Guidehouse and American University Speaker Series

Cautionary Tales: How Technology Implementation is Impacting the Law Enforcement Landscape Webcast

JOHN SAAD: Let's go ahead and get started. Welcome to our session today on "Preparing for an Evolution: Strategies for Implementing Change in Law Enforcement." Before we get started, I'd like to hand it over to Patrick Malone. Dr. Patrick Malone is the Director of the Key Executive Leadership Program, and the Executive in Residence in the School of Public Affairs at American University. We've been thrilled to partner with Patrick and his team at AU. And Patrick, over to you.

PATRICK MALONE: Thank you, John. And on behalf of American University and the Key Executive Leadership Program, I just want to welcome all of you to the discussion today. We've been privileged and honored to continue our partnership with Guidehouse, an organization, much like American, with a long-standing commitment to the values of public servants and to the heroes that deliver civilization to us every day.

Enjoy what I know is going to be a fascinating discussion of technology and law enforcement. And John, I'll turn this back to you. Thank you again.

JOHN SAAD: Great. Thanks so much, Patrick, and welcome everybody. And thank you for being here today. As Patrick mentioned, my name is John Saad and I'm the Managing Partner for Guidehouse's National Security Segment. We're thrilled to be launching this speaker series and as you'll see in a moment, we have got an esteemed group of panelists who are going to start to tackle some of these challenging topics, as we begin to explore this over a series of sessions.

This session is part of our series on "Preparing for an Evolution: Strategies for Implementing Change in Law Enforcement," as we mentioned, which is working through many of the complex aspects of strategic change in this dynamic environment. Today, we're excited to be discussing "Cautionary Tales: How Technology Implementation is Impacting the Law Enforcement Landscape."

Given the need for increased public transparency and accountability, as well as the complexities of integrating emerging technologies, we thought it would be appropriate to explore the best practices and lessons learned regarding managing these new technological capabilities, which enhance security and accountability, including cautionary tales of misuse and challenge implementations.

We will also discuss the current capabilities and the policy and legal landscape in areas where the law continues to evolve. While public discussions are currently focused on state and local departments, all law enforcement entities, including those at the federal level, are impacted by evolving public perceptions and expectations.

Thanks again for joining us, and I will now hand it over to my colleague, Jim Chaparro, who is a Guidehouse Partner, who will be moderating today's panel. And thank you panelists for being here.

JIM CHAPARRO: Thanks, John. Jim Chaparro here. First of all, I want to say that I'm really excited about today's panel. And before we jump into it, I just want to give some quick logistics for the audience. Throughout the session your mics will be muted, and you can ask questions by typing into the question box. I encourage you to do that throughout and we will field the questions. We're going to make sure

that we leave ample time at the end. So please, if something pops in your mind, feel free to ask it. If we run out of time to answer the questions, what we're going to do is try and get those addressed in the podcast that we're going to do to follow this. So please keep your eyes and ears tuned for that.

The field of law enforcement is rapidly evolving. The advance in technology, such as facial recognition, artificial intelligence, big data analytics, body cameras, and many, many others, are really changing the landscape of law enforcement. And as often the case, the technology often outpaces our ability to keep up with it.

I think it's also fair to say that the law enforcement agencies and individual officers are facing increased scrutiny from the general public, from the media, and others, with respect to how they carry out their missions. Notwithstanding that, the shifting technology and social landscape, the men and women of law enforcement put their lives on the line every day to keep our citizens safe and protect and serve our communities.

Today I'm thrilled to have such distinguished panelists here today to talk about the technology implementations and how it impacts law enforcement. I just want to do brief introductions to our panelists because we really having an impressive group.

John Markovic is the Senior Policy Advisor for the Department of Justice, Bureau of Justice Assistance. John has oversight of the body-worn camera policy and implementation program. He has also managed multi-million-dollar grant projects, as well as associated delivery of training and technical assistance to hundreds of law enforcement agencies across the nation. John also supports the national and public safety in partnership for violence reduction, crime analysis efforts, predictive analytics, as well as the national technology standards development under BJA's purview. John holds a bachelor's degree in Sociology and in Criminal Justice from Northern Illinois University, and also a Master's in Criminal Justice from the University of Illinois at Chicago.

Kumar Kibble, our second panelist, is a Certified Leadership Coach and Chief Executive Officer for GuideQuest. He specializes in coaching leaders within mission driven organizations. Kumar brings 30 years of experience in leading teams as a military officer, a special agent, a diplomat, and a government and corporate executive. As a former U.S. Department of Homeland Security Deputy Assistant Secretary, Kumar served as a Chief Operating Officer for Homeland Security's largest criminal investigator agency. He also received the Presidential Rank Award for his management of a six-billion-dollar budget and leadership of a global workforce consisting of 20,000 employees in 48 countries. Kumar is a former army ranger serving in leadership positions in the 82nd Airborne, as well as a graduate of West Point. And he also has a Master's Degree from Johns Hopkins.

And our third panelist today, Dr. Cary Coglianese, is an Edward B. Shils Professor of Law and Political Science Director for the University of Pennsylvania. He has a JD from the University of Michigan and also a PhD in Political Science from the University of Michigan. He has also served as a research fellow for Harvard University. Cary specializes in the study of administrative law and regulatory processes, with an emphasis on empirical evaluation of alternative processes and strategies and the role of public perception of technology, as well as business and government relations in policymaking. He has been extensively published on these topics, including the use of artificial intelligence in government agencies, as well as transparency in federal rulemaking.

So suffice to say, we have some real experts on the panel. And without further ado, I just really want to jump right into the questions and thank the panelists for volunteering to be with us today.

John, I'll throw the first question out to you, if that's okay. Body-worn and dashboard cameras have become more commonplace in law enforcement. There's often a great deal of public pressure that the media release footage of an incident soon after it happens. From your perspective, and from the perspective of the work that you've done with BJA, can you discuss some policy best practices you've seen to help guide responsible decision-making around the public release of video from law enforcement encounters?

And then maybe while you're at it, can you also talk about how the technology itself is evolving to help agencies more efficiently capture, or search and redact, as well as share digital evidence. It's a mouthful, but I think you're well-qualified to address it.

I think you're on mute, John. No, we can't hear you. No, we don't have you. Okay. So, let's, let's do this, I'm going to switch up the questions. So then let me go to Cary.

Cary, a number of law enforcement agencies are increasing the use of artificial intelligence and machine learning to further their missions. And we're seeing that in federal law enforcement organizations, state, and local law enforcement organizations, as well as other government agencies at large. Can you talk a little bit about some of the use cases that you've seen, for AI and ML, as well as the policy and regulatory challenges? As well as the opportunities around these technologies? And from your perspective, are there effective strategies to help convince the skeptics of the benefits of employing these technologies since, you know, the benefits versus the risks that they potentially pose?

CARY COGLIANESE: I'm pleased to be here and happy to talk about artificial intelligence and how it's been used in the law enforcement context. I think the uses throughout the criminal justice system fall into three main categories. The first would be in allocating law enforcement resources, the second would be in actually helping to detect potential criminal activity, and the third would be in the actual process of sentencing those who've been convicted of crime.

And I can talk a little bit about each of those in brief, happy to expand on any of them, but let me just take the first, which is the allocation of resources. This is a challenge with law enforcement at any level, in any context. There's more possible sources of legal violations to detect than there are inspectors or police officers to detect that noncompliance with the law. So, there's always a resource allocation challenge, and artificial intelligence tools, machine learning algorithms, are increasingly being used to make those allocation decisions that can occur at the local level, where local police departments are money balling and using analytic techniques to determine where to send police patrols on any given day. Basically, trying to forecast areas that might be of greater likelihood of having crimes and addressing those by sending more patrols there. Those data can be based upon past complaints, it could be based upon other kinds of data that are available to the law enforcement authorities.

And this is also being used by regulatory agencies, the federal agencies, such as the Securities and Exchange Commission and the Internal Revenue Service, faced the same kind of resource allocation problem. There are so many possible sources where there might be fraud in securities markets or on tax forms, and so these authorities will use artificial intelligence tools to determine which filings to look at for further review.

It’s important to note that in this context, artificial intelligence is not substituting for human judgment. At least it's not substitute for human judgment in the determination of any legal violation, but it is helping direct where humans should go. So that's the first use.

The second use would be in detection. And here, most prominently with the greatest degree of public concern, I think, is the use of artificial intelligence and machine learning algorithms in technology that we refer to as facial recognition technology.

This is, in some ways, a straight straightforward application of machine learning tools, which are really powerful in many contexts, for pattern recognition. And these tools are now capable of helping to detect people who might be, for example, wanted by law enforcement or suspected of committing a crime. But there's been a tremendous, I think, amount of public backlash to facial recognition technology. Over half a dozen states and probably about two dozen or more cities around the country have banned or placed significant limitations on law enforcement use of facial recognition technology.

There are two major concerns that arise with this. One is what we might think of as a big brother watching us concern, and the second is with racial bias, as these, the algorithms, do a better job of recognizing patterns because of the way that they've been designed, and probably more importantly, even the data on which they've been trained, they do a better job of facial recognition on some individuals, some races they are less accurate, at present, in recognizing faces of people of color. So that's generated some really significant and important public concerns, and it's so far a backlash.

The third area in criminal justice is in the sentencing process. And here too there's been a considerable amount of backlash. Many states have adopted risk assessment scoring systems. These algorithms tend to be very straight forward at first generation. They're not even what we would think of as complex or advanced forms of artificial intelligence, but they're used to try to come up with a score of how likely someone who has been convicted of a crime is to recidivate.

And there's a great deal of concern about racial bias in the use of these risk assessment algorithms. In all of these contexts, you know, there's both potential advantages for law enforcement, but there's potential risks too, or risks of error, and that consequences for the public are really quite high. So, I think that you asked about best practices. I think these tools have to be really carefully deployed and designed and validated before they're put into use. They need to be tested, piloted. Maybe used in conjunction with human decision-makers to validate that they work at least as well as humans, and that efforts have to be made to involve the public. To make the workings of these algorithmic tools transparent to the public and to really build confidence and public trust in these kinds of technologies.

There's other kinds of technologies that are used in the law enforcement and criminal justice context that have won a good bit of public trust and confidence of the legal system. I'm thinking here of DNA technology, breathalyzers, drug testing, even certain kinds of speed detection used for traffic enforcement.

But you know, there's a tremendous amount of algorithmic aversion, and particularly when the consequences to members of the public are as high as they are in the law enforcement context, where there's criminal penalties, potentially, and loss of freedom at stake, the governments need to be at their utmost of caution and concern and care in deploying these technologies.

I think if anybody is listening to this, if you'd take one thing away from this, I would say don't just go to the lowest bidder when you're putting out a contract for these, and don't just sort of think that the contractor will do all the hard work for you. You really need to be aware of how your purchasing or your deployment of these tools is conducted and how well validated it's being used. And you need to make sure that you can involve the public along the way.

JIM CHAPARRO: Thanks. That was really insightful. And I think the one thing you said that really caught my attention was to gain the trust of the public, to be as transparent as possible with the technologies. Obviously, law enforcement organizations don't want to give away, you know, all of the secrets on how their algorithms work and with some of the technologies. But I think allowing the public to participate in those discussions and really understand how the technologies work and what the strengths and limitations are goes a long way towards providing some credibility. So, it's a really good insight.

Let me check with John. Do we, do we have your audio back?

JOHN MARKOVIC: Can you hear me now?

JIM CHAPARRO: Absolutely. So, would you like me to rephrase the question for you or you think you got it?

JOHN MARKOVIC: Sure. I'll go ahead. So, the first question, I think, is I discuss some of the policy best practices that I've seen that are responsible for good decision-making around the public release of video from law enforcement in powers. And it's probably fortunate that Cary actually went first. I think there's some answers that he provided that are very relevant, particularly just keeping the public informed and working with the public.

So, I can definitely say there are no simple answers and it really depends on context. So, one of the background things, I think the fundamental element, is to understand what's happening across the state. So, the release of body-worn camera footage is often dictated by state legislation. And that's something that's been happening more and more over the last three or four years.

Increasingly, states are mandating the use of body-worn cameras. I know New Jersey and Illinois and Delaware were states that moved towards mandating, and many states beyond those that have mandated body-worn cameras have developed prescriptive legislation related to retention of body-worn camera, and more relevant to the question, the release of body-worn camera footage.

So, needless to say perhaps, now agencies should perform or proceed in accordance with what their state laws are. So, in essence, there are basically, roughly speaking, two types of states. Right? Some states treat body-worn camera footage as a public record, what are called open records state, and some treat it as evidence.

On the open records side, we see California and New York that require the release of police videos that involve critical incidents in most cases. Others, the closed records states, I guess it might be the term of art, require court orders before a body-worn camera footage is released.

So California is an open record state, and then beginning in about 2009, they required that all police departments in the state be equipped with body-worn cameras and that they also had to release critical incident body-worn camera recordings within 45 days of the recorded incident. And those basically are incidents that involve use of force, use of deadly force I should say. And use of deadly force, meaning that it's some type of force that has the potential to result in death or serious bodily injury. The definitions vary in legal context and by state. But it's basically serious use of force incidents. On the other hand, North Carolina is a state where a court order is necessary before the release of footage.

There was an incident back in April where the Pasquotank County, I'm not sure if I'm pronouncing that correctly, a county Sheriff's Deputy had served a warrant in Elizabeth City that resulted in an officer

involved shooting, and the D.A. was very clear that the body-worn camera is not a public record and can't be released to the press or the public without a court order. So, we see states sort of fall in line there, and many states are changing their legislation.

There's a great site, the National Conference of State Legislatures, that has a website that tracks body-worn camera law, as well as other legislation responses to policing that you might want to Google if you're interested. But as a Chief, you know, it behooves you to know what the law is in your state. So, within that broad framework of the state laws, the local agency, the police chief has some discretion and leeway in how they decide when to release and how they release body-worn camera footage.

I think one of the go-to people that we've relied on in our body-worn camera program is a woman by the name of Laura McElroy. She's a former journalist who was then Communications Director for the Tampa Police Department. And she does consulting now. She recently presented at our national body-worn camera meeting and she outlined about 70 elements. So, one is you need to realize that the public nowadays expect to see a video, right? People have their cell phone videos. Videos may be recorded incidentally on nearby CCTV systems. And her recommendation is to act quickly to prevent a false narrative. Obviously, in accordance with the state legislatures. Sensitivity though is key. It's advisable to offer the family the first viewing, because sometimes the information about this subject may be sensitive or embarrassing. It's important to keep in contact with community leaders to share information and build support.

Before I came to the Bureau of Justice Assistance, I was with the COPS office, the Office of Community Oriented Policing Services. And there was a mantra that a lot of community policing executives use, you know, "to build those relationships with your community, that's money in the bank." So, when something does go wrong, you've built that trust with the community, and they're willing to give you a break. Easier said than done, but it's key.

I think the other things that you mentioned were to be consistent in releasing video. So, don't be willy-nilly in your policy. Have a policy that's clear and execute it consistently. You know, obviously making adjustments for the particular circumstance. Once you do that, you should monitor social media to see what impacts you're having.

And I think fundamentally, the overarching thing is to establish your agency as the source of information. The credible source of information. So, one of the great examples that is coming to the floor initiated by the Los Angeles Police Department is, they've developed critical incident community briefings for all critical incidents, use of force incidents, which are viewable on the web. I think they have a YouTube site. And these are very, very well documented, well produced narratives of body-worn camera where they show not just the footage of the body-worn camera, but the footage of all the officers that might've been involved in the incident. Oftentimes here, there are multiple officers responding when there's an incident with use of force.

But they also generally will play the dispatch call to really give context. And somebody from their public relations unit, usually it's one officer, provides the context, provides the appropriate caveat. They're very well done. And there's a couple of departments, I think now, that have followed suit very closely, yeah, Los Angeles County Sheriff's office; the Austin, Texas; Mesquite, Texas; Santa Maria, California; Norman, Oklahoma; Mesa, Arizona have all sort of copied or adapted that model. And it's great. I think it provides things in context. I recommend people watch those if they get a chance.

So, kind of shifting to the second question with respect to how this technology's evolving to keep agencies up to date to more efficiently capture, store, search, redact, and share digital footage. I think

Jim's initial caveat about the technology outpacing the abilities of agencies, I think is something to keep in mind here. With respect to point of capture, the goal of the body-worn camera program is to have those body-worn cameras activated consistent with policy.

So generally, you know, they vary from department to department, but basically it boils down to anytime that the officer has contact with the public. So, it could be a field stop, it could be an arrest, it could be a traffic stop, it could be a casual encounter. So, much of the compliance then relies on training, to ensure compliance. But increasingly I think there's technology that will help. In a lot of stressful incidents where the officer may be distracted or inhibited from hitting that button and turning on the camera, vendors are increasingly providing features that start cameras automatically. Sometimes they start it automatically, remotely. Some are tied to the weapon draw out, or the taser draw. Some are tied to lights and sirens. Some are tied to accelerometers, so when an officer might start to engage in chase, they'll turn on automatically. That said, those bells and whistles are expensive. They cost extra, not every department can afford those and maybe not every department needs those, right?

Some departments are more tranquil and others they don't have a lot of chases. They don't have a lot of officer involved shootings. Most of their incidents are routine. So, we do see some innovation there, just some simple things like the dispatcher notifying routinely when they place a dispatch, remember to turn on your body-worn cameras. And oftentimes they're turned on in route to a call when there's a call for service.

The other thing that I think we're struggling with, a lot of our grantees are struggling with, even the large ones, is just integrating all the digital evidence media, from in dash cameras, for body-worn cameras, from CCTV, from Ring or Nest doorbell cameras. A lot of departments are supporting it, it is just generating tons and tons of video. And it's really, really difficult to keep a pace with that video, to manage it. To leverage the evidentiary value of that video, and thus leverage other values of that video. We're just starting to understand the metrics and we think that about 5% of video gets used. About 5% for evidence, a small percent gets used for routine, sort of, overview.

A lot of departments have policies that mandate sort of a random viewing of body-worn cameras by officers of officers, just to ensure compliance, sort of an early warning system, always balanced against the union's interest in making sure that these supervisors aren't going on fishing expeditions. So, it's a generally random and very tightly controlled.

But there are also other things that agencies are looking at to leverage that video, some in very inventive ways. We just had our national meeting of grantees. We had a great presentation by some detectives from Rochester, New York. And one of the detectives will do the body-worn, if there's a suspect in a case, he will view the body-worn camera video and that video of anything you can get for the video, of anything you can get his hands on related to that subject.

Now Rochester doesn't have a sophisticated digital evidence integration platform. They're storing their video on their server, which is becoming more and more rare. But I have an incident number, I have a defender number, this detective, or the analysts that support him, can do a search of the various videos. And the detective just gives those videos for evidentiary value to see if there's something about the behavior of that individual on prior arrest. You know, information about other people who were in these previous videos that might be witnesses that might be able to tell the detective something about the suspect. Obviously, he does this not in all cases, but pretty much in more serious cases.

JIM CHAPARRO: It's complicated. Right? As you said, it's not just the technology itself, it's the policies around that and the training that's associated with it. And then you layer on top of that the expenses associated with the technologies. It's a lot of the important decisions, I think, for law enforcement organizations to make when thinking about implementing.

So then that kind of leads me to you, Kumar. We've talked a little bit about some of the policies associated with implementing advanced technologies, AI, machine learning. We've talked a little bit about some of the issues around training for body-worn cameras and different policies and best practices, but at the end of the day, it's going to be officers who are using these technologies and implementing them. And successfully adapting new technologies requires changed management.

As a former law enforcement executive, I think you know firsthand how hard it can be to manage change in a law enforcement community. Can you tell us a little bit from your perspective, and your experience frankly, about strategies and practices that you think can help individuals and organizations manage change successfully? And what are the human factors required for successful implementations of technology in a law enforcement field?

KUMAR KIBBLE: Yeah, sure Jim. And I actually come at this not just from a perspective as a law enforcement executive, but also, you know, a sales executive trying to introduce technology into the department of Homeland Security at one point. And then also now, currently as an executive and change management coach.

I think that there are three key principles that you have to hold in mind in one hand, while at the same time applying a change management framework. The first is that, as we've talked about, the pace of technological innovation moves faster than the legal and policy frameworks can. And so therefore it's essential to kind of be disciplined about developing use cases, business cases, and common process templates for implementing these technologies. And to do that, you have to identify stakeholder needs and get buy in. Obviously not just external, but also internal.

You know, what comes to mind as we've been talking about body cameras, I was interviewing a Police Chief recently and he was tasked with introducing body cams into his police department. And he started with traffic because there was already some comfort with dashboard cameras. But then he also saw this as an opportunity for them to defend themselves against false allegations. And then once he got a small win there, he did kind of a land and expand approach and broadened it throughout the department with his traffic division as ambassadors for the body camera adoption, based on the small wins they were getting in terms of being able to defeat false allegations. So, identifying stakeholder needs and buying and building some support behind that is critical.

I think another really important piece that we've been talking about is integrating security, privacy, and civil rights protections into these common business processes. You know, our guidelines remaining consistent, legal precedent is often lacking and the public's expectations are shaped by TV shows and advertising and it can really affect what their expectations are versus, you know, what the technology is actually delivering. I felt this in a really direct way in the sense that, and actually, let me just skip to the third point. We've got to educate the public on how these technologies work or they don't work, in the real world. And so, let me kind of wrap this together in in like a concrete example.

A couple of years ago during the last mass migration challenge, I was tasked with trying to bring rapid DNA into the border response along the Southwest border because there were challenges with fraudulent family units and potential human trafficking issues. And so, there was a big opportunity there to introduce a new technology. However, you know, while the department had been working on a

framework for adoption of rapid DNA, we were now talking about rapidly accelerating its deployment before the policies were fully mature and before all of the buy-in had occurred.

And yet there was this tremendous opportunity to have an immediate impact on uncovering human trafficking, which was done, and in identifying significant numbers of fraudulent claims in terms of family units because that's how they were defeating the border security policies at the time. Probably some of the biggest obstacles were the fallacies regarding what was going on with the DNA testing. There are a lot of, and Jim, you're familiar with it in your background, but you know, border security, homeland security we've seen in the recent years, always a lot of controversy associated with it. There were a lot of stakeholders, advocacy groups, other agencies, state and local partners, and there were concerns about, "okay, is this rapid DNA, or is this the same as ancestry DNA? Are they able to get my whole medical profile?"

And in fact, what we were doing is, to the point I think Cary had made earlier, we're really leveraging very well-vetted, traditional STR DNA identifications that are nothing more than a hyper-accurate fingerprint. And yet that messaging was hard to keep, we had to hit it again and again and again with one stakeholder after another, because of the TV shows and other things that are out there in the atmosphere that affect and influence what external stakeholders, and particularly in this case, particularly advocacy groups, might be concerned about.

So, those are three principles I think that really have to be, the business processes and use cases, making sure those are down. Protecting system security, privacy, and civil rights protections. Those have to be in place to assure to build that trust with the public. And then finally that public education piece.

Now, in that example I've actually also been seeding some key things I think to keep in mind from a change manager perspective. Opportunities, you know, there is opportunity in every crisis, and so, for the organization that's seeking to adopt that technology, it's really important to create a sense of urgency around that opportunity, around that crisis.

And this comes from John Kotter, he's a change management guru that's done a lot of work in change management. His most recent book is *Accelerate,* and he talks about some of these eight accelerators. I think there's three that we could keep in mind here. There's that creating a sense of urgency. There's building and maintaining a guiding coalition of all the vested stakeholders that need to be a part of that, so that you can identify concerns and resolve them and manage them. And then finally, the other one I would highlight just is this idea of celebrating visible, significant short-term wins. Not just for the external stakeholders, but as I just shared in the example of that one police department, for the internal stakeholders as well.

JIM CHAPARRO: Thanks.

CARY COGLIANESE: Can I just add something, Jim, to that?

JIM CHAPARRO: Please.

CARY COGLIANESE: You know I just think what Kumar has said, and it builds on what John was saying too, even though this is a panel session about technology in law enforcement, it's not just about technology, you know?

JIM CHAPARRO: Right.

CARY COGLIANESE: It's about how the organizations are interfacing with the technology. How that organizational interface then is interacting with the broader public. This is a people enterprise, as much as it is a technology enterprise.

JIM CHAPARRO: Yeah. You took the words right out of my mouth. You know, the technologies themselves are phenomenal and offer all sorts of benefits for law enforcement organizations, but if you don't take those other factors into account, engaging with the public, scoping the use of the technologies appropriately, making sure that you're vesting change management processes, putting a good policy and training framework around those technologies. You can have the best technology in the world, and if you're not doing those things appropriately it's going to be an expensive failure. So, I think that, go ahead Kumar. Do you want to say something?

KUMAR KIBBLE: Yeah, I was just going to add, you know, I think, often vendors, and again that's one hat I wore at one point, get very excited about their technology in a vacuum. And that's where they miss. In fact if they want to be more effective in introducing that technology into an organization that could use it, that can enhance their mission, they really need to think also about the existing business processes in cases, because they exist for a reason in that bureaucracy. They bake in oversight. They bake in stakeholder support. They reconcile many competing interests. And so, you know, much more successful strategies that figure out how to weave that new capability into the existing enterprise. To maintain that trust that you were talking about.

JOHN MARKOVIC: I have two things that have to do with what Cary and Kumar said, I think one is, policy is key. One of the elements of our body-worn camera program is that a policy has to be established, it has to be deliberate, it has to be comprehensive before we release the bulk of the funds to the agency to purchase cameras. And that policy should be done in consultation with other stakeholders. Stakeholders within the organization the rank in file to the executive, the unions if they have a role with other criminal justice stakeholders, but also with the community. So, a lot of our practice and a lot of people doing best practices are out there in the community discussing what their body-worn camera policy will entail.

And then, continually updating the public on what their body-worn camera policy is. And those are very much embedded in the critical list and reviews that I alluded to before. And I think the other thing that's interesting is like for the ethical and constitutional policing angle, you know, even the body-worn camera vendors are a little wary of it.

Talking about the topic Cary spoke about is facial recognition. They're holding back on that. The technology is advancing pretty quickly, but they recognize that it kind of turns the tide. Right now, the public generally embraces body-worn cameras. Officers have basically embraced body-worn cameras because they know, they found that it probably exonerates them more often than it implicates them.

It lays bare some of the frivolous complaints, or sometimes complaints that somebody just thought they were mistreated because they were in a stressful situation. When they review the camera video they say, you know something, I wasn't treated that badly. We see, we hear stories of that over and over again. But I think, you know, if body-worn cameras become perceived as a surveillance tool, I think that lifts the equation, and the public at least would become less receptive to them.

So, it's both the practical and the ethical consideration I think, that we're holding back on facial recognition in body-worn cameras. And I think it's because it's worthwhile to maintain that trust.

CARY COGLIANESE: Yeah, and I think what's been a little bit unfortunate, if I could just add a little, is that we've kind of moved a little bit too quickly on some fronts, like with facial recognition software. Too early, where we skipped some steps about really validating it, really vetting it, really building public trust and confidence in the education that Kumar was talking about, before we've introduced it.

And to Kumar's point about how vendors do very well if they would not only worry about the technology, but also the organizational context and not only to think about themselves as technology consultants, but also in some sense management consultants. I've seen far too often in the space of AI tools, that vendors are very protective and they want to claim proprietary coverage of all things related to their algorithm.

I recently published a paper called "Contracting for Algorithmic Accountability" in which I try to speak to public agencies who are contemplating contracts in this space to vendors, making sure that at a very minimum, if you're not working with one of the more enlightened vendors that Kumar would advise you to work with, at least make sure that your contracts anticipate the kind of disclosure of information that you will need to have the vendor release in order to make sure that you can build public trust and confidence.

And you can do that without really disclosing things that would be otherwise protected as law enforcement, you know, or security related. You can talk about what's the objective, how has it been validated? What's the peer review that's been given to it? These are all things that can be disclosed without actually giving away, in some sense, you know, the underlying logic that could enable people to evade or gain the detection system.

JIM CHAPARRO: Yeah, that is 100% correct and I think it really kind of puts icing on the cake in terms of how to successfully implement the technologies. And, you know, sometimes contracting is an afterthought. And you know, a requirement comes from a program and they say, we want to put out an RFP for something like this and maybe not even understand, because the technologies are so new, things that you should be thinking about. So, thanks for that.

We only have about 10 minutes left and I promised the audience that we would have time to entertain some questions and Sasha let me know that we had a couple of questions that have come in. So, we'll just do a speed round of those. Sasha, you want to start please?

SASHA O'CONNELL: You bet. Can you hear me okay?

JIM CHAPARRO: Yeah.

SASHA O'CONNELL: Great. So actually, the first question, and Cary, it's the perfect follow on to your last point, our attendee was asking about, you had talked about bias in the training data of AI, and they were actually asking for your thoughts on bias in those algorithms you were just talking about in terms of transparency. Can you talk about maybe best practices or ways to, again, protect against that bias in those algorithms themselves, as well as the training data piece that you already talked about?

CARY COGLIANESE: Well, sure. I mean, I think, you know, we have, in some sense with AI a blessing and a curse associated when it comes to bias in existing data. The blessing is that you have a tool that in principle can be unbiased, or at least adjusted more easily than humans.

The reason why often you're seeing bias in a lot of AI tools is because the data that are being used are drawn from human-based systems that have bias built into them from our implicit, or sometimes explicit bias, you know, we have a history of racism and we can't deny that. And those data that have been collected and that algorithms train upon have that human bias built in.

Now, what's the blessing again is that we can understand that because we're using data, we can statistically detect this in a way that historically we just haven't had with humans making decisions. We haven't often really been able to perceive or detect that kind of bias in the system.

The curse of course though, is that, you know, these tools depend upon data. So, you've got to get it from somewhere. I think the best practices are, one, is to make sure you are fully analyzing and taking account of those biases. I think too often all of us get into kind of a kind of tunnel vision. We have a purpose that we want our technology or our artificial intelligence system to serve. So, we fixate on that and we overlook the side effects. We overlook the concerns about bias, but you've got to be aware of it. You've got to vet that data and have come out with it. And then you can mathematically adjust for it. I mean, there may be some trade-offs at times between fairness or equity or adjustment of bias and accuracy, but, you know, there's a value for dealing with that.

So, I would, you know, urge you A., to be mindful of it and B., then look for tools that can solve it. And in principle at least, with our artificial intelligence, it's going to be easier to address those sources of bias ultimately than trying to train a workforce of say, thousands of human beings who have their own biases that are very hard to really fully get rid of.

JIM CHAPARRO: Thanks, Cary. Sasha, I think we probably have time for one more quick question.

SASHA O'CONNELL: Okay, one more quick question. Specifically for John, but others maybe have a thought on this as well. Somebody asked about cell phone camera videos and how that fits in. Both from a change management perspective, a regulatory perspective, and John sort of, they asked also specifically about in the two different kinds of states, right? This sort of open state versus the evidentiary state. Maybe if folks can spend a minute, I know it's a hot topic of interest talking about those cell phones, personal bystander cell phone videos.

JOHN MARKOVIC: Yeah. Well, I think that's a big part of the digital evidence integration and management equation. So, law enforcement are getting tips from cell phone cameras. I don't know the legal ins and outs of those, but I would imagine that it probably has the same cautions in terms of treating that as evidence. And probably since it's generated from outside the police department, I'm not sure what the implications are for open records.

It may fall back to the individual who provided it, it may become the property of the police department, in which case it would be subject to open records laws, but that's certainly a big part of the equation. So, what we're moving towards, hopefully, is these integrated systems that can store all that information in a repository along with still photos, with license plate reader data, and make that query-able so, you know, you can do investigations.

You can look for evidence in particular cases. Like I said, what the detective in Rochester did, could be done more efficiently in an automated sense. But I think as we say that, we have to keep all these cards, we don't want it to be fishing expeditions turn into surveillance because that can quickly come to floor, so that's where your policies are important. Your compliance mechanisms, your tracking mechanisms and so forth.

But I don't know the particular law on cell phone cameras generated from citizens or confiscated from citizens in terms of whether those are public records or, are considered evidence. I'm guessing that, you know, they're treated pretty much the same as the body-worn camera footage, but I'm not real certain about that. I'm not a lawyer, so.

JIM CHAPARRO: Very, very complicated set of issues. I have to say, unfortunately that is all of the time that we have for today's session. So, for the panelists, I want to say first and foremost, thank you so much for sharing your insights with our audience today. We did not have time to get to all of the audience questions.

So, for those of you in the audience, just be aware that, we're working with the panelists after this to produce a podcast out of this session and we will incorporate some of your additional questions into the podcast. So, I would say, keep your eyes and ears open for that and other speaker series events on the Guidehouse National Security LinkedIn page. And you can find news about that if you want to like us or follow us there.

I would also like to very much thank the American University for helping to organize not just this session, but for all the series of insightful sessions and podcasts that we've, brought over the last few years, as well as additional ones coming up in the near future.

So with that, I will say thank you to the panelists once again, and thank you to the audience for listening in and please listen in for the podcast as we kind of dive into some of these issues a little deeper. Thanks.