BIG BROTHER IS WATCHING AND HE'S HERE TO HELP

By Mandi Bohrer and Ron Granieri October 6, 2020
https://warroom.armywarcollege.edu/podcasts/facial-recognition/

Welcome to **WAR ROOM** the official podcast of the U.S. Army War College Online Journal. Graciously supported by the Army War College Foundation, please join the conversation at warroom.armywarcollege.edu. We hope you enjoy the program.

The views expressed in this presentation are those of the speakers and do not necessarily reflect those of the U.S. Army War College, the U.S. Army, or the Department of Defense.

Ron Granieri: Welcome to A Better Peace the War Room podcast. I'm **Ron Granieri** Professor of History at the Department of National Security and Strategy at the U.S. Army War College and Podcast Editor of the War Room. It's a pleasure to have you with us. The best form of security is one that identifies potential criminals before they act. Such preventative action, at least outside of the novels of Philip K. Dick, is however limited by imperfect human clairvoyance. Facial recognition technology however, promises to offer creating databases that can help security forces identify and track suspicious individuals. The more promising facial recognition becomes as a technology however, the louder grow the voices concerned about the potential invasion of privacy that such mass collection could or would entail. Only the guilty need worry may be the comforting reply, but how does a free society protect itself while also protecting the privacy of its citizens? Our guest today to help us wrestle with questions of what facial recognition technology can accomplish and how it should be used is **Lieutenant Colonel Mandi Bohrer** of the United States Army. Lieutenant Colonel Bohrer is a current student in the Resident Program at the U.S. Army War College Class of 2020 who received her commission as a military police officer from the United States Military Academy in 1998 which a Bachelor of Science degree in psychology. Lt. Col. Bohrer also holds a Master of Military Arts and Sciences degree from the School of Advanced Military Studies and a dual master's in Business and Organizational Security and Human Resource Development from Webster University. A highly decorated officer, she has served in a variety of leadership positions from the Pentagon to Kabul and Baghdad, including command of the 701st military police battalion at Fort Leonard Wood in Missouri. More recently, Lt. Col. Bohrer served as the chief of the tactical maneuver support within the concepts, organization and doctrine development division within MSCOE, Capability Development and Integration Directorate and as the chief of law enforcement and security for the military district of Washington. Welcome to A Better Peace, Lt. Col. Mandi Bohrer.

Mandi Bohrer: Thank you. I am excited to get to do this today.

RG: Well we are glad to have you here. I want to ask, you have a distinguished career in military police, what got you interested specifically in the technology of facial recognition?

MB: Specifically, for facial recognition, I have been interested in just what biometrics in general provide as a security professional for several years. But my most recent job, as you mentioned, as the chief of law enforcement security for the military district of Washington, really made me look at the capability even more. Because we have a number of events in the Washington D.C. area that the military is heavily involved in. We are responsible for either leading the security or supporting the security and during those events, you bring in so many people, so many civilians, members of the public into those events and so we always looked at ways where we could maintain a high level of security that made it easy to access the event so that the public would be encouraged to attend—it would be easy for them to attend and share in the military experience—without creating huge delays but at the end of the day, it being a secure and safe event for everyone involved. Facial recognition, the more I learned about it, was just a great opportunity for us to leverage for the security of those events. While we were there, we started to look more at how we could leverage that technology using facial recognition to enhance the security of those events and started work to establish an Army pilot program that we hoped and still hope one day will be adopted across the Army and then potentially across the DOD.

RG: And so, was the idea that the images would be collected passively? In a sense you wouldn't have people stopped to get their picture taken, but rather well-positioned cameras would get a look at everybody's face and download the images to a central database? Is that the basic idea there?

MB: That's the basic idea. And it would depend on the event or the purpose. So, if it's a special event, yes, those cameras would be oriented in locations around the entry control point. People probably don't even notice that they are there, but there are a number of cameras and they are tied back to a security command post or a security location where we are able to constantly monitor and make sure that we are not picking up on people that are on a watch list or have wants or warrants or essentially people that could be there to do harm.

RG: So, Mandi, the way I envision this then, it would require a degree of coordination between agencies in the sense of who would own the photos that were being compared against. At an event you are taking in the images, but then if you are taking about people with warrants, people who have been arrested for other things or are on a watch list, each of those kinds of photos would be held by different organizations, right?

MB: Correct. The three major players for this are the Department of Defense, the Department of Homeland Security and the FBI, the Federal Bureau of Investigation. Each organization has a database of faces, of biometric data for watchlist personnel. Each of those organizations are

maintaining compliance with federal privacy laws and making sure that they are doing things properly for the access and security of their database. And depending on what the event is, who is the lead agency that would drive what happens after you get a potential match. There are information sharing agreements between the DOD, DHS and FBI where depending on what's going on, you could pull in those various databases if needed.

RG: Obviously, we are speaking purely open source here, so no secrets are being traded. How do you or the officers in charge of this program, how would you envision it working? Let's say you are doing security at an event in Washington, doing the scanning of the crowd and you come up with a match, let's say you discover that there is someone who is on a watchlist who is milling around in a particular crowd or who entered through Entrance A, would the goal be then to enhance surveillance of that individual based on the fact that you know that that individual is there? Or what would you do next?

MB: So, the facial recognition software and that technology produces probabilistic results. So, whenever that computer screen pings saying we have a potential match, you can set it for a minimum level of confidence that you are looking for and it will tell you, there is 99% certainty that this face matches this face out of the database, and we consider that lead generation. You may continue to monitor them from a distance, you may approach and ask for identification and try and confirm if that is indeed the person. And it might not even go that far. The screen may ping that you have a match and that security professional looks at it and goes, nope, I think the software, they got a mismatch here and you can discard it. I just want to clarify one of the things you said before, with my recommendation for how the DOD could use this, we would not continue to maintain captured images of those people in the crowd. It would be, you walk in front of the camera, it takes that split second to compare your face to the database, and if it's not a match, it is gone just as quickly as it came in. Those would not be things that we would want to save.

RG: Understood. That is an important distinction. Thanks for bringing that up because I was curious about that. Where are we, broadly speaking, in terms of the technology that allows us to have any confidence that matches are accurate? There's the *could* question and the *should* question. So, we will start with the could. Could we really be confident that we are identifying someone as someone who is in a database or at least as the way things stand, are we still at a point where it's possible for people either to thwart the technology themselves or just for the technology to be imperfect enough that it will come up with false positives or false negatives?

MB: I would say the technology is still imperfect. And I think that's why it's important to have your competent security professionals that are taking a look at things and treating this as lead generation and not treating this as we got to grab that person right now but for further investigation to see what's going on and figure out who the person is. You may have read in the

news concerns about facial recognition having a higher misidentification rate for people of color and the National Institute of Standards and Technology (NIST), they found that, but when you look over time, as the software and the algorithms get used more, those algorithms get smarter and the technology improves. So, you increase the confidence of the system the more we use it. And it's getting better and better every year. I think that with the proliferation of it, the UK is a very heavy use of racial recognition technology, Russia is investing far more in facial recognition technology, South Korea is a huge user of facial recognition technology, and I am sure you have read about China's safe cities initiatives and their investment in the technology both in their country and in other places. I think all of those things combined are going to make the technology better and smarter and this is projected to be a growing industry worth $12 billion dollars estimated in just four more years. That's pretty big.

RG: Indeed. And it is interesting because the idea of using technology to identify people who are going to break the law, takes on a different flavor depending on what laws we are talking about people breaking. In a dictatorship, simply expressing a legitimate critical opinion of the government is a crime, in a free society of course crimes are very different, we would like to think. It's interesting that you mentioned at least two states, the United Kingdom and South Korea, who are friendly allied states with the U.S. Is there a degree of technological sharing or best practices sharing that goes on between friendly states when it comes to the development and use of this kind of software?

MB: A large portion of the development of the software from my research is done by the private sector. And those countries are international, the NEC for example is a major player in facial recognition technology and they have contracts and systems all over the world including the U.S. So, as they improve what they learn in Korea, for example, or what they learn in the U.K., they are going to apply those lessons across the systems that they offer.

RG: Gotcha. So, we may be talking about the same firms that are offering variations of the technology to many of the same international players.

MB: As countries learn more about faces in their nation of different demographics, that can go toward closing that gap that the NIST recognized where the tests that they did showed a preponderance of misidentification for people of color. We can learn from other nations and what they have and different cultures and backgrounds and apply that.

RG: This may be outside of your specific experience, but I am curious about your opinion as police professional and security professional, should there be limits on the availability of these technologies? Should the United States be encouraging companies not to sell this technology to unfriendly states? Or is it already too late to stop the proliferation of this technology to states that we would rather not have it?

MB: I would say that unfriendly nations like China and Russia are already well on the road for developing their systems so it would be hard to undo any of that or to stop that. I think that they have got their own capability of developing it and they are moving out on it. I do think that if they had access to what friendly nations are collecting, that could be a security vulnerability. That is something that we have to protect and certainly with the way that other nations use their information, I wouldn't want that to happen to the American population.

RG: Am I correct that your research as a student at the War College included research specifically on new programs or thinking about how we could develop and use this technology going forward? Is that true?

MB: Yes. I did some research and considered how other nations use it, what the privacy and legal concerns are, what authorities grant us the ability to do it, and how we can do it in a way that continues to protect American civil liberties and Americans' expectations of privacy. I think those controls are in place, those authorities are in place. So, I made a few recommendations on how we can leverage this technology to increase the security of our installations and of the people and events that are coming and going around all DOD activities.

RG: What's the first recommendation that you had?

MB: The first recommendation is that I think that we should expand its use. There are a few installations across DOD that already do this. I think that we should expand it across the board, make it available for all installations to use particularly during special events whether that be an air show that a base may be hosting or a major fourth of July celebration. These events bring in hundreds of thousands of people onto the installation, lets our military connect with the American population, pretty important. We want to maintain security when we do that. We also don't want to have a line at the gate that's ten miles long of people trying to get in. Facial recognition is something we can use that can quickly make sure that that person—not to be too simple—but to make sure that person is not a bad guy. It will, in seconds, do that background check on them, make sure they are who they say they are, and they can access the event, they have fun, everyone stays safe.

RG: What strategy do you think security professionals should take with dealing with public concerns about privacy? Is it enough to tell people, we are not going to keep this information? Is it enough to tell people, you give more information in a way when you sign up for Facebook than you are ever going to give up looking at a camera on your way into a military base? Is that enough to satisfy people? Because it's one thing to tell people they shouldn't be worried about this, but if people are, if that is a fact that they are worried, how do you dispel those fears without simply telling people, you have nothing to worry about?

MB: There are a couple parts to this. One, you are absolutely right. I totally agree that people either knowingly or unknowingly give up their personally identifiable information all the time for everyday conveniences whether it's you using facial recognition unlock your phone or providing your location constantly so that you can get a discount on insurance or you can get access to your bank. We do it all the time and we don't even think about it. And that is largely unregulated. The government use of it is regulated. We do have a number of controls so that only personnel that have a right and a need to access the information will access it. We have controls, that we have used every possible means not to potentially invade on someone's privacy and that we are going to control how we use that safeguard and use that information. That doesn't mean that people aren't going to be concerned about it, I think it's fair. You always want to make sure that the government is not only providing for your security but doing it in a proper way. I think we should be prepared to openly, number one, notify the public that in order to access this installation or to access this event, we are using facial recognition technology to enhance the security. I think that's absolutely essential that we do some sort of notification. But also, with this, I know that you have been on an Army installation and for anyone else listening, whenever you come onto any military base, if you look off to the side, there is a brown sign somewhere near that gate before you drive in and you probably don't pay much attention to it. It's got lots of words on it, but what that sign is saying is that by entering this installation, you are giving your implied consent to additional security screening procedures. That means that we can do a background check on you, we can check your ID, we can make sure that your face matches the face on the driver's license and that that face matches in the big database that we use, that national law enforcement uses. Those sorts of screening protocols are already in place, but you could the same thing, the same level of screening, checking those exact same things with facial recognition in a second. People say, you are violating my privacy, or I'm concerned about my privacy, we are looking at the exact same things with this technology as we would have looked at if you went and sat in line for 10, 15, 20 minutes to do these checks.

RG: Right. But of course, you are saying as long as there is a degree of disclosure, so we are not collecting this information in secret, we are letting you know that we are collecting this information?

MB: Yes. And that is actually part of the controls that are already in place. Whenever any federal government entity is going to do something that collects information on people, you are going to do a notice on that. And we do a formal one, it gets published, people can go look at it. So, that's in the system, its official government record. But also, I think it's important just because of our culture and to be transparent in the use that we notify people that that's what's going on whenever they are attempting to access an installation or event.

RG: And to be clear, what we are talking about so far is people entering, accessing a military installation or a sensitive government related structure. What about the prospects of the use of facial recognition software more broadly in public spaces? We know that in Great Britain there is a proliferation of close cameras and in South Korea, we won't even talk about places like China but what should we or how should we as citizens think about the way that that kind of information is or is not being collected, is or is not being used by security forces on a day-to-day basis?

MB: Well, first to clarify, I'm not going to advocate for the DOD using facial recognition at the corner of East and Main in whatever city.

RG: Right.

MB: That's not part of my argument here. But you are right, police agencies and a number of major metropolitan areas and even some smaller towns are using this. It's probably more common than people realize. Fortunately, and perhaps I'm biased as police professional, there are a number of controls that are already in place just for the military on how they can use this information and how they can safeguard it. So, the good thing is that it's regulated and that if someone is going to violate those controls, there will be repercussions. What I find more concerning is that there is not currently any regulation on the private use or commercial use. There is a major convenience store chain that uses facial recognition in their stores to keep an eye on people they consider to be troublemakers. Not regulated. They are using that as a fair use. They are trying to protect their product. I think it's a little bit more concerning when those companies then are selling your information, your routines, where you go, what you spend your money on, all these things about you to third parties and then you completely lose track of your own personal information. And maybe that's a slightly separate topic.

RG: When we think about the things that people are afraid of, people are afraid of a lot of things, we all have things we are concerned about. One of the fears is that this kind of information is going to be shared without people's consent or knowledge. And if understand what you are saying here is where the use of that information within the DOD, within security space is limited by statute, whereas in the private sector, there is no specific rule against a private company sharing with another private company or selling to another private company information that they collect on their private premises.

MB: Correct.

RG: So, people perhaps should be concerned about that, but they should focus their concern on the source of the concern. It's not big brother that people should be afraid of perhaps but it's a proliferation of little brothers out there who are collecting people's information and selling.

MB: Yes. I understand the concern for a government overstepping and invading on a person's personal privacy. I understand that and I am not saying that people shouldn't worry about it but to me, at least that is regulated and there will be repercussions on me if I do not properly safeguard that information or if I decide to share it with someone else that doesn't need to know. There will be an audit and I will be held accountable for that. If whatever store you like to frequent starts selling your shopping habits because they have tracked you around the store, to a hundred other stores and across the world marketing firms, all that, it's a little bit much.

RG: Right. And they aren't likely to get reprimanded for that. They might get a quarterly bonus for managing to sell that information.

MB: Correct.

RG: Well, that may indeed be a subject for another time. As a final question for us to wrap up today, how do you imagine yourself working in this space or with this topic in your future assignment when you go back to Fort Leonard Wood at the end of this academic year?

MB: That is an interesting question. I am going to work in a directorate called the Fielded Force Integration Directorate and it will cover a huge array of capabilities that cover engineer, chemical, biological, radiological, nuclear and military police. So, a big protection portfolio, maneuver enhancement, lots of unique ideas in there. So, I could see that this could come up as we discuss protection capabilities for our force and for the homeland and finding ways to equip, employ, field and what the doctrine should be for it. I think that would be pretty exciting if I could see something like that come to fruition, I'm able to work it through to a much, much bigger audience in a future assignment. That would be pretty neat.

RG: That would be pretty neat. Well, I hope you get a chance to do that, Mandi Bohrer, and I hope that you will get a chance to continue your work. We really do appreciate you taking the time to join us today to talk about facial recognition and everything that you do here on A Better Peace. Thanks for being here.

MB: Thank you.

RG: Thank you. And thanks to all of you for listening in. Please send us your comments on this program and all the programs. Send us your suggestions for the future. Please, if you are listening to us for the first time, please subscribe to A Better Peace and rate and review this podcast on the podcatcher of your choice because that's how other people find it and can listen to it. We are always interested in hearing from you because we always hope that we can provide

things that you are interested in listening to. We look forward to seeing you back here again next time, but until next time, from the War Room, I’m Ron Granieri.