Constellations Podcast

Episode 73 – Security, Privacy and the Blurred Lines Between Them

Guest: Robert Cardillo, Former Director, National Geospatial-Intelligence Agency– 32 minutes

John Gilroy: Welcome to Constellations the podcast from Kratos. My name is John Gilroy and I'll be your moderator. Our guest today is Robert Cardillo, former director of the National Geospatial Intelligence Agency, current distinguished fellow at Georgetown University's Center for Security and Emerging Technology and founding member of Orbital Insights Federal Advisory Board. During this episode we'll be talking about new developments, both good and bad, concerning artificial intelligence and machine learning and we're recording this interview from the floor of SATELLITE 2020.

John Gilroy: Robert, having fun at the conference here?

Robert Cardillo: I'm having a great time, but I have a feeling it's about to get a little better.

John Gilroy: Now, hopefully we'll have a little fun here. Back in your NGA days, you said that monitoring and exploiting commercial and proprietary video and imagery feeds around the world is on the precipice of a data explosion similar to when the internet took off. Has that growth met or exceeded your expectations?

Robert Cardillo: So one, John, thanks for having me. I'm going to enjoy this conversation and look forward to our exchange. I would say that since I've left government, it's been about a year now, the confidence I had before about that explosion has only been increased as I become exposed to more and more companies and more and more innovators and more and more approaches to sensing our planet in a way to advance humanity's cause, I have been refreshed and rewarded by those advances. And while I know there are concerns that we should discuss today about the other side of all of that sensing, I'm quite confident that we're on a good path.

John Gilroy: You know, I heard the folks from Planet give a talk yesterday and they talked about generating 11 terabytes of data every day. I mean that's just a number I mean 10 years ago would you believe that number? I mean it's incredible.

Robert Cardillo: That's right. And I'm sure tomorrow it's going to be more.

John Gilroy: Wow. So the question is how do you analyze that data, huh?

Robert Cardillo: So one, if you still have any sort of proclivity to doing it the way that Robert Cardillo did it as a young analyst, you need to get over that. What I mean by that is that if we don't take every advantage of what I call automation augmentation and then eventually artificial intelligence, we have no chance. You jumped to the verb "analyze", I would take it in stages before you even get there. I think

there's a certain amount of just pre-processing that needs to happen, filtering, synthesizing, amalgamating in a way that gives you context. You do want to get to the point where you can make sense out of all that data which gets you to analysis. But there's many stages on the way from one to the other.

John Gilroy: You know, a wise man once said with all this information out there, all these terabytes information that they have to try to derive coherence from chaos. Now who said that?

Robert Cardillo: Indeed. Indeed. It may have been coined in this hall when we held the GEON symposium here in 2015. Well look, I thought it was a catchy way to grab attention.

John Gilroy: It's a great line. I love it. And it was thinking about that will all those terabytes.

Robert Cardillo: It fits on a bumper sticker, which is important these days. And interestingly, I was in the green room after my remarks in which I first used that phrase and then the Deputy Secretary of Defense, Bob Work was about to go on next and I took it as a great compliment that he turned to me and he said, "I'm stealing your line." Because it does work in many different scenarios.

John Gilroy: Steel it fair and square.

John Gilroy: Well of course there's much news about big data and artificial intelligence, machine language, space, data collection. How was NGA adapting to these developments as you left the agency?

Robert Cardillo: Well, let me put it this way. When I got to NGA, came back to NGA in 2014, NGA was in the midst of a debate and the central question in the debate was "Should we?", Should we engage with these new companies and these, what we would call, nontraditional sources and partners. When I left NGA last year, so four and a half years as director, that debate had shifted from "Should we?" to "How do we?" Now we hadn't finished answering that question and happy to talk more about where I think we made progress and where I think we need to make more progress, but we had moved to our front step. We were leaning into the question, we were leaning into the opportunity and we were beginning to make progress.

John Gilroy: I see a lot of parallels with people talking about open data and open source software and especially people in the intelligence community, being kind of wary but careful and examining options and trying to consider how it can work for them.

Robert Cardillo: Where it's appropriate. As intelligence professionals we're somewhat trained to be wary, to be cautious, to be deliberate. Because that's in the nature of the trade craft. What I would say though to my teammates who have that wary hold them back from perhaps engaging with the opportunity is that the day in which our profession was predominantly government owned and operated is over. Doesn't mean the government's not a big player, not an important player, not a big contributor to the outcome, but if you think of the baseline of information that's available to all humans, the preponderance of that is open. So if you're going to properly frame a question or an opportunity or issue a warning, you have to do it within that broader context. So engage with it, sustain your wariness, always ask questions, be deliberative, but then carefully move to that point of decision and use whatever government opportunity that you have to create a better outcome.

John Gilroy: Back when you started your career, the catch phrase was, "Trust but verify." Maybe pull that out of the 40 years ago and apply it today, huh?

Robert Cardillo: I think it's the same. I just think we have less time between that trusting and that verifying. I think it's a continual loop these days. Whereas it was more segmented back in the day.

John Gilroy: All kinds of presentations being given here at SATELLITE 2020, artificial intelligence and the space satellite operations and everything else, so what can you tell our audience about Sentient, this is a product that uses AI to analyze data of all sorts. Can you give us a clue what Sentient does?

Robert Cardillo: Sure, so Sentient is a, I'd call it a test bed, we were pursuing in the government to try to take technology that's either on this floor today, current off the shelf capability, or a new piece of research that's being tested and evaluated, apply that technology though against government challenges. You mentioned some of the conversations that are happening on the floor. I mean I'm hearing things about agriculture improvement and environmental security and water resources, all important things for humanity. On the government side, we might want to take that same technology that would increase the yield of an agricultural effort, but apply it in a way that gives us insight to perhaps a threat or an opportunity. So Sentient was a way to bring those tools into the government space and then create a different outcome. Again, it could be based upon a military employment of force, or it could be on the reverse, it could be something to secure an area of great import.

John Gilroy: Now if you take off your headphones, you can hear a presentation behind us and they're talking about precision agriculture. I never realized that they can plant seeds down to the centimeter now. I mean, it's really amazing what's going on now.

Robert Cardillo: Yes, indeed. I mean, like I said, I joined the community three and a half plus decades ago now and when I joined if you needed to image sense something in an area that might be denied to you, so in those days the country was called the Soviet Union and that was a denied area, you had to learn how to fly a very large camera in space and you had to learn how to figure out how you're going to get that image back down to the ground.

Robert Cardillo: To your point about the agricultural conversation behind us, that could be a drone collection that's operated by the owner of the farm to create minute detailed understanding of their agricultural production and then to be able to tweak it, tune it to create the outcome they see with a higher yield and more income.

John Gilroy: So Sentient can be used for doing some predicting of what's going to happen in the future. And this is really the important part, I think a lot of what Sentient's doing, is that correct?

Robert Cardillo: That's right. Not everyone has the issue, but since you raised the word, I'm not big on prediction in the intelligence business. Weather forecasters can do that, I prefer the term anticipation or anticipatory. Because let's face it, at the end of the day, even with all these sensors and all this information coming in, what we're really trying to understand as an intelligence professional is what another human will do tomorrow, and humans remain complex characters. And so I think I prefer to say the best thing I could do for a decision maker was to give him or her the most likely outcomes that we anticipate given our current understanding of a situation. And then that decision maker can then make a more informed, arguably better, decision about how they're going to behave or how they're going to act.

John Gilroy: Well, let's talk a little bit about humans. 2000 years ago a couple of humans come up with this phrase, "Who guards the guardian? Who watches the watchman?" You know? And I think this is coming to more and more in favor what's going to happen with what's going on in the world today. Now when we were preparing for this podcast, you indicated that you had a strong interest in the concept of machines watching us, machines watching machines, back to Ancient Rome isn't it.

Robert Cardillo: Indeed.

John Gilroy: So can you explain your interest in these topics to our listeners?

Robert Cardillo: This will, I think, be a nice segue, John, into the conversation about the other side of this persistent, continual sensing that's ongoing. And what I mean by that is we've talked about some of the advantages and some of the insights and

some of the improved outcomes that can be created through this sensing. I think we also need to acknowledge and have an open conversation about what are the limits that should be applied to the access to that data, to the use of it. Can it be applied in a way that enforces a legal constriction? Or can it be used in a way that would inhibit my sense of personal privacy. And the answer to those questions is yes, depending on where you're sitting at the time. So to go back to your central question, what I think we need to do is have conversations now about who's watching the watchers, meaning who's monitoring the data that's being collected? How's it being stored? How can it be accessed? And while I have a strong belief that that conversation won't ever end, nor should it, I think having it will lead us to better decisions about the use of that data.

John Gilroy: And we both are involved in the university community. And this is a question that doesn't have a multiple choice answer. It's not a multiple choice answer. It's a long involved answer that has to flex and change with what's going on in the show floor.

Robert Cardillo: That's right. I mean I believe strongly that this question, this challenge that we have is one that we're going to have to manage continually. To your point, there's no outcome. There's no date specific outcome. People talk about, "What's the balance between security and privacy?" Right? Like there's some midpoint in there that if we just found it we could just move on to the next challenge.

John Gilroy: Multiple choice, yeah.

Robert Cardillo: I think the reality is, the answer to the question is, it depends. And so you have to be case specific. You have to talk about what are the uses? What are the outcomes? What are the implications and consequences, etc.? But as soon as we conclude that conversation today, guess what? We'll have another one tomorrow.

John Gilroy: If you did a study, I'm sure you'd find that around 75 out of 176 countries are actively using AI technologies for surveillance purposes. So what is the risk to personal privacy as surveillance, especially government surveillance, becomes more pervasive?

Robert Cardillo: The risk is all around us. So let me put it this way, it's difficult if not impossible to walk through a major urban center on this planet today and not be imaged almost continually. Some of that imaging could be local government, could be police, could be rescue, could be local law enforcement. Some of it is, and I would believe most of it is, private because for security purposes and monitoring purposes, businesses, etc., want to be able to secure their livelihood. The question then becomes, as I'm transiting through public space,

but now being sensed through both public police or private company sensing technology, one, I think that's our reality today. I don't think there's any reverse switch on this. I don't think we were going to go back. Two though, I do believe we should have more conversations about your question about how could that be used either for me, so personal security to counter crime for example, or against me if, say for example, I didn't have an interest in someone knowing that I was in this part of town at this time of day. And so to me that again is the conversation that needs to be elevated. Who has access, who has control and who has use.

John Gilroy: I think everyone listening remembers the Bourne movies. There's a famous Bourne movie, they were in a train station, all the cameras are watching them, right? They're directing at him and trying to find out where he's at. And I think that's traditional what you think of surveillance, AI supporting cameras maybe, and they're on train station or a lamp post in London or a convenience store down the street, what happens if this surveillance goes up in the air? It goes up into satellites, what happens when we're no longer aware of the fact that we're being watched and analyzed?

Robert Cardillo: So John, I hate to break it to you, but it's not a future tense question because even though you and I are, because of my background, talking more about imaging, photographs, that sensing from space is happening now. You and I will have a smart phone on our person most of the time. When we open up any mapping application on that smartphone, you'll see a blue dot which identifies your location. Now, the reason that blue dot appears on your phone is because there's at least three satellites at geostationary orbit, so 23,500 miles above us, that are triangulating our position continually. I consider that sensing. Now we are, I'll say I am, okay with that blue dot because it helps me find my coffee sooner, get home in a more efficient way, avoid traffic, etc. However, though, the corollary question is, I think, germane, who else can use that blue dot? And if you combine the locational information in today's technology with that CCTV camera that might have some facial recognition that can say, "Oh, that's just not a generic blue dot, that's the Cardillo blue dot. And look at the pattern he has set up or look at who he's meeting with and what can we infer about that?" I do think there is some risk to the latter.

John Gilroy: Let's talk a little more about the surveillance here. Now in many countries such surveillance is marketed as crime prevention or counter terrorism. We've seen it being pushed a step further in other countries and used to suppress political activity and for social control. Those are kind of scary words. So what's the risk of this application spreading to more countries?

Robert Cardillo: I don't think it's a risk. I think it's a reality. As I said earlier, I don't think there's anything that's going to slow this trend. I actually believe that the government, in my experience for the US government, policy development around this

question is trailing the technology. In some ways that's good, in a sense that, you know, the way this country works in a market based economy, you want innovation to move quickly and you want companies to be agile, et cetera. However, I think when it moves so quickly that the government can't keep up, which I think is the case now, I think it gets to your question about the downside risk.

Robert Cardillo: Let me put it this way, John. I think, as I said, I believe that our current sensed world is going to continue to grow and to become more complex. I would offer that, in such a world, I would be in favor of the liberalization of that data. What I mean by that is the open sharing of that data so that we have, I'll say, a kind of a common level of transparency. Again, to go back to my blue dot, we have found at least some level of comfort, now I'm sure that isn't a word everyone will use about that blue dot, because of the advantages that we create from it or we gain from it.

Robert Cardillo: I think we're going to have to find a similar level of comfort with this enhanced awareness. And, again, I believe strongly that the more we share it equally across society, I think the safer or the less chance we'll have of the downside to your inappropriate use of government action for example.

John Gilroy: Robert, thousands of people from all over the world have listened to this podcast. If you're listening now, just go to Google type in Constellations Podcast to get to our show notes page. Here you can get transcripts for all 71 interviews. Also, you can sign up for free email notifications. We have folks like Robert in the next six or seven months. Kind of tough to beat this interview.

John Gilroy: So Robert, I'm going to read a quote and you tell me who said it. Okay, you ready?

Robert Cardillo: All right.

John Gilroy: Here we go. "Geography is destiny." You should know that one.

Robert Cardillo: So Napoleon?

John Gilroy: Yeah, that's right.

Robert Cardillo: Look, people, oftentimes with kind of a scary, well, scary, sometimes a confusing name. What is geospatial? What is this geospatial intelligence thing, etc.?

John Gilroy: Right.

Robert Cardillo: I would talk to, especially in public; I would have to explain to people what this thing is. And I used to say, I said, "Look, the first time somebody moved into a cave, one of our forefathers or foremothers, they became interested in who was living next door." And then the first time somebody delineated, "This is my property and that's your property." And put some sort of barrier, a fence or a wall in between it, one became interested in what was happening on the other side of that fence or that wall. Good things or perhaps threatening things. That's geography, right? I mean humans have always been interested in where they are, where their friends are, and where there might be risks. I think Napoleon's application clearly was directly tied to the outcome that he sought.

John Gilroy: Yeah.

Robert Cardillo: And so I don't think that's changed. I do think that there are good and bad uses of it and I think, again, the more we have these conversations, the better we all will be.

John Gilroy: Before we took the little break there, we were talking about surveillance and you were touching on the word, "transparency", but you were just getting close, didn't actually say the word transparency. Let's talk about what's going on today. Last month, San Francisco became the first city to ban facial recognition technology by police and other government agencies. A similar ban is being considered up in Massachusetts, in Somerville, out in California, in Oakland. Now I think these are the exceptions for today, but more liberal areas of the country have some concerns. Do you think that measures such as these are an overreaction or is this just transparency or what does this all mean?

Robert Cardillo: First of all, I wouldn't say overreaction. Again, to my point about having this conversation and this debate and the discussion we're having today, I think these conversations are appropriate. And look, we live in a society in which we elect officials to manage the social compact between government and civilian, between privacy and between security. You've mentioned a couple of elected officials and entities that have made some decisions about limits that they want to put on the technology because in their mind, the risk, okay, to that sensing, to that transparency, is outweighing the benefit. I mean, it's a choice that they're making. So I'm all in favor of people making choices. I just would want them to be as informed as possible. And again, I'm not questioning whether or not those decisions were informed, I assume they are or were. What I'd like to do is to contribute to the conversation so that that next decision is, again, done in as much light as possible.

John Gilroy: I want to go back to that Bourne movie. They were just trying to identify a face, okay? "Who is this guy, Jason Bourne?" And what happens in the plot of the movie. But I think there are companies today that are developing products that attempt to infer and predict emotions, intentions, and anomalous behavior

from facial expressions, body language and voice and tone and even direction of a gaze. I think that's maybe moving into a little more dangerous area than, "That's Jason Bourne over there." Isn't it?

Robert Cardillo: I think it could be but, again, let me say, and by the way, I don't have time inside of the TSA and Homeland security but I've worked with them. But I am aware that, and this isn't just in our country, that for a long time people have been looking for signs or tell-tale indicators of nefarious activity; somebody's pacing outside of a bank or somebody's surveilling a movement of an armored truck, et cetera. And the reason that you would do that as you wanted to make sure that the bank or the truck was secure. And so again, humans have always been looking for those signs.

Robert Cardillo: I hear you, okay, that we're now taking algorithmic applications, applying them to facial features and trying to infer, anticipate a future activity. I do think because of the scale question, because it's one thing for humans to look for somebody acting funny. It's another thing for a machine to look at thousands of people over a long period of time. So I'm not disparaging the question. I just think that we need to scale it in a way that gets us to, as I said, the best answer we can today and then a better one tomorrow.

John Gilroy: Well, if we talked about Jason Bourne, we've got to talk about Lady Gaga. She does a famous song called Poker Face. Huh.

Robert Cardillo: Okay.

John Gilroy: Poker Face. It seems to me that there's some scientific warnings that facial expressions and other external behaviors are not reliable indicator of mental or emotional states, it's a poker face out there. So how worrying is that trying to draw conclusions from your poker face? Or not a poker face?

Robert Cardillo: Not something I worry about. And I guess because, as I said, humanity, human interaction, I think has some fundamental qualities to it. We're constantly going through our day without algorithms right now. Okay? We're not wearing the algorithmic glasses that are projecting an assessment of your facial reaction to my comment. But we're all looking for those tells today; body language or a nod or an expression to understand whether or not, "Ooh, am I making my point? Is this a safe environment? Should I trust this person?" I think we're making all those judgements constantly anyway. I agree that we need to be careful as we apply the machine filter to that, but I don't think it fundamentally changes, again, what is the human challenge of, "How do I make it through a day?" In the most efficient way and most effective outcome.

John Gilroy: There's an ACLU report out called of the Dawn of Robot Surveillance. Talks about all these identification characteristics and it would seem to me that if I were to bring this up in a conversation of eighth graders or 10th graders in the high school kids, they may talk about the Orwell book they had to read and go, "Well this is a lot like George Orwell. This is really what's going on." You think it's leading towards that?

Robert Cardillo: Well look, I think Orwell's warning is, has been and remains germane. I would offer another book, this is by David Brin who wrote The Transparent Society. And in the beginning of that book, David laid out a couple of scenarios in the future and one was, by the way, both states looked Orwellian, okay, because everything was surveilled continually. But the two differences he laid out between the two outcomes, one is all that surveillance was shared amongst everyone to include the police station and the interrogation room and etc., so that people could self-monitor other government behavior.

Robert Cardillo: The other outcome was the Orwellian solution in which that data only went to police headquarters, and so it was kept. And David challenged the reader to say, "Which outcome would you prefer?" Again, I've already told you my preferred outcome. If we're going to move to such a society, I prefer that it be open and shared across to everyone versus it held by the state. What I love about David's challenge is he wrote that in 1996.

John Gilroy: Wow. Impressive.

Robert Cardillo: He was way ahead of his time in thinking about these challenges.

John Gilroy: Well, we are at the SATELLITE conference, so we got to go from these heavy, serious ACLU conversations to the sky. So what happens when surveillance shifts from terrestrial campus to satellites, good or bad? How's that going to impact everything?

Robert Cardillo: I mean I would argue, given my background and my experience, I would say good, but I'd also say good or bad it's going to continue. And the reason is nothing to do with governmental use. It's commercial use. There is monetization, there is commoditization available with access to space. And so that reality will take companies from this floor, both launchers, satellite builders and then analytic applications on the other end and continue to create more and more of them. I think the bigger question which we've been talking about now here during this podcast is the, "Okay, so that data is going to exist. How can it be used? How could it be misused? And who decides when it's the former vice versus the latter?"

John Gilroy: Well, if we started this conversation with Jason Bourne, we've got to end it with Arnold Schwarzenegger. That makes perfect sense, doesn't it?

Robert Cardillo: Saw that coming.

John Gilroy: Yeah, we did. And Skynet, and the convergence of everything. I have a grandson and is he going to see Skynet? Is he going to see a conversion? Is he can see the singularity where all these cameras get together and they merge with artificial intelligence and storage? That could be a significant change to human civilization.

Robert Cardillo: How old is your grandson?

John Gilroy: He's two months old.

Robert Cardillo: Yeah. So I think one question is, "Will your grandson ever need or want to get a driver's license?"

John Gilroy: That's a better question, isn't it, yeah.

Robert Cardillo: The reason being, autonomous self-driving vehicles will appear before he turns 16, okay? That's for sure. He'll make a choice at that time as whether or not it's worth the trouble and the cost, etc. And I'm just going to make an assumption that the young man will find that to be an advantage, that he has that choice at that point. Okay, if most of the vehicles on the planet in 15 years from now are autonomously navigated there's almost no way to do that without some form of Skynet. Meaning that singular vehicle doesn't exist in and of itself. It exists within a network and a system and all of the vehicles have to be synced. And so, I guess I'm telling you, I think we're going there any way. I appreciate the Schwarzenegger warning that Skynet can be used nefariously, and that's why I think this conversation's so important. Let's not just blindly head into this, this world in which everything is interconnected, let's talk about it in a way that keeps it, I think, above the table and I think it in an open way and I'll say in a liberal, Western, democratic, lower case d, society, I think that's to our great advantage. The more that we can share.

John Gilroy: Instead of a brave new world, a transparent new world. Maybe that's another bumper sticker.

Robert Cardillo: Another bumper sticker. "Transparent new world."

John Gilroy: Yeah, we got three thoughts, great. I'm sure there's very few conversations like this taking place on the floor here of SATELLITE 2020, but Robert, unfortunately, we are running out of time.

John Gilroy: I'd like to thank our guests, Robert Cardillo, former director of the National Geospatial Intelligence Agency and current distinguished fellow at Georgetown University Center for Security and Emerging Technology.