Mission is Possible

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

SASHA: Hello, I'm Sasha O'Connell and I am thrilled to welcome you to Mission is Possible—a series of audio episodes where we break down and dig into management issues of particular relevance to the national security community. This is a joint project between Guidehouse and the School of Public Affairs at American University. We are pleased to have you join us.

On today's episode, we are going to discuss the challenges associated with IT implementation, specifically within law enforcement agencies. To address this topic, in late June we hosted a panel with experts in the field, which Jim Chaparro, a Partner in the National Security Segment of Guidehouse, moderated. Additionally, I had a chance to interview some folks as a follow-on to the event as well. What follows is some of the highlights from those deeply enlightening conversations. I hope you enjoy. Jim, over to you to kick this off!

JIM: Thank you, Sasha. The field of law enforcement is rapidly evolving. The advance in technologies, such as facial recognition, artificial intelligence, big data analytics, body cameras, and many, many others, are really changing the landscape of law enforcement. As is often the case, the technology often outpaces our ability to keep up with it from a policy perspective.

With us for our panel was John Markovic. John is a Senior Policy Advisor at the Bureau of Justice Assistance at the United States Department of Justice. He is focused on body worn cameras, amongst many other things. John talked at length about his perspective on some of the key challenges of technology integration in law enforcement agencies. So, let's listen in.

JOHN: 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 states. 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, agencies should perform or proceed in accordance with what their state laws are. So, in essence there are basically, you know, roughly speaking, two types of states. Some states treat body-worn camera footage as a public record, what are called open records state, and some treat it as evidence.

So, within that broad framework of the state laws, the local agency, the police chief has some discretion and leeway in how they release, decide when to release, and how they release body-worn camera footage.

JIM: Thanks John, that is so helpful for context. Within that framework, are there best practices for implementation, specifically in the area of body worn cameras?

JOHN: 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, 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.

The other things 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. 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

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 dash cameras, from body-worn cameras, from CCTV, from Ring or Nest doorbell cameras.

A lot of departments are supporting, 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 then 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 in lines and early warning system. Always balanced against maybe the union's interest in making sure that these supervisors aren't going on fishing expeditions. So, it's generally random and very tightly controlled.

JIM: 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 important decisions, I think, for law enforcement organizations to make when thinking about implementing.

With that, I am going to hand this back to Sasha to pick up the conversation with our other panelists.

SASHA: Perfect, thank you. Kumar, can you just tell us a little bit about your background and what you're doing now?

KUMAR: Sure. I retired from homeland security after 30 years of government service a couple of years ago. And then I went to work as a Vice President of Sales at a tech startup for a couple of years. And I am now a principal at a leadership coaching company that I founded, called GuideQuest.

SASHA: Close to Guidehouse, related, cousins of Guidehouse, GuideQuest (laughs). Well, it's wonderful to have you and thank you again for joining the panel and for joining us for this Mission is Possible episode focused on "Cautionary Tales: How Technology Implementation is Impacting the Law Enforcement Landscape." I had the opportunity to just hear you on our panel and some of that will be included in the podcast, but for our listeners who didn't get a chance, I thought it was just so interesting the way you laid out sort of three key points that law enforcement agencies should be thinking about when it comes to technology implementation. Could you just summarize those again for our listeners?

KUMAR: Sure, I mean, one is to ensure that they develop use cases and common process templates for implementing new technologies. That actually comes from a RAND study. That was a report that was done in 2018. As they identified criminal justice technologies being adopted by law enforcement organizations. The second point was integrating security, privacy, and civil rights protections into that common business process. Then the third was, and I think it's a really critical piece, educating the public on how these technologies work and what they don't do as well, what the limitations are in the real world.

SASHA: Thank you, and as we talked on the panel, you talked too about how it really comes down to change management and the people piece and the integration into existing processes. In that vein, can you talk about from your experience, leading law enforcement agencies, which of those three things are maybe the hardest given the people and existing processes? Kind of where do you think there may be some low hanging fruit, places that people could start?

KUMAR: I think it begins with, I referenced this during the panel discussion, but John Kotter is a change management guru who has published on this extensively, and he talks about the importance of creating a sense of urgency around a single big opportunity. So, I think the challenge there is recognizing that opportunity. That would be the coaching question I would give to organizations, "What's your big opportunity?" To leverage technology, to affect it? To make life easier, not just for your internal staff, but to promote your public safety mission? What is your big opportunity?

And that's so important because you need something galvanizing to overcome the inertia of bureaucracy. And then when you do that, when you find that opportunity, you need a multi-disciplined coalition that can help to shepherd and steward and carry that over the goal line because inevitably there will be resistance, there will be roadblocks, there will be all kinds of setbacks. It's really important that you have a coalition that can then drive that forward and again, it's important to emphasize this, and I remember reading this, I had read this book by Robert Gates "Passion for leadership," I think it was you called. He drove change at DOD, at CIA, at the University of Texas, and he talked about the importance of putting together these task forces that are composed of representatives

from all of the interested stakeholders. That's hugely important so that you can have an effective guiding coalition.

SASHA: That's amazing, as a recovering strategic planner for the federal government, I relate to that guidance very well. We sort of would call it a "burning platform," right? Like what's the burning platform for change, as you're saying, and then how do you get all the right stakeholders?

Do you think when it comes to technology implementation, is it hard for folks to kind of translate? Is it because there are technical folks involved who maybe aren't on the mission-side on a day to day basis? Is that, sort of those steps, more challenging when it comes to technology implementation or is it the same challenge kind of for any change management, in these organizations?

KUMAR: I think the complexity comes in the dimension having to do with security, privacy, and civil rights protections. Because technology in a very powerful way can have a huge impact on that, depending on how it's channeled and how it's managed. But to the more fundamental, I think, point, you know, I'm thinking here now for example, of the innovation lab that exists at Homeland Security Investigations. They bring technologists together with operators, so that they can be more responsive to the needs in the field. And so, I think to the extent again you can break down the walls and you can have the people that are developing the technology sitting alongside the people that are going to use it. I think that's important in terms of refining that capability so it's useful, but then I think you got to add another layer to that. You've got to make sure you've got the civil rights aspect of it covered, the privacy aspect of it covered, and that's a little bit of what we did when we were doing rapid DNA with HSI a year and a half ago or so, was trying to make sure you had the right people paying attention and having discussions around how to shape this, frankly, into what was a new business process because it didn't really exist.

SASHA: You mentioned the rapid DNA deployment example. Can you talk a little bit more about how that went and maybe lessons learned from that?

KUMAR: Yeah, sure. So, with the last mass migration challenge we had at the border with the folks emanating, the caravans emanating out of the northern triangle heading to our southwest border. It was overwhelming our human resources at the border. It was overwhelming our entire infrastructure in terms of detention capacity, transportation, all of those kinds of things. And there was a great concern around people being exploited. Children being exploited in particular, because one of the ways that the smugglers, the coyotes, would market their services down at Central America through Mexico was that if you arrive as a family unit, the border authorities will release you into the interior of the US. And so, there was a huge premium on identifying fraudulent family units and child rentals schemes that existed, child purchase schemes, human trafficking, all those kinds of things. When we ultimately did a pilot deployment, we identified a 50-some old man that had purchased a six-month-old child for like $80 dollars, I don't remember what the, it was ridiculous. But anyway, that's the background the context of the challenge.

So that created an opportunity. It was a big opportunity for HSI. They wanted to do more with rapid-DNA, adding DNA as a capability into their investigative tools. And it was also a big opportunity for the company that I represented in the sense of introducing rapid DNA into the Department of Homeland Security beyond just a testing kind of sandbox, kind of approach, that maybe they had been pursuing with S&T, Science and Technology Directorate.

So, that really did create a rapid opportunity to come together and in very short order, design a pilot, but that nevertheless we had to be mindful of how we were managing civil rights and privacy with DNA samples, with swabs. Whether they be immediately be disposed or the chain of custody on that. All these different things that you need to think about when you're putting together a program like that. How it would be collected. There were all these factors.

But ultimately, we partnered with HSI as a vendor. We partnered with HIS, who was also in discussions that we weren't a part of with DHS civil rights and civil liberties and with the privacy office and with CBP, because CBP was hosting this ICE function in their facilities. So, there's a whole bunch of coordination that needed to come together and a big part of that too was, again, the public education piece. And really kind of identifying and calling out what had been designed into the technology to protect privacy, to destroy the sample. You know, all of these different things that had been kind of designed upfront into the technology to address some of these concerns.

SASHA: Such a cool, like specific mission-focused example, of really neat and important technology. Well thank you so much Kumar, it's been our honor and pleasure to have you. Before we let you go, is there anything I should've asked you that you think is really important for our listeners to know about tech implementation, specifically in law enforcement agencies?

KUMAR: I would just foot stop again this idea of the stakeholder engagement, internal and external. We do pay a lot of attention to the external stakeholder engagement. I do think it's also critically important to ensure you build the case for it internally as well.

Thank you for the opportunity to share some thoughts with you today.

SASHA: Thanks so much for joining us.

Next, it is my privilege to welcome Professor Cary Coglianese. Cary, could you please introduce yourself for our audience?

CARY: I'm Cary Coglianese. I'm on the faculty at the University of Pennsylvania Law School, where I also direct the Penn Program on Regulation. I've been working in the area of regulatory law and public policy for the last 25 plus years, initially at the Harvard Kennedy School of Government and now at the University of Pennsylvania Law School.

SASHA: Awesome, thank you so much for joining us. And for our podcast listeners, I'm hoping, you know, you lay it out really clearly, kind of three specific ways or uses or use cases for technology for law enforcement today. Could you go back through that summary for our listeners?

CARY: Sure, I think there is a need for, and a potential benefit for technology in three main areas. The first is in resource allocation. Law enforcement is inherently outnumbered. There's many more possible sources and sights and individuals in potential violation of the law then there are people in law enforcement or regulatory inspectorates to actually identify all of those violations. So you have to think about how wisely you're using your resources. Are you just sending people willy-nilly, or are you really targeting the most likely or the most significant potential sources of violations of the law? So, we

see cities, states, and the federal government using artificial intelligence tools now to make better choices about allocating resources.

The second area that AI is being used is as part of a larger component of other technologies for detecting violations. This can be used in a form of natural language processing, for example, to be able to identify patterns of people or other information, extracting it from large amounts of text or audio, social media. This is all now often being analyzed through tools that draw on artificial intelligence or machine learning algorithms. But also, I think most controversially, pattern recognition occurs in the area of facial recognition. Which is certainly an understandable area where law enforcement might be able to use technology to process the many of hours of video that are recorded, whether it's security cameras, Nest cameras, or whether it's body worn cameras of law enforcement officials.

But on the other hand, the algorithms right now are not able to detect faces as accurately among people of color. And so, we have NIST, for example, issuing reports saying this is problematic. We have about seven or so states that have put a pause or a ban on the use of this technology by law enforcement. And I think about two dozen or more major cities across the United States have adopted laws limiting, or banning, the use of facial recognition by government authorities. Not only in addition to the accuracy and bias concerns about facial recognition, I think there's a general public creepiness and concern about big brother watching us. And we certainly can look at other countries that are using facial recognition technology that are much more authoritarian than we have.

The third area where algorithms, and to some extent what might be thought of as artificial intelligence, come into play is in criminal sentencing. Here, actually the algorithms that are being used for risk assessment purposes are pretty crude. But the aim is to try to forecast whether a defendant is likely to recidivate and then how should that be factored into sentencing. And there's been a good bit of public controversy about reliance on these risk assessment tools, as well for concerns about racial bias.

I think in all three cases it's pretty clear that technology can have some side effects, some unanticipated consequences that public officials haven't thought through. Particularly about bias and that government officials deploying the tools relying on artificial intelligence need to take those other factors into account and roll it out slowly to know that it's properly validated, that it's not creating unintended consequences. And that it's building in public concerns and responding to public concerns.

I mean there are points that I think were raised in our conversation that I would build on. Kumar emphasized the importance of public education. Totally agree with that, but there's also a component of *listening* to the public. It's not just public education from the standpoint of propaganda, getting it out there and we're just going to tell you, the public, what this technology does and why it's good for you. But also, public officials, law enforcement officials, need to be really attentive to public concerns, open to hearing them.

Listening doesn't mean necessarily you can satisfy everybody's concerns, of course. But at least you can (a) be open to them because you might learn something and that prevent problems down the road, and (b) You can at least demonstrate to the public that you have heard them, even if you're not able fully to address all of those concerns. I think when it comes to AI, for example, one public education opportunity and public listening opportunity involves asking "What's the alternative to AI?" Just having a conversation that, well, maybe sticking with human beings making decisions is not always going to get you a fair outcome either. We should work collaboratively trying to address the very legitimate

concerns that members of the public have about AI tools, about bias. But also recognize that there's bias in the status quo too. And what we want to do is improve. So that's one thing that I would add on.

SASHA: One thing you mentioned on the panel, I was hoping we could talk a little bit more about, it sounds like you've done some work specifically around the role of vendors and contractors in this space. How does that uniquely create challenges or opportunities? How does that work? And what recommendations or best practices do you have, whether, you know, some of our listeners sit on the vendor/contractor side and some sit on the government side as well, and then some are taxpayers and citizens as well. But how do you see that relationship playing out in this kind of space?

CARY: Well, I guess what I'd say to the vendors, first of all, is that if you want to see your technology introduced on a more widespread basis successfully, and if you want to avoid the kind of backlash that we've seen, in particular with algorithmic aversion and the like, then you need to recognize that your role is not just as a developer and a seller of technology. You need to serve your clients' holistic needs. And those holistic needs are to build public trust and support and confidence in the technology that you're developing. What does that mean? That means that you can't claim proprietary trade secret protection over every little thing related to your technology. Does that mean there can't be some reasonable accommodation where the real innovation that you have with your technology is protected? No. But it does mean that you shouldn't over-claim.

Now, speaking to the government, that is, to the procurement officers or agency officials that are working with the contractors: You need to think ahead. Think ahead to the litigation that might occur. Think ahead to the public controversies that might develop around this new technology and ask yourself, "Does this contract afford us the opportunity to gather the information and to disclose it to the public that we can anticipate we might need when those situations arise?"

Now when it comes to litigation, the courts, so far at least, have been pretty protective and have accepted claims of trade secret protection. They haven't tried to pierce the veil of that. But it sometimes has meant that the government has sort of lost. There was a case in Houston involving a school district—this wasn't in a law enforcement context—but the school district had adopted an algorithm to evaluate its teachers and the contractor claimed total trade secret protection over it. And the court said, "Well, you know, there's nothing I can do about that and, in that case, I have to let this go to the jury because who knows, there could well be some problems with it. And the city, the school district, can't assure us that there isn't a problem."

So that's in the litigation context, but in the context of the court of public opinion, it's also essential to be able to demonstrate that some rudiments of how the algorithm is designed. What type of data are being used? How has it been validated? Can we put forward the auditing results? Have we had it peer reviewed?

By the way, you can get some third-party validations sometimes of these technologies that can help, and those results can be disclosed to the public. Maybe the third parties go in and they understand, and they're looking at what's happening under the hood, so to speak. But these are all things that I think should be anticipated up front when undertaking the contract. And I think it's in the interest of vendors to be accommodating to this. And quite frankly, I think it's very short sighted of them to try to do otherwise if you want to have the technology be widely adopted by the government.

SASHA: Thank you so much. That's so insightful about a very specific piece of this. It's so critically important. Anything I didn't ask you before I let you go that I should've asked you or that you want to follow up on.

CARY: Using these tools wisely and building public confidence is really the key. I mean, having them do what they're supposed to do can really help, but also they must be accepted by the public. And the public deserves that. They really do deserve that. So, thanks so much I enjoyed talking with you.

SASHA: Thank you so much for joining us! Be well.

Dr. Amy Grubb, thank you so much for joining us on Mission Is Possible. It is a real treat to have you with us. To kick off and get started, could you, just for our listening audience, introduce yourself and tell us a little bit about your background and what you're doing now at FBI?

AMY: Yeah, sure. Thank you so much for having me. These are some of my favorite topics, so I'm excited to be here. My name is Amy Grubb and by training I'm an industrial organizational psychologist, which means I am interested in people at work and the behaviors that they do. And I've spent most of my career working in the space of culture and leadership and change and how all of those things kind of help make organizations work with the trade craft and mission that they're trying to accomplish.

In the last few years, I've spent most of my time working in the technology sector and working within the FBI as we try to digitally transform the organization and move forward, not with the technology piece of it because I am not a technologist and I am in a lot of ways, the epitome of user error, but instead, the human-side of technology and how do we make it easier for humans to do the right thing with the technology and harder to do the wrong thing with technology? How do we make technology part of our response package and not just like, do we send humans or do we send technology, but how do we marry the two of them together and make them better friends?

And then also thinking a lot about the change initiatives that we have associated with it, what the cultural elements are for technology in the organization and how do we enhance them through different types of behaviors? And what kinds of leaders do we need to be making these smarter technology decisions as we're moving forward and implementing them across the organization?

SASHA: Awesome. Well, I know you're the perfect person to talk to because as you know, the topic of the day for us is, we're calling it sort of "Cautionary Tales," right, "How Technology Implementation is Impacting the Law Enforcement Landscape." And we've been talking with Cary and Kumar and John about a couple of examples, rapid DNA implementation on the border and AI in law enforcement and body cameras. One of the things that keeps coming up, and I wanted to dig a little deeper with you into, because I know this is absolutely kind of your sweet spot and area of expertise, is a number of them have said, "This isn't really a technology issue, this is a people and change management issue." Can you talk a little bit about that based on where you sit your experience at the Bureau?

AMY: Yeah, I mean, I think most of the time, no matter what the subject matter is or what the trade craft is that you're talking about, most change initiatives in terms of the "what piece of it" are fairly solid. No one in management says, "You know what I want to do? I want to really mess up our performance and I really want to institute something that's going to be awful in the organization." It

always starts as something that people think is going to enhance the performance of the organization in one way or another.

But then people get involved and a lot of times I think the issues with people are, one, there's a skills issue. People either don't have the skills to enact the change, or they're afraid to admit that they don't know what it means. There's an identity issue. If we enact this change, my job might be diminished, what I actually do might significantly change, and that kind of gives people some heebie-jeebies.

And then there's always some history and political issues. So, depending on who the messenger of the change is or who the enactor of the change is, you may or may not have more or less trust in those humans, or that function, or that entity to really drive that change. And I think technology just sort of exacerbates that because technology is one of those things that is not very tangible for people. The outcome is tangible, but what happens in the little black box, most people don't quite understand, and especially in law enforcement. Law enforcement is a very tangible-based entity and profession. And so, that there's an unknown is even scarier than what unknowns typically are.

So, I definitely think that the change initiatives, especially around technology, are very much human-based and a lot of the same basic principles hold. You just may need to kind of amp a few of them a little bit differently when you're talking about the implementation of a technology.

SASHA: That's perfect. Can I pull on that thread a little bit? I mean, in terms of while the change management kind of typical issues apply, that it is a little different or a little amplified, you mentioned one example of that the results aren't tangible. You know, we were talking to Kumar about the classic kind of need for a burning platform. And how do you describe that in the technology space? Are there other areas where this is different? I mean, I think from my experience about sort of the people, again, back to the people aspect, right, the technologists involved and then the change-people or the business people and those kinds of cultural or personality changes, are there other ways that it's amplified in the IT change space?

AMY: I think one of the key areas is that if you think about the people who work in the technology space and people who work in the law enforcement space and you think of them as two circles and you overlap those circles, the overlap of venn in technologists and those who practice law enforcement is very, very small. So when you are talking about highly complex technical issues and those sorts of areas, you don't have a lot of translators to be asking the really good questions on like, “Well, what does that word mean to you or what are we actually trying to solve for here and then who are we trying to solve it for?”

When you talk about typical change management projects, you have enough people in the overlapping venn of whatever the trade craft or whatever the change is that you can get people to translate. I think in law enforcement and technology especially, those two groups so don't overlap with each other that it's almost like you have people speaking Swahili and you have people speaking Swedish and there are no Swedish-Swahili translators, but there might be an English translator in between who can like do all these things, and it just makes it more difficult.

I have seen, that on a smaller scale, it works super well because people are willing to ask really good questions of each other and be vulnerable that they don't know this other stuff, but you're talking about two populations who kind of pride themselves on being really smart and really knowing a lot of stuff.

So on a larger change scale, people might not be as open to doing that, but on the smaller scales, I think it works pretty solidly, I think it's really a matter of getting people comfortable with asking questions and admitting what they don't know. But I mean, that's in every change initiative, but I think because you don't have people who can translate very well that it just really exacerbates the problem in law enforcement and technology intersections.

SASHA: Such an interesting point. And I know you sit often squarely in that tiny, tiny space of overlap and kind of working that space and making that happen. So, I wonder for our audience, if you can offer any other thoughts. I mean, the idea of sort of starting small is such a good, tangible suggestion, right? Like if the two groups are just smaller, it seems more manageable and maybe possible to bring those groups together.

You talked a bit about encouraging vulnerability and asking questions. Can you just offer our listening audience, for either folks who are trying to sit in that space or maybe someone who's looking for someone to sit in that space and doesn't know where to start, what are sort of your tips and tricks? Because I know that's the space you spend most of your time (laughs).

AMY: Yeah. I mean, I am a huge fan of questions. Like find somebody who's willing to be like, "You know, I just... can you help me understand that a little bit more?" Like, "What does that look like on the back-end?" Or, "When you say 'validation,' what does that word mean to you?" You know? And having somebody, and oftentimes I would say that having somebody who is neither a technologist nor a law enforcement person, but like somebody who can just be that, like, "Hey, how does this actually work?" To be sort of the person asking the questions for both sides in the public forum. So, if you have somebody who's a really good facilitator or somebody who's just genuinely curious and can do those things, that's an awesome person to sit in that space.

One of the things that I think is an awesome advantage in terms of technology and law enforcement folks, is that they both just really want to get stuff done and they really pride themselves on getting stuff over the goal line. And so, I think a second kind of tip or trick is to really focus people on what is our end-state and how do we get there as quickly and as good as possible because both of them also want things done right, by the book in the most elegant way possible to get us to that end conclusion. So, if you can get people focused on what the end conclusion is, that's a second tip that I would add that can be very helpful.

And then the third tip is really driving towards practical examples. So, bringing it down to the tangible level, because even technologists, they're very straightforward and they're very much thinking about "What does this actually physically look like and how do we map this out?" And they're kind of mapping out on the technology side, maps out to giving it to the human to use it. But that's when their mapping starts of like, "Well, if I use it this way, then this is what happens and this is where the data goes, and this is what I want to do with it, and this is what the outcomes could be." And drawing that map from beginning to end for both of them, not where the handoff is, but on both sides of it, it just draws the picture up there and then allows you to kind of see where the different conversations need to be and then that way you know that everybody's schema is the same.

So, all three of those tips really aren't all that different than what you would do in a change management initiative of any kind. But I think with technology, it's especially important to be focusing on the language piece of it and the totality of what that change looks like from beginning to end and

keeping in mind that the people who are doing the designing don't do the outcome job and the people who do the outcome job, like they're very different than the designers and neither one of them are communicating for themselves, they're communicating for the other person. And so just trying to create that is, I think, super important and the more practical and tangible it is, just the more people can hold onto it and see where there might be challenge points going on.

SASHA: Thank you so much. That's incredibly helpful. As we've worked together for years, the first piece is to acknowledge the people piece, right? In any of these large challenges, you always remind me "How about the people?" and then so helpful to really think as you just laid out, really very specific and tactical suggestions about how to make those connections, bridge those communication gaps, so helpful. Before we let you go, Dr. Grubb, anything I should have asked or you want to add for our audience before we call it a wrap?

AMY: Yeah, you know, I think one of the other things, you just really nailed it, is it's not, you know, all these practical tips, or you could put them in a standard operating procedure or in a book and people could follow them and can come really close to a blueprint of what to do. But these are humans who are part of this. And humans have drives and motivations and likes and dislikes and personality conflicts and all those things.

And just because both technologists and law enforcement folks tend to be very by the book and standardized and stuff like that, they're still people and you just have to expect that there's going to be bumps and people are going to get mad and people are going to get frustrated and people are going to be excited about certain things and just allowing for that to be part of the organic process. It sounds so flowery and cheesy, especially in these two disciplines, but that is a real thing. Because neither law enforcement folks or technologists are machines, they're actual humans. And you just have to kind of build in for that space as well. Nobody fits either stereotype particularly well.

SASHA: Well, Dr. Grubb, so helpful as always. We really, really appreciate your time and having you join us for this episode.

AMY: Sasha, thank you so much for having me. It was a pleasure.

SASHA: On that note, I'd like to thank all of our guests today for their time to talk with us and to share their insights into this critically important topic. Thank you for joining us for this episode of Mission is Possible. To find more information on the Guidehouse/American University Mission Is Possible Speaker Series, please visit us at Guidehouse.com.