, because the skills that you would use to guide yourself in emergency will start to atrophy, because we're so willing to follow technology. Personally, I refuse to follow my ways about, maybe a third of the time, because it's wrong so often. But if it got more accurate, I'm sure I would follow it.

David Atkinson: I think there's no question that we lose skills. How many people know how to build a fire in the woods with wet wood? Oh my gosh, okay. I'm shocked. Okay, bad example. But the point is, this is the history of technology. We don't build fires in California.

The history of technology is giving up some things. Okay, how many people know how to shoe a horse? Okay, fewer good. Better example. That used to be a real important skill. It's not anymore, and life has moved on and there are alternate ways of getting the function of mobility done. And so, I think we've sacrificed a lot of skills. And the question is, we're not actually being conscious of the fact that we're shifting like that.

David Atkinson: My kids can't use a map very well at all. Their entire world is based on point-to-point. I get into my car here, and I follow the line on the road, and then the phone tells me to follow. And they just don't have the spatial context anymore.

Audience: Do we have a grip on how this is affecting our brain development, on how this is affecting our evolution as a species? I mean, I think we don't take these costs seriously enough. It's not just, "well, I don't need to shoe a horse anymore. So, never mind, I don't have to worry about that." These skills really are critical for development at all stages of development with children and learning.

Alan Wagner: There is research showing and more recently showing drops in empathy with younger generation—specifically, people that grew up with cell phones—lack of emotion recognition, emotion understanding, nonverbal behavior. These types of things. This all sort of shows a very age-based curve which mimics, to some extent, cell phone usage.

Alan Wagner: We see that these things do impact people. There's especially more recent results that show that children under the age of two or

three that spend more than an hour on a phone or any kind of device, lose language ability pretty quickly. And that length, lost language ability doesn't come back very quickly. So this is not necessarily permanent, but it is certainly sort of delayed development with regard to these technologies.

Alan Wagner: So, you can wonder how the sort of humanoid robot taking care of a child might impact them if a cell phone is already impacting them.

Audience: Sure. So this is actually a good segue into things. My point is that, what I've been hearing is sort of anecdotes, and you pick up the elephant and you say, "This part doesn't look good." There was a comment which says, the audacity or something like that of human beings to think that an automated plane could fly. I think there is a reverse audacity in thinking that you could actually beat a computer in chess.

The point is not to pick individual pieces that we say, we can find out several examples where it's bad, we can find out several examples where it's actually saved thousands of lives. The thing to do, perhaps, is to get a total evaluation, a more realistic evaluation with projections, and then have a conversation. So, is the conversation getting just primarily focused on what we want to see? And should we move on to a bigger picture overall evaluation?

David Atkinson: No, take a seat. There is a mindset that persists that says, we're going to put the human at the center of things and consider the systems and the technology around the human. But as our machines get increasingly intelligent, as they

communicate with us and ever more natural ways, as they gain greater ability to manipulate, they're going to become more like partners and less like tools. And we have to ask the question, what is the combination of a person and a machine together as two cognitive entities in this larger system? What is the capability of that larger system? And stop thinking about just the human and augmentation is a partnership.

David Atkinson: That may be far out, but that's the vector. That's the direction we're going. And so this is a very good question, and thinking of things in that system context.

Marc Canellas: If I may, just briefly, to bring up something like the Boeing accident, or autonomous vehicles, or I think even like the face recognition systems is exactly this. A lot of automated systems are not designed even accounting for the human at all. It's, "I can do this cool thing. I can deploy it really fast. I'm going to take the market. This is going to be great." Not, "how can I design a good team mate?"

As we talk about in chess or driving, and I'm sure a lot of the tools that are used by the police. How can we work to together using both of our skills, and both our checks and balances on each other to make sure we're both operating effectively?

I think if you approach it from that mindset – not as one has to be better than the other and replace or substitute – but teammates. That is the way to go about it. Unfortunately, I think that's often not the way it's gone about.

Anne Toomey

McKenna: I think, I mean, the major gave us an example of that's how Pennsylvania State Police are using facial recognition. So very, like, it's a team-based approach to the use of not just the technology as this is the person, and the technology is providing maybe more secure responses than an eyewitness potentially could at the get go. That combination of human investigation and technology. We're out of time.