

THE BROOKINGS INSTITUTION

A CONVERSATION WITH THE CIA'S PRIVACY AND CIVIL LIBERTIES OFFICER:
BALANCING TRANSPARENCY AND SECRECY IN A DIGITAL AGE

Washington, D.C.

Friday, May 31, 2019

PARTICIPANTS:

RYAN TRAPANI, Moderator
Federal Executive Fellow
The Brookings Institution

BENJAMIN T. HUEBNER
Privacy and Civil Liberties Officer
Central Intelligence Agency

* * * * *

P R O C E E D I N G S

MR. TRAPANI: Good morning, everybody. Welcome to Brookings. My name is Ryan Trapani. I'm a federal executive fellow here at Brookings. Federal executive fellows come to Brookings for about a year away from their home agencies or departments. And as a matter of full disclosure my home agency is, in fact, the CIA, where for the past four years prior to Brookings I was one of the spokespersons.

And so today, we're going to be having a conversation about privacy and civil liberties and other related matters as they touch on the CIA. And we have a great guest to talk about that, which is Ben Huebner.

Ben Huebner is the CIA's privacy and civil liberties officer. He came to CIA just over three years ago from the Department of Justice where he served as the counsel for intelligence to the assistant attorney general for the National Security Division, where he advised the department leaders on intelligence-related matters, including operations, litigation, and oversight. He has extensive experience developing and managing oversight programs, in particular related to intelligence collection and related to the Foreign Intelligence Surveillance Act, otherwise known as FISA, which many people now have heard about.

We're going to have a conversation up here for about 40 minutes and then we're going to open it up to questions. So, if you have some, start thinking now about what those might be. And I'll preview now and say again later, please make sure they are in the form of a question, so I don't have to cut you off.

So, Ben, welcome.

MR. HUEBNER: Thank you.

MR. TRAPANI: Let's start with the basics. What is your job?

MR. HUEBNER: All right. So first, thank you all for coming. Thank you, Ryan, for having me here. Certainly, thank you to Brookings. Gosh, almost 20 years ago, I spent a lot of time in this building in a program for young people -- at that point I was young

-- coming into public service. And then and now this has just been an amazing place for really pragmatic scholarship and good debate. And so, it is actually an honor to be back here, so thank you all.

All right. So, what is this job? Privacy and civil liberties at CIA, I think half the people will say why would you have this job at the CIA and maybe the other half would say of course you have to have this job at the CIA. A privacy and civil liberties officer, what is that?

So, these officers were created in a number of different agencies as one of the 9-11 Commission Report reforms. And there was realization even at that time, even right after 9-11 that there was going to be, needed to be an expansion of certain authorities. And yet, at the same time the fact that the government needed the ability to do certain things didn't mean that we actually should do those things in all contexts and that you needed to have someone at the table thinking about that "should" question.

I sometimes call my office the "Office of We Can, But Should We? And If So, How?" Right? You have an Office of General Counsel who gives us on the long -- as appropriate for the Department of Justice that "can" question of the legal authority. But then you have that separate question of should and how, and that's shortly why you have an office like this.

So, I came in that role. So, I report to the director. My office is up there with some of the other offices like the Office of General Counsel, the Office of Inspector General, that have that sort of Agency-wide function.

MR. TRAPANI: So, I think that's one important thing is that you are a direct report on the org chart to the director of the CIA, right?

MR. HUEBNER: That is correct.

MR. TRAPANI: You are not under the general counsel or the IG's office or some other?

MR. HUEBNER: No. There are different ways of structuring this, but at the

CIA we thought it was really important that this be a role that -- I certainly work every day, every hour sometimes for the Office of General Counsel, but it's a separate role.

I actually think that's really helpful to an organization, as well. When you're getting information from your attorney, they are always going to provide counsel, as well, and that's really appropriate. But it's good to know when -- the difference, that can and the should, right? What is the scope of the authority? And then when are we shifting to a discussion of how is the best way of doing this given the kind of broader privacy and civil liberties concerns that might arise, particularly in an intelligence field.

MR. TRAPANI: So, let's talk a little bit about how you go about doing the job.

MR. HUEBNER: Okay.

MR. TRAPANI: So typical day or where would you say is the two or three things that are the core elements of your job?

MR. HUEBNER: Sure. Can I go six instead of three?

MR. TRAPANI: You can six, sure. (Laughter)

MR. HUEBNER: So, the good thing about jobs like this is there isn't a typical day, which is why -- which is what makes it fun.

I tell my own officers as I bring them in that we really do have sort of six different roles: three of them internal to the Agency, and three of them external. Internal and primarily is this advisory role, right, whether it be operations or policies or how we handle the information to advise the Agency on these privacy and civil liberties concerns. And not just be there to raise concerns, but to really do the hard work of thinking through how are we going to address them? What are we going to do or not do? How are we going to mitigate them? And that takes a lot of work, a lot of relationship-building to do that, hopefully, and do that well. So that advisory role is really important.

What is does like practically actually mean? So, we have -- and I'll certainly talk about this later, we had a big role when we revised our controls on how we're going to

handle Americans' information a couple years back. But it also means if there is going to be a policy change Agency-wide, that policy change always goes through my office as a matter of course. And we're looking at it for those privacy and civil liberties concerns. Sometimes it's that. Sometimes it is, you know, hey, are we going to collect this thing or not? And everything in between. So that's the big one.

There is also --

MR. TRAPANI: Can I just stop you?

MR. HUEBNER: Sure.

MR. TRAPANI: It sounds to me like that is a proactive thing. It's not necessarily that you are passively reviewing say at the end of the year how did we do. People are coming to you and saying I have an idea for an intelligence collection program. I'm going to implement it. Can I do so consistent with the requirements?

MR. HUEBNER: Absolutely. So that advisory role, it is that proactive role.

We also have a review role, right, and that's in the statute, as well, where, great, we've made these commitments to protect privacy and civil liberties. How well are we doing? And so, we have this oversight role to evaluate for those U.S. person controls, for some of those controls for non-U.S. persons. How are we actually complying with those? And so, we do oversight reviews to look for that compliance, to try to find and spread best practices.

The vast majority, not surprisingly, given that the CIA is classified, we've done some unclassified work, as well. We have a report on FISA that's up on the CIA's website. And so, we'll do those reviews on a regular basis, sometimes related to a specific collection activity. And also, sometimes someone will raise a concern, right, someone within the building, within the Agency, someone within the intelligence community, someone within the public will raise a concern and we'll look at it and at times find, hey, there's some validity to that concern. We need to really conduct a formal review of what we're doing here. And then that feeds -- this is why you have it in the same office, that feeds into that advice role.

So that's another, you know. Advice and review, like that is a good 80 to 85 percent of the work.

MR. TRAPANI: So that's two of the six.

MR. HUEBNER: So that's two of the six.

MR. TRAPANI: Okay.

MR. HUEBNER: The third one internally is educate. So, if my office is the only one thinking about privacy and civil liberties at the CIA, we have done something horribly wrong. We can't be everywhere and, also, every single officer takes an oath to support and defend the Constitution. It is the role of every officer to be thinking about these issues.

But if we're going to give them that role, we're going to give them that responsibility, it is on us as an Agency to give them the tools to do that. So, we need to spend some time and we do spend some time with training in terms of how to spot these issues and how to mitigate them. Some of those things could be and are Agency-wide, some of them are us bringing in experts from the outside to talk about particular issues, some of them could be small groups. I've been doing some really interesting work with some of our data scientists on some of these issues and trying to provide that kind of feedback and that kind of training on an in-person basis. So, we think that's a really important role, as well.

So those are the big three internal ones. We also, and this is more unusual, certainly, for the CIA, is we have an external role. One of those roles is a coordination role. The intelligence community, the intelligence work is a team sport. And so, we are working, as we have to, with a lot of other agencies in doing that work.

But in turn, that also means when we're thinking about privacy or civil liberties concerns it is insufficient for us to only be thinking about the CIA's impact. Right? You've got to be thinking about it in connection, in collaboration with that overall. It might be that what we are doing combined with what some of our friends over at the Bureau are doing

changes the calculus. And so, there are other privacy and civil liberties officers throughout the government. They are on my speed dial. We talk absolutely every single day to do that coordination role.

And another aspect of that coordination role is to help facilitate the oversight of other actors. One of the things that the intelligence community very much does in terms of oversight is to ensure we have overlapping oversight, intentionally overlapping oversight. So, if you take something like the Privacy and Civil Liberties Oversight Board, which is this board of presidentially appointed folks within the Executive, with access to an enormous amount of classified information, we will facilitate their work as they review in the context of counterterrorism, what the actions of the CIA are and, more broadly, the IC. And so, we are certainly coordinating with them, as well.

MR. TRAPANI: What are the other oversight institutions or mechanisms that you often are interacting with?

MR. HUEBNER: So, the PCLOB primary -- PCLOB, Privacy and Civil Liberties Oversight Board -- PCLOB primary among them, but certainly Congress, as well, with our congressional oversight, talking with them. Each of our agencies has an Office of Inspector General, so they are a very important contact and we coordinate, as well, in terms of kind of a scope of our reviews. They find things and they send them to me. I find things and I send them to them, as well. And so, they are a really critical component of that oversight ecosphere.

The Department of Justice does certain national security. That was my prior work, oversight of the intelligence community. So, we're working with them, as well. So, there's a lot of different actors in that space that we need to coordinate with.

So, the last two, five of six is this, right? And this is actually one of the reasons that I agreed and really was excited to come over to CIA is this informed role. I found when I was at the Department of Justice doing oversight of the IC agencies that when I dug really down, as we certainly needed to do, that the CIA was really actually at the

forefront of protecting privacy and civil liberties on the activities that we were reviewing. And honestly, simultaneously, it was the Agency least capable of articulating that fact. It's not something we have historically been great at, about explaining to the public what we do and how we protect information in this space.

And so, coming out, doing sessions like this, talking to small groups, talking to large groups, talking to the NGO community is an important aspect of that role and something that not all our officers can do. If you are undercover, this isn't something that you can do. And so, we need to have folks who have the ability to reach out and talk to the public about these issues.

And the sixth of six is, great, we're providing information, but we also need to take in information, as well, in this space. You know, believe it or not, the CIA has not answered every privacy and civil liberties concern and is not the sole source of great ideas in this space. There are really difficult issues in the digital world that we live in. We have some thoughts on those and some input, but there are great ideas out in the private sector, there are great ideas out in the rest of government. And there are a lot of things where, honestly, CIA is not the policymaker, we shouldn't actually be making the decisions. Right? We can inform them, but we shouldn't be making them. So, we have to have the ability to engage with the public, with the NGO community to talk about some of these difficult issues.

MR. TRAPANI: So, let's talk a little bit about then the meat of what it is that you are trying to protect, how you go -- what are the specific rules maybe and maybe some of the issues that come up from those things. You talked about going into the -- talking to the people in the advocacy community, external oversight, getting input from other people, and that in this new environment there's all kinds of interesting questions that come up. And in some cases, the rules that were put in place in 1947 or 1977 or in the -- he's under the Executive Orders that are in place, they are a little bit outdated in the sense of the language they use and the structure that they have in place.

But maybe it'd be a good thing just to start with what are the civil liberties

and privacy issues? How do you protect those in terms of what's the specific thing that you're enforcing, so to speak?

MR. HUEBNER: Sure, in terms of what those controls are. So, start all the way at the top, right? The CIA has certain authorities and certain restrictions, and has since 1947. So, the CIA Act, the National Security Act, those are the starting points of what we're allowed to do and what we're restricted from doing. There are other more specific statutes that apply to some of our work, as well, like the Foreign Intelligence Surveillance Act in certain areas and the Privacy Act in certain areas, as well. So, you have that statutory baseline for a lot of these protections.

A really critical one for us is one of those Executive Orders, Executive Order 12333. Executive Order 12333 really defines the role of each of the intelligence community elements. It defines the CIA as the CIA and the FBI as the FBI. And also determines what scope is going to be for each of those agencies.

And really critical to my work says that if you're an agency, as the CIA does, that is going to in any way collect or retain or share, the word we would often use is "disseminate," Americans' information -- "U.S. person information" is the technical term -- you have to have a set of rules that are approved by your director and by the Attorney General. So, we refer to these as the Attorney General Guidelines. It is a horrible rule. It's kind of a reverse *Pirates of the Caribbean*. They are not guidelines; they are, in fact, rules. But they're referred to as the Attorney General Guidelines, and they govern those things about that collection, the retention, the dissemination of the U.S. person information.

So, we very substantially revised ours pretty recently and we released those in the past two years, and we did a couple of things. The first thing is actually the release. So, we had had these rules since the '80s. Before, we had once released them under a FOIA, I'm going to say somewhat heavily redacted. And that was our only kind of public communication about those.

So one of the things that we want to do and very much did with our U.S.

person rules is we revamped them, we rewrote them, and we did so in a way where we can and did release them entirely to the public. So these rules that govern how we collect information and how we retain it, how we disseminate it are entirely unclassified, were proactively released by the CIA. They're on our website right now. And they are the entirety of the rules. It isn't these rules plus a classified appendix. Right? You are looking at the whole rule set.

That was very revolutionary for us and it really actually required us to rewrite the rules from the ground up to be able to do that. But we thought it was critically important that we be able to communicate with folks about that, and I'll explain a little bit about why later we thought that was important.

But that wasn't the only reason we revised the rules. The reason we revised the rules is because our operational environment had fundamentally changed. We had a great set of rules if you were going to get a sheaf of papers in some darkened alley about military intelligence. And you could look through them and figure out what was the foreign intelligence information and you would send that back to Washington, and if there was Americans' information that was irrelevant, it was just left on the cutting room floor right then.

And I don't want to suggest that we don't still do that. We do and we still have rules that allow us to really just get rid of Americans' information right now on the front end if it's irrelevant, share it if is relevant. That is something that we absolutely do.

The change in the operational environment is the change for all of us. We are living in a digital space. So if you think about that rule set and then try to apply it to a different scenario, let's say you have a foreign adversary, a foreign hacker, and the CIA is able to obtain in an authorized way the hard drive of that foreign adversary's hacking, right, their hard drive, so that's going to be gigabytes and gigabytes of information. And it's going to have lots of information about the hacker and how they did what they did. It's also mostly likely going to have the fruits of some of that hacking, right? And if they are targeting

Americans, there's going to be some pretty sensitive U.S. person information on there potentially.

So what do you do with that? At some level you need to acquire that information and you need to know what was compromised. You need to be able to work with some of our partners in the rest of the federal government to advise people that they've been victims of that hacking attack. But you also have all of that American's information. And just play that out in a lot of other spheres. When you have digital information these ideas of boundaries just mean less, right?

The CIA is -- was, is, will continue to be a foreign-focused organization. We are going after foreign intelligence information. We have a worldwide presence. We are not looking inward. There are other agencies that do that. We are not one of them. The CIA has no law enforcement authorities, for example.

That used to protect us more than it did in terms of Americans' information. It used to be that you could reasonably assume you're not going to really come across too much Americans' information abroad. That's just not true anymore.

And so what we did with these new protections, these new Attorney General Guidelines, is we said we need to think about it differently. We need to continue to have and still do have rules for -- when we're actually looking for an American's information, there needs to be a rule set for that. The word we would use is "target." That is sometimes a fraught word. "Target" for CIA just means you are the person who we are trying to get information about or from.

MR. TRAPANI: Meaning the foreign person?

MR. HUEBNER: Meaning the foreign person, but also could mean a U.S. person, right? We might think someone is acting on behalf of a foreign government, for example. So that is what I mean by "target." I don't actually mean more than that.

So we have specific rules. If it is the case that we're targeting information about an American, there are specific rules for that. And those rules change depending on

the sensitivity of what we're doing. If we are getting information that is publicly available off a website, there are still a set of rules that govern that. If we are getting information from another government entity, right, if I ask the FBI about Ryan Trapani, so I need approvals to do that. I need a supervisor's approval and there are a set of protections based on that.

For more sensitive --

MR. TRAPANI: How did that request go?

MR. HUEBNER: How did that request go? Really well. (Laughter)

MR. TRAPANI: Very good.

MR. HUEBNER: And there are specific rules for doing something much more sensitive than that. And to be blunt, for CIA in particular, there's a lot of things we're not allowed to do. Right? The CIA is not allowed, other than to test their own equipment, to conduct electronic surveillance in the United States, period, end stop. The CIA is not allowed to conduct a search, a physical search, something that would require a warrant, of an American's information in the United States, period, end stop. The CIA is not permitted to conduct physical surveillance, to follow someone around secretly, of an American here in the United States, period, end stop. Well, the exception for that actually is you and me, if it's a CIA officer.

MR. TRAPANI: I'm a security risk.

MR. HUEBNER: Yes.

MR. TRAPANI: CIA Security can --

MR. HUEBNER: CIA Security, if I'm a security risk, can follow me around because I work for the CIA. But if you don't, we can't. Not to say there are other aspects of the government that can, they certainly are, but it's not the CIA. But there are certain things that we can do, and so we have a whole rule set for that.

The big thing -- and that really didn't change, honestly. Not too much. The big thing that changed was for that digital space. It's what do you do about large datasets where we're going to be taking the information in? Because of the volume we're not going to

be able to look at every bit and byte and make that individualized determination right there, you know, that information is foreign intelligence information, that information is not, but we're going to need the information to do that important foreign intelligence work. And so we set up a set of rules for that and we also changed the presumptions. Like our presumption, if we're collecting one of those large datasets, unless we have reason to flip the presumption and sometimes we do, but our presumption is not that all of that information is Americans' information because it's not, given what we do. We are targeting foreign, right? We are targeting for a foreign intelligence target. But we do presume that there's some Americans' information in there somewhere unless we have reason not to.

We start at that point and think, okay, we're going to build our rule set presuming there's some Americans' information in there somewhere and set our protections at that level with that presumption.

MR. TRAPANI: So let's unpack that a little bit. What does that mean? So you're an analyst at CIA. You get a set of data that comes in or somebody gets a set of data that comes in off a foreigner's telephone, cellphone, right, or, you know, some other kind of - or the hacker's hard drive. What does it mean to handle that data with a presumption that some of it is a U.S. person?

MR. HUEBNER: So let's go even earlier than that. Let's talk about the collection.

MR. TRAPANI: Okay.

MR. HUEBNER: We'll start with the collection and then talk about what we do. So what do we have to think about in terms of the collection? So when you're collecting with that presumption, that there's going to be some Americans' information, not that we are targeting it, but there's going to be some of it in there, what does that mean?

So the first thing it means is, as always, you know, you're thinking about the collection itself, making sure that from a legal standpoint it is authorized. You are thinking about how you collect it. You're thinking about using the least intrusive means for collecting

that information even though your target is foreign. You're thinking about the least intrusive means because of that potential additional U.S. person information and because it's just good intelligence trade craft. Why do the more dangerous thing when we can do it in a better way?

You are also thinking about what you're collecting. Right? It is a requirement for us that we scope our collection so that we are kind of reasonably collecting the least amount we need to actually achieve the mission that we are going for. And each time we do a collection we have to think about it in that scope. So you have all of those things at that collection point.

You are also then thinking, okay, now that I have the information, from that privacy and civil liberties standpoint how sensitive is that information? What sets of protections do we need to wrap around it given the sensitivity?

Using your example, if you have telecommunications, right, we're targeting someone's and getting electronic communications from that foreign target. But, no, they might be communicating with Americans, right? There's a certain significant level of sensitivity about that. And we are going to wrap those types of information around a greater set of access controls, limiting the access; we're going to require different things in terms of additional training; we're going to keep that information as a default for a shorter period of time.

MR. TRAPANI: Can we just stop for terminology. "Access controls," what does an access control mean?

MR. HUEBNER: So an access control just literally means who's going to be able to see that information. Is this information that's going to be available more broadly within the intelligence community or even more broadly at the CIA or is it going to be more locked down in terms of who has the ability to see that information?

And, you know, not surprisingly, the CIA cares a lot about access controls. We care about it for privacy and civil liberties; not the only reason we care about it. Right?

Having those -- you know, for whether it's counterintelligence or mission or privacy and civil liberties, all those things point in the same direction, which is you want to think really carefully about who has access to any dataset that we have. So we certainly think about that. But we're going in thinking if this is more sensitive information from a privacy and civil liberties standpoint, we're going to have to tighten those access controls.

So you have that. You think about how can that information be used? A big one is how can that information -- the word we use is "queried." That's where the rubber really hits the road. We can collect the information, but it's when we're retrieving it and actually going to use it that a real sort of privacy and civil liberties impact practically happens. And so you've got to make sure that you have the right controls in terms of ensuring that the scope of that query is related, reasonably related to the foreign intelligence threat you're going for. And for us, again, it's always a foreign intelligence threat as opposed to a law enforcement activity.

We might come across evidence of a crime. When we do, we take that evidence of a crime and we share it with our good friends at the FBI, and it is over to them at that point. Right? But we are not going in and kind of looking for that information.

MR. TRAPANI: So another stop and talk about defining the term "query." In practical terms that means that the information's -- there's a hard drive that we've gotten overseas or somebody's cellphone that we've gotten overseas, that we're targeting a foreign person for that. The data comes in. It's then put somehow into a system where it can be analyzed, dissected, access controls can be put on it in some way. But then the analyst or the person who needs to have access to that information, it's to query the data. They get to go and say -- do a search term saying, you know --

MR. HUEBNER: So it's definitely that, and I would say it's not limited to that. In terms of thinking about what the right level of controls are, it is that query using a search term.

MR. TRAPANI: Yeah.

MR. HUEBNER: But if we're going to use some sort of advanced data science analytic, we still need to be thinking of all those things, right? It's not limited to that simple search term.

MR. TRAPANI: So there are controls being put on how people access it, who can access it, and even what data is initially put onto the system to be accessed?

MR. HUEBNER: Absolutely. And then on top of that, then we think, okay, now that we have those controls, how are we ensuring that our use of that information, how we're doing that analysis, you know, doing the analytics, be it a search term or something considerably more advanced to that, how is that ensuring that we're bringing back the foreign intelligence information that we're actually looking for and, as much as possible, screening out the information that is irrelevant? Good privacy and civil liberties practice.

Also, these are not conflicting things. Better intelligence practice, right? As every agency, we have limited resources. We do not want to spend our time looking at information that is irrelevant to our mission. And so those scoping things achieve both of those goals.

So we have all of those. And then on top of that, then you've got the additional question of, okay, you've found information. When and how can you share it? Be it with the intelligence community, more broadly, be it with policymakers, be it with foreign liaisons, right, for a partner that we in the field on some foreign intelligence threat.

MR. TRAPANI: Maybe we could also define just "U.S. person." It's a term that gets thrown around a lot.

MR. HUEBNER: It's a term that gets --

MR. TRAPANI: People may have an idea it means citizen.

MR. HUEBNER: So it means citizen. It's not limited to a citizen. So a U.S. person is defined in Executive Order 12333. So a U.S. person is always it's a U.S. citizen. It's a lawful permanent residence here in the United States. It is also a corporation incorporated here in the United States or any unincorporated association that's substantially

composed of Americans. So those protections apply to each one of those categories.

MR. TRAPANI: So it's a very broad term in itself.

MR. HUEBNER: It's an intentionally broad term in and of itself. And there are also certain presumptions that go along with it. If you are here in the United States and we can't determine your citizenship status, we're not going to presume you're a non-U.S. person. We're going to do our due diligence, but we're not going to have that as a presumption.

MR. TRAPANI: Is there anything else you wanted to say about the mechanisms and the rules just before I -- I'll just into a question.

MR. HUEBNER: Sure, jump in.

MR. TRAPANI: So you talked about one of your jobs as engagement, going to public forums like this, engaging with the advocacy community, engaging with the business community who we may have to be working with. What are some of the troublesome areas that come up recently or what are the topics that seem to cause consternation that you get the difficult questions, so to speak?

MR. HUEBNER: So I think they kind of fall into two camps, right? I think a lot of them do have to do with what is that sort of proper and ethical use of information in this space? And that is something the CIA is dealing with, but we are not at all alone, right, in terms of thinking about how you're analyzing information. These ideas in data science, when you're talking about, for example, machine learning, right, how do you account for bias? And how are you going to evaluate it? How are you going to determine and get to a place -- so the technical term they use in this space is "explainability."

One of the interesting things about machine learning, which is an aspect of artificial intelligence, is they found, in many cases, from the analytics that have the most accurate results have the least explainability, the least ability to explain how the algorithm got to the answer it did.

MR. TRAPANI: Meaning the algorithm that is pushing that data out?

MR. HUEBNER: The algorithm that's pushing that data out --

MR. TRAPANI: Is really complicated.

MR. HUEBNER: Sometimes almost a black box. So that's a problem if you're the CIA. Right? As a little while back, our Directorate of Science and Technology said, and I'm paraphrasing because otherwise I'll butcher it, for CIA you show me an analytic that doesn't have explainability and I'm going to show you something that isn't decision ready. Right? We don't just have to have it be accurate. We have to know how we got there because of what we're doing.

It is great that people are using this in a commercial space, but we are not pushing you to a better brand of coffee here. Right? You need more than accuracy. You need to know how you got there. And so looking at how do you get that explainability, so that when you come back you can interpret it and determine to a policymaker how you got to that result and the level of trust that can be put into that.

I mean, that's a lot of the work that we're doing in this space is how do you communicate to those folks what the analytic is telling you and what it's not? How much reliability can you put into it? That's something we have to do in any intelligence product. How do you do that in this type of space?

And so that's something we are certainly looking at. We are not at all alone in that space. I tried to count the number of folks -- the number of different efforts working on AI ethics, you know, within the government, I stopped at a dozen. It's a lot. And there's a lot of work being done internationally and there's a lot of work being done domestically. So that's a big, complicated issue that we are very much thinking about all of the time.

I think sort of second to me, and it's not quite related, but a comparable type of program, is how do you evaluate and mitigate those privacy and civil liberties concerns in a really complex environment, where you're talking about systems that are complex enough that almost by definition there is no one person who's going to have all of it in their head.

I'm going to fawn here a little bit for Brookings. The best article I've seen

about this was put out by Lawfare a couple years ago. It was by Brookings' Susan Hennessey and John DeLong, who used to head up NSA compliance. It has the very unlovely title, "Explaining Footnote 14." They need to do better on titling their things, but what it's talking about --

MR. TRAPANI: That's that witty Lawfare style.

MR. HUEBNER: It is. It is. But what it's talking about is this footnote in a Foreign Intelligence Surveillance Court opinion. It is not a pretty footnote. It is really excoriating the government for some of the representations that were made regarding some of NSA's programs. And I think there are folks who certainly read that footnote and were very concerned and rightfully so on being concerned, but then leapt to this really shows that the government was having a lack of candor with the government [sic]. And what this article --

MR. TRAPANI: With the Court.

MR. HUEBNER: Sorry, with the Court. The government was having a lack of candor with the Court. And what this article does, and I think it's right in its analysis, is that's actually both not true, kind of missing the point, and in a really important way. It isn't the lack of candor. It's that in these very complex environments, there were representations that were not accurately made not in any way with malice, but because you had the lawyers, you had the compliance folks, you had the mission folks, you had the technical folks, each of them had a piece of it and no one had the whole. And so --

MR. TRAPANI: And they were trying to, just to back up a little bit, they were trying to explain to presumably the FISA Court --

MR. HUEBNER: How a --

MR. TRAPANI: -- how a specific program was working?

MR. HUEBNER: Exactly, how a program was working and how they were trying to get to compliance. And they did in the Court's view and the government ceded that it missed the mark because they hadn't brought all four of those types of folks together to get

to that sort of common understanding. And that's something organizationally we have to think about a lot in terms of -- it's one of the things, for my officers, I see that as one of their central roles is to try to be that connective tissue so that we are bringing all of those people to the same table and understanding what's the impact, but really how are we doing this, right? It's not just about the collection. It's not just about how we're sharing the information. It's not just about the analytic. It's about the whole. And that takes a lot of work and it takes a lot of work on the front end to do.

MR. TRAPANI: One of the other topics, kind of shift a little bit here, but I think is related to, is underlying some of the things we've been talking about, which is one of the other things that you try to do is talk about a word that is sometimes confusing and misleading, which is "transparency." Transparency in some people's minds is a binary. You either are transparent or you're not. But for the intelligence community, for CIA, they can only be somewhat disclosing. There's still things they need to keep secret. And yet, you are still a person who goes out every day and talks to people about what we're doing and shed some light, even if you're not shedding complete light.

Could you talk about your ideas about -- there's actually two different things we need to unpack here. One is the need for secrecy. And how do you view secrecy vis-à-vis the intelligence community and then vis-à-vis a democracy which rightfully has expectations of some understanding what public institutions are doing? And then given that, how do you think about releasing information to the public and bringing them in in understanding what's going on?

MR. HUEBNER: I think the important thing is to talk about when we say about transparency, transparency about what? And then why, right? This is, frankly, really difficult for the CIA. And the reason it is really difficult for the CIA is actually the reason you have a CIA is to, in some part, you know, we have three roles: to collect foreign intelligence information that can generally only be done in a secret fashion; to analyze intelligence information that we are trying to provide to policymakers to give a decision advantage, and

you can lose that decision advantage if you give that information to everyone; and then the third authority of the CIA is to conduct covert action. And "covert" is right in the word. If it's not covert, it's actually not something you can even do.

So given that scape, why do we talk about transparency at the CIA almost at all? And the answer to the question is, in part, we have to and we should because of those public expectations, the rightful public expectations, regarding our activities. I think of transparency -- you know, when people are asking about transparency, they're generally asking about three things.

The first is historical. What was the CIA doing back then? And this is sometimes back in the old and not terribly great days. So we do a lot of that actually. We put out a lot of information about some of the historical activities of the CIA. We've been putting out for a few years now and are going to continue to put out the Presidential Daily Brief and its predecessors, so we will get to the point where all the way from Truman on at least through Ford, which if you think about it, it's sort of really a big deal. We're taking literally the most classified document on Earth and we are doing some, hopefully, pretty light redactions and putting it out to the public. We spend a lot of time and actually a lot of resources trying to put out that historical record for folks, so we do a lot of that. Great.

The second thing people want to know is, okay, fine about the history of the CIA. What are you doing right now? And that is by far the most difficult one for us because if we are too revealing with that, we're going to lose that decision edge. It's really important when you talk about secrecy to also think about secrecy from whom. And it's not you all, right? The necessity of the secrecy is to protect that source and method from a foreign adversary. And that can be really difficult to also communicate because there are, sometimes information will come out and the CIA will have to defend it, and people will say, well, why on Earth was that secret? And the real answer to that would be, yes, based on the information you have, really questionable about why that would be secret. However, based on information we know a foreign adversary has, that is a really important piece of the

puzzle that's going to allow them to see something broader.

So we have to think kind of very carefully and it is a line-by-line thing when we release information, I've done this myself, to try to think about those questions before the release. And I think most people, given particularly what the CIA does, understand that. But the rightful question they ask us is, okay, if that is true, you at least, at least, CIA, need to tell us more about what's the overall threat picture so that we as the American public and through our members of Congress can understand what the real threats are to the United States. And you need to be clearer about what's the scope of your authorities? What are you actually allowed to do? What are you not allowed to do? How are you handling this information which falls more into my bucket?

And, again, even more critically important in a digital environment and in a space where you have an increased importance of the private sector, right, and when in cyber 90 percent of the landscape is in private hands, the U.S. Government, largely to include but not limited to the CIA, needs to be able to work with the private sector. And the private sector needs to be able to trust us, right, that we're going to appropriately handle their information.

And so we need to find a way and have been trying to find ways of declassifying as much as possible of that, how are we going to handle your information, as possible, so that we can show folks that we're going to do it appropriately. And to the degree that we make an error, be public about that and how we're going to correct it.

MR. TRAPANI: Coming up on question-and-answer time if you want to start to formulate those. I'm going to ask a couple questions before we get to that, which is -- this is maybe a softball question, but on the registration form for this event there were a lot of people who appeared to be here for the summer as interns.

You came into CIA midcareer. You had worked at the Department of Justice and came into this strange, mysterious organization as an outsider and got to walk around the rather plain halls of the building. I don't think I'm giving away a secret that it's a

plain government building on the inside mostly.

What would you say or what do you say to people when they find out that you work at the CIA and say what's it like?

MR. HUEBNER: So it's a lot of fun, which is an important thing. Like don't denigrate having a job that is fun.

So one good thing about when I came to the CIA, I came to the CIA, I was at the Department of Justice, but when I was at the Department of Justice doing oversight of the intelligence community, doing oversight including of the CIA. So when I came to the CIA, a good news story is that there actually weren't a lot of surprises for me. That would be a problem, right? If I was doing oversight of the CIA and realized it was a fundamentally different organization than I thought, that's concerning, right? And that did not happen. So eyes wide open for me going in.

So one of the great things about it is, it is an incredibly mission-oriented place and it's a mission that is exciting and incredibly challenging. So my training as a lawyer, the ability to work on issues where there hasn't been a resolution. I've been talking a lot about this digital space. I mean, think about that, right? When you're talking about privacy and civil liberties in the context of the home or the office or the public fora, so we have like 500 years of case law on that. We've been thinking about those issues for a really long time. And there are new things that come up on the edges, but the core aspects of that have been really worked out.

So social media's been around for like less than 15 years. There's a lot of work still to be done. And so that is interesting and exciting. And a great thing about the CIA is, you know, multiply that times 1,000 in terms of all the different things you can do there.

One of the things that was surprising to me, I should have known, but it was surprising, is the variety of skills that you need to do what the CIA does. We hire carpenters and hairstylists and enormous number of librarians to do some of the work and to work in a

space that isn't just lawyers as it was for me in the Department of Justice, but has people for all of those different skillsets doing all sorts of different things. Again, fun. It is a fun mission and it is a fun place to work. And it is great that it is fun because of the seriousness of what we're working on to have both of those things.

MR. TRAPANI: And then going back to how does it feel to represent an agency that you often are put in this uncomfortable position of defending not telling people things? You get to tell people a lot and you've spent more than a few minutes today talking about a lot of specific mechanisms and rules and things that are in place at the CIA, but there still is a line that has to be preserved, as we talked about, with secrecy. What's it like in your job to come up to that line and realize there may be something I can't tell you? And then how do you think about that?

MR. HUEBNER: It's incredibly frustrating. I think it's something that people don't realize about the secrecy rules. Like they are very much there for a reason. They're a cost. They're a necessary cost, but they're a cost. And it means that, you know, the inability sometimes to engage and to say, you know, with some of the NGOs that we work with, who have some very legitimate concerns, there are instance where with a sentence and a half I could say I understand why you're concerned, but actually you don't need to be concerned about that thing because it's not a thing.

MR. TRAPANI: But trust me.

MR. HUEBNER: But, you know, trust me is about as far as I can say, you know, without some of those secrecy concerns. So why can't I say that? Why can't I say your concerns about attorney-client information are actually really -- we have really good rules on those and I can give you the specific rules. Again, it comes actually back to people can have -- use those types of information to change their operations on the adversary side to prevent us from doing the work that we need to do.

So I like doing these types of engagements. I like talking to the public. But it is frustrating insofar as, again, we're not actually keeping the secrets from you. Or really

that's -- well, we are, but not for that purpose. And so when people have these very legitimate questions and you want to be able to answer them, but you know also that there's a line there.

I also have to say, though, it's fundamentally different than it was 5 years ago, certainly 10 years ago. Ten years ago my wife did not know what I did. She knew I worked at the Department of Justice for the National Security Division, end stop. Right? The fact that I was running some of the particular FISA oversight programs on programs that are now publicly known, but certainly weren't then, I could not conceive of being in this seat five years ago. And yet we now have folks who do this kind of thing, certainly not just me, at the CIA on a pretty much weekly basis, up on panels talking about whether it is China or cyber threats or procurement. We have people doing these types of engagements. So there is a shift that has certainly happened.

MR. TRAPANI: So speaking of legitimate but difficult questions, we're now going to open it up to the audience. There are microphones that will come to you. And I will be calling on you and maybe we can do a couple of questions.

Let me start with the man with two fingers up, suspiciously familiar.

MR. BARNES: Thank you very much. Julian Barnes with *The New York Times*. Thanks for doing this. Thanks for answering Ryan's questions.

Two questions for you. The first is on your transparency, and you talked about the balance of secrets and keeping secrets. In the current era, when foreign intelligence agencies are trying to influence entire populations, does that tilt the balance in some cases to revealing more about what you know because they are trying to affect an entire population? How does that current era impact you?

And secondly, and a more difficult question, there's been a lot of public controversy over whether the intelligence agencies were looking into the Trump campaign. Without compromising, talking about what you can't talk about, can you say, whether as privacy and in your role, did you after the fact review what the CIA had done in 2016 just to

ensure that it was in compliance with your U.S. person rules?

MR. TRAPANI: You want to take that or are we taking a couple more if you want?

MR. HUEBNER: So we can sort of see -- remembering the second one, I'm going for the first. The first real question was in terms of --

MR. TRAPANI: Covert influence in terms of the United States.

MR. HUEBNER: Yeah, covert influence. So I think actually the short answer for the first question is, yes, it does change. You know, we have had for many years, you know, for example, the Annual Threat Briefing where we talk to the American public about what those threats are. But you have seen other communications from the IC more broadly in terms of what those threats are and what a context and nature of them are.

There is still very much a line, right? We can't say something that is going to compromise our ability to continue to collect on that type of information. But to understand the scope of that threat of foreign influence and some of the things that everyday Americans, myself included, need to think about as we consume information, you can't actually effectively do that unless you have an idea of what the scope of the threat is. And I think to the degree you've seen more information come out about that, that's not accidental. That is an understanding that this is a different threat that requires more information to go out. Particularly, I'm sure, *The New York Times* would like more information to come out. That is your job to want more information to come out. But that, I think, it does change the calculus some on that.

MR. TRAPANI: It also -- can I just stop you there? Because I think there's another point to this question, which is -- or another element to answering it, which is that it also involves other people in making that decision. That is, you have a specific job enforcing specific rules, educating on certain rules. But then there's also a point at which policymakers come into play and it's not merely your decision or even the director of CIA's decision. It could be a presidential decision. It could be somebody else's decision.

MR. HUEBNER: Absolutely. No, I mean, it is generally actually not our decision at the CIA to determine in that kind of arena which information is the information that needs to go out. It's our job to collect that type of information and to present it to those policymakers and help them with that choice, but it's their choice in terms of determining how much information needs to go out. But I think you've seen a shift and for exactly that reason.

As to your second question, so I'm not going to speak to the scope of my particular reviews. I will say that the Attorney General Guidelines that I talked about before talk about the fact, and this is not -- this is clarifying, it is not new, we were -- always the case: CIA cannot collect, retain, or dissemination information to influence a U.S. political process, end stop. Like that is the rule, has been the rule, remains the rule.

MR. TRAPANI: How about in the back there? Sure.

MR. JAO: Hi. Thanks for speaking. I am Abraham Jao, intern at the Hudson Institute.

I had a question that was sort of underlying a lot of this discussion. You talked about your role as connective tissue, interacting with the public, and you spoke of the rightful public expectations at some point. What is your sense for why public citizens in the U.S. want this right for privacy if they could have more security at the expense of exposing personal information? Yeah, what's the sort of reason that people aren't as willing to share data in your opinion?

MR. HUEBNER: It goes back to the founding of the country itself. Right? Think about the reasons for the revolution. It was British soldiers coming into Americans' homes and taking information. It was the Stamp Act. It was the quartering, right? This is literally who we are is to think about this. And that is always true. That is true for Americans. That is true for the Americans who happen to be CIA officers. This privacy and civil liberties, this is not a tack-on. This is not an addition of a thing that we do. This is not a thing that takes away from mission.

Collecting foreign intelligence information against those threats in a way that protects privacy and civil liberties is the mission. It is how we define what it is to be an intelligence officer. It is what makes a CIA officer different from a Russia SVR officer. We have defined what it is to be an intelligence officer in the United States differently, so it is part and parcel.

So Ryan talked about my coming to the Agency three years ago. So that very first day that you become an officer, the moment actually, the particular moment you become a CIA officer is not when you get your badge. It's not when you get your assignment. It's not when you pass your clearance. The moment you become a CIA officer is when you go to our Memorial Wall and you stand up and it's the director or the deputy director in front of those now 133 stars as you swear a constitutional oath to support and defend the Constitution. Do not tell me that does not make an impact on people. It absolutely does. And every federal employee takes that oath.

I will say personally it has meant something different in this job at this Agency. And I have found that while -- and I will not denigrate any other agency who takes that same oath. But it is incorporated into the culture in a way that I haven't seen anywhere else. It comes up in topics as we discuss these issues about how this is going to -- how an action comports with that oath. It is literally how we define ourselves in this job.

MR. TRAPANI: Can I ask a follow-up question to that, which is -- I somewhat know the answer because we've talked about it in the past, about the idea of the tradeoff, of protecting civil liberties and being a more public organization than many of our other foreign counterparts and yet somehow, we still do the job.

MR. HUEBNER: Yeah. I mean, so I think in terms of the tradeoff -- Ryan knows that I hate the word "tradeoff" because in a lot of what we're talking about, what makes -- what is good privacy and civil liberties practice is also really good intelligence practice. Right? It is good intelligence practice.

The public demands -- think about this -- the public demands from us that

we are focused like a laser on our target. The public demands from us that we are objective in our analysis. The public demands from us that we protect information, for among reasons privacy information to not let it be compromised. The public demands from us that we be accountable for our actions. Those are the things that actually make us a really great intelligence agency.

This is why it's not a paradox that you have the U.S. intelligence agencies, very much including the CIA, who are simultaneously and really objectively some of the most restricted agencies in terms of what we're allowed to do and how we're allowed to do it compared to other foreign intelligence agencies. And yet also the most effective at what we do. The reason that's not a paradox is because of that public pressure to get it right. And people want us to get it right in all of those ways because they have those privacy and civil liberties concerns, because they have those concerns about national security. It literally makes us better.

And on the transparency front, I think that really is that shift, particularly to this new digital environment. I've certainly spoken many times to folks with some of our foreign allies. Some of them think we are a little bit crazy to be as transparent as we are. And that might seem somewhat shocking. I think probably many Americans say the CIA, not a very transparent organization. Our foreign partners look at us and think we have gone way off the deep end sometimes in terms of what we do.

We think it's critical. We think it's critical because of those public expectations on us, on what we do. We think it's critical because we have to be able to work with the private sector and others and they have reasonable reasons for wanting to know how we're going to protect information.

MR. TRAPANI: Up here in the front.

MS. VINCENT: Thanks for your insights today. I'm Brandi Vincent from NextGov.

I was wondering if you could elaborate on the work you've done with data

scientists and how you're harnessing emerging technology to do your job better in today's age.

MR. HUEBNER: Sure. Our conversations with our data scientists are actually some of my favor parts of the job because you've got this very dedicated cadre.

Let's start, what is data science? This is a word that's come up a lot recently. And it's this very interesting amalgam of things that were already out there but are now put together much more importantly. So some of it is statistics, some of it is coding, some of it is graphical representation. Some of it is utilizing these new analytics that we have, particularly for large datasets, to look at information in ways that we weren't able to do before and to use kind of improvements in machine learning to see insights that us humans just from a capacity standpoint we can't see.

We at the Agency have over 100 AI initiatives that we're working, and that's going to continue to be the case. I think people look at AI -- I don't like it actually when people look at AI as something so functionally different. To me this is a little bit like in the '70s, '80s, we're going to start using computers, right? Or in -- not for us, we weren't around then, but for the FBI in its early days we're going to start using cars. This is one of the tools that is going to be used in a lot of different places.

The interesting and fun work with the data scientists that we're doing is, great, everyone wants us to think about bias. What does that actually mean? What are you actually asking us to do? What are the questions that we should be asking ourselves as we look at a dataset? Particularly interesting in a place like the CIA where, let's think about it, for AI -- AI often works better with very large datasets. The CIA is authorized to collect foreign intelligence information. We are not authorized to collect data solely for the purpose of making our AI better. That's not something we have the authority to do. We are allowed to use the information that we have properly collected.

We also might, in certain cases, purchase things from the private sector. But when you're thinking about things like bias, the training data, how you train that machine

learning analytic, that's where some of the bias really can seep in. So you really want to know about that training data.

Now, at the same time, you might not want CIA to have that training data. Right? It might be very private information that has no foreign intelligence relevance but is useful for the analytic. So we simultaneously say I don't actually want that information, it doesn't come within our ambit, but we need to know things about that information because we need to account for bias certainly for privacy and civil liberties, but also for the rest of the mission. If we get something -- accuracy wrong that is a mission problem and that is a privacy and civil liberties problem, that could be a threat to our own officers and what they're doing.

And so those are really fun topics. And I think to me, what I'm looking to do and what my officers have been looking to do is as we think about those, not develop this in terms of a set of here are 8, 10, 12 ethical principles that look fabulous on the wall, like the Ten Commandments. But instead, from a practical standpoint, what's the framework that you're going to use when you have a new project? What are you asking yourselves to say if I'm going to deliver this analytic for mission use, it's not done yet unless I have thought about these things.

And really critically, what are the questions not for the data scientists, but for the people who manage the data scientists? What do they need to know and ask of those folks to ensure that the analytics that they have is going to really meet that mission need?

MR. TRAPANI: Great. So I just want to wrap it up here. And I just want to say thank you to the staff at Brookings and the staff at CIA for helping us put this together. And most importantly, thank you to Ben. I'll let you get back to those interesting questions now. But to the audience, thank you for coming. And to Ben, thank you for participating.

MR. HUEBNER: Thank you, Ryan, and thank you.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

ANDERSON COURT REPORTING
1800 Diagonal Road, Suite 600
Alexandria, VA 22314
Phone (703) 519-7180 Fax (703) 519-7190

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020