THE BROOKINGS INSTITUTION

THE RISE OF AMERICA'S SURVEILLANCE STATE

Washington, D.C.

Thursday, March 11, 2010

PARTICIPANTS:

Moderator:

BENJAMIN WITTES
Fellow and Research Director in Public Law
The Brookings Institution

Featured Speaker:

SHANE HARRIS
Homeland Security and Intelligence Correspondent
National Journal

Discussant:

KIM TAIPALE
Founder and Executive Director
Stilwell Center for Advanced Studies in
Science and Technology Policy

* * * * *

P R O C E E D I N G S

MR. WITTES: So I think we're going to get started. Before I forget to say it, please turn off cell phones and blackberries, or at least the ringers. And in this forum, I suppose I should say that if you don't, we'll know.

So welcome to the latest Brookings Judicial Issues Forum. This is a somewhat unusual one for us. We normally don't do, you know, events for narrative books, you know, we usually do these sort of public policy books, you know, and arguments and studies and what not, and this is a little bit of a change of pace, because Shane's book is actually the story, you know, told as sort of a – as a, you know, in an almost novelish forum, although all the facts are true, of kind of a development of a technology or a set of technologies and a set of public policy problems that arise along side those technologies, in the context of a developing confrontation with global terrorism.

So I met Shane – I'm Ben Wittes, by the way, a Senior Fellow here in Governance Studies, and I met Shane a number of years ago when he called me up one day and asked if he could talk to me about the Foreign Intelligence Surveillance Act, which is little old hobby horse of mine that I've sort of spent a lot of time on over the years. And then, as know, I get a lot of calls from reporters on the subject, and generally speaking, you know, I'm an ex-reporter myself, and I don't mean to be dishing dirt on the profession, but generally speaking, this is a very hard statute to understand, and relatively few people actually make the effort to understand it, and among the relatively small number who do, a relatively small number do so successfully.

Shane had an understanding of both the law and the technology underlying the law that was evident in about, I don't know, 30 – 40 seconds of the conversation's beginning, and was just qualitatively different from anything that I had run across, and somebody who reports on this stuff, and I was – we've been friends ever since.

And he began shortly after that conversation working on this book, which was – admittedly seems like an odd counterintuitive project, which was a look at the history of data mining with the hero was John Poindexter. And the – if that sounds provocative or counterintuitive, I would urge you to read the book actually, because I think what it reveals is that the people we think of or sometimes think of or instinctively think of as the bad guys in this conversation are complicated, sometimes very complicated, and the problems are excruciatingly difficult, both from a technological standpoint, and from a moral standpoint, and from a legal standpoint, and from an operational standpoint.

And so what wanted – what I've asked Shane to do is to come here and talk about, you know, outside of the realm of the sort of standard book talk about some of these things, just talk about some of the public policy problems that underlie the book and what gave rise to this, you know, this set of questions that he took a look at in this.

Shane is, in his other life, his day job; he's a reporter for National Journal, where he writes about intelligence matters, technological and non-technological. He recently wrote a very long and very involved and very influential piece about legal objections to the Predator Program, which I would commend to you all.

He's been named twice as a finalist for the Livingston Awards for Young Journalists. And his work has appeared kind of all over the place. And I've asked to comment on the book and on Shane's talk Kim Taipale, who is a – one of the most interesting voices in this entire conversation. I first ran across his work a few years ago when I was writing my book, and I was trying to figure out, you know, what's the – if you wanted to really be disruptive in this area and kind of not buy the orthodoxies that drive the conversations, what would that look like. And I ran across a law review article that he had written about surveillance in – about warrantless surveillance as analogize to stop and frisk – stop and search, police searches under a case called Terry, an old Supreme Court case.

It was one of the most eye opening pieces of legal scholarship I have read on this whole subject before or since, and it greatly influenced the way I think about the subject.

Kim is the Founder and Executive Director of the Stilwell Center for Advanced Studies in Science and Technology Policy. He's also a Fellow at the World Policy Institute and an Adjunct Professor of Law at New York Law School. And he serves on the Markle Task Force on National Security in the Information Age. And he will be offering thoughts after Shane speaks about the subject and about the book and about whatever else may be on his mind. And then we will have a discussion with you guys at that point. Thanks.

MR. HARRIS: Thanks, Ben, very much, and thanks to Brookings for having me. This is really an honor to be here and to discuss the book with all of you. As Ben said, this book really is a narrative and it's a story and I like to sort of equate it to a non-fiction spy thriller, I don't know if there's ever been such a thing, but that's sort of how I approached it in my mind.

And one of the reasons for that was, I thought that perhaps the best way to sort of illuminate a lot of these abstract issues of technology and some of the more difficult legal and policy problems surrounding things like data mining might be to do it through a human story and to make that more accessible to a broader audience that way.

But I do want to focus today, as Ben said, really on a lot of just the policy issues at play here, and it sort of undercurred the entire story of the book, because these are not necessarily new issues, as I'll explain here in a few minutes, but they sort of present new problems based on the evolution of technology.

So the way to sort of frame this as a policy matter I think is maybe first actually to start with the people in the book and to give you a sense, first of all, for just who the Watchers are. And the Watchers is a title that I've given to five people who are sort of the centerpieces of the book that have spent the last 25 years of their careers working either in the intelligence community or the high tech industry and often both, and they share this common theme, and that is, a dream, I would say a somewhat elusive dream, of being able to build a technological system with the capacity to ingest large amounts of electronic data and then to filter through it or to mine through it, if you like, for patterns of activity that indicate a terrorist plot in the offing.

We're talking about people who are trying to, broadly speaking, connect the dots about terrorism and national security crises using electronic data and information technology, which is increasingly more powerful, just as the amount of data increasingly gets larger and larger.

So the Watchers are really the people who have been doing this for the past quarter century. And as Ben said, John Poindexter is sort of the chief Watcher, if you like, among them. And I think that if you understand a little bit about his past and the main issues that he worked on, it's a good way of sort of diving into what is the conflicts that are at the heart of this policy issue. Most of you will remember Poindexter, of course, as the architect of the Iran Contra Affair, from his perch as National Security Advisor to President Reagan in the mid 1980's. What a lot of people don't know is that Poindexter actually came to the White House on a technology mission.

He was brought over in 1981 by the National Security Advisor as a military aid to the NFC staff, and his job was basically to modernize the situation room.

We have this picture today of the situation as being this kind of this nerve center 24 kind of style operation, and back then it really was sort of a technological backwater. And Poindexter was the guy who brought in modern communication lines and data encryption and video teleconferencing systems. He actually introduced email as we know it to the White House, which eventually ended up playing something of an ironic role in his involvement in the Iran Contra Affair.

But nevertheless, he was a brilliant technician and a systems thinker and was also somebody who was very interested in national security policy, and suddenly found himself in a position to influence that vis-à-vis his position on the NFC staff. But where I became interested in him was in the second career that he had in government after 9/11. He had spent the previous 15 years working as a contractor, mostly for the Defense Department, and after 9/11, came back to government with an idea for building a system that was essentially the kind of system that the Watchers have been looking for all along, something that could go out and create virtualized data bases, go out and touch information and mine it for these patterns of activity that we're talking about.

He called it total information awareness, which arguably was probably not the – maybe a catchy name, but from a public relations standpoint, maybe not the best, but nevertheless, accurately described this vision that he had of being able to get access to all relevant information to terrorist plots.

I was a technology reporter at the time working on a magazine here in Washington, so I was very intrigued by this idea that he had, and it was sort of premised on two ideas. The first was that, while it was true that before the 9/11 attacks, the government had access to a large amount of data on Al Qaeda and these particular terrorists both held in the data bases let's say of the CIA or the FBI or the NSA had its information, all this data was siloed and it had not been fused together. The CIA was monitoring some of the terrorists abroad, the FBI was monitoring some of them here, the right hand was not talking to the left, so we understand this theme that developed not long after the attacks, and that had a technological component.

But Poindexter's rationale, and I think not illogically, was that once the hijackers were here, they were moving around in a public space, they were opening bank accounts, they were transferring money, they were renting apartments, they were renting cars, they were traveling on airplanes, they were communicating with each other using the systems that we all use every day.

And to accurately predict or to forecast their activity and their plans, the government needed to get access to that private information, as well. So this was the sort of grand vision of TIA that, at the time, I think went farther than anyone had proposed, at least had dared to say publicly, in terms of how we could do data mining, information sharing, and intelligence gathering better to predict the next 9/11.

There was a second component to this plan, though, that is often overlooked, and I spent quite a bit of time on it in the book, and it presents a very interesting policy decision I think on Poindexter's part. He recognized, I think, that this kind of far reaching data gathering and analysis effort was not only going to make people uncomfortable, but would probably challenge not only our notions of privacy, but might even require substantive change to privacy law if it were to be implemented.

He wanted to have a policy debate on these issues, which was unusual given the place where this research was being conducted, at the Defense Department, at DARPA, their R&D agency. It's not a place where policy discussions often happen; this is sort of the realm of techno geeks and of technicians like Poindexter.

But his proposal was to actually use the very kinds of technology that was capable of gathering and analyzing information on all of us effectively and to turn it back on the Watchers themselves, to actually create audit logs that would recognize every key stroke, every file that was accessed by a government analyst and make a record of that that could not be deleted, and to actually use the pattern sensing technologies and capabilities if you like of TIA to sense if somebody in the government was accessing information inappropriately. He also wanted to use data encryption to effectively anonymize information in these vast data bases that he was going out and proposing to touch, and actually imagined a system whereby an analyst sitting at its computer screen looking at information ingested by TIA would not actually see names and maybe not even location of the people attached to this data, he would merely see patterns of activity based on what kind of plots they were trying to decipher, and that only under order of a judge could someone come and unlock this information and actually see the people underneath it.

So these two fairly radical ideas of how do we gather and collect and analyze information and how do we use this technology to sort of maybe not redefine our concept of privacy, but certainly redefine our process of oversight when it came to these kinds of issues.

I found that to be utterly compelling, both for its ambition and its – but obviously also because of the man who was proposing this. I mean I think it’s fair to say that John Poindexter is not the poster child of public trust and confidence. And I was intrigued as a reporter what it was about him and this idea that was so compelling that he was basically willing to court this kind of public debate and make himself the lightening rod for it, if you like. To fast forward a bit, it’s fair to say this plan is not met with great enthusiasm by the public. After it becomes widely known what Poindexter is up to, and it was not a classified project, I should add, the outrage of it is palpable, it’s intense, and he doesn't survive it. At the end of 2003, by the summer of that year, Congress has publicly defunded the TIA program and Poindexter resigns and goes back into private life.

Now, it was about six months after he left that I actually got the opportunity to meet him at a conference that we were both speaking at in Syracuse on homeland security, and I approached him and asked him if he would be willing to actually sit down for an interview to talk about these issues.

He had actually denied all my interview requests the previous year and a half or so. He was under orders from Don Rumsfeld not to talk publicly about TIA or to make any public statements at all.

And he actually said that he would do this on one condition that he would do the interviews on one condition, and that was that I had to come out to his house in Maryland for several interviews for several hours each and they would all be on the record. Now, it has been said that John Poindexter, one of the reasons that he did not fair well in the aftermath of Iran Contra is because he didn't really understand how the media works and how journalists operate. And it was after this proposal that he made me that I realized that this was true. Because anyone who understood what makes a reporter tick would realize that an invitation to come out to the home of one of the most notorious and enigmatic political figures of the past quarter century is actually inviting, it's not an onerous task, and I think perhaps he viewed it as something of a test.

Needless to say, the interviews did occur. And I wrote a profile of him in 2004 for the magazine I was at at the time, Government Executive, and then eventually these interviews kind of morphed into a series of discussions over the years that formed the narrative crux of the book.

And without going into all the, you know, the colorful details of that kind of Tuesdays with Maury-ish experience that we had, it's safe to say that in diving into what it was that was driving him and this post 9/11 environment, that it didn't begin for him on 9/11, that as a policy issue, this question of how do we harness information in government systems, or wherever it resides to try and see the future, has a much earlier sort of starting point in the narrative. It actually goes back to 1983, October 23 of 1983 specifically. This is where the story actually begins in the book.

Many of you will remember that President Reagan had deployed the marines to Beirut to act as a peacekeeping force amid the civil war there, and most of the marines were encamped at a base at the Beirut International Airport.

On the morning of October 23rd, a suicide terrorist drove a truck laden with explosives into the barracks and killed 241 marines, most of whom were asleep at the time.

This was actually the introduction I think for most Americans on the concept of religious suicidal terrorism. They hadn't seen this kind of a strike before; this was something quite novel which we perhaps take for granted today.

At the time, it fell to Poindexter, along with a number of senior Intelligence and National Security Council officials to kind of figure out how this happened, how this surprise attack on the marines was pulled off. And what they found sort of bears an eerie parallel to the narrative pre-9/11. There were signals that were missed, there were dots that were not collected, there was information being collected in silos and not put together. Just to give you a quick example of this, from the spring of 1983 until October of '83, the month of the bombing, the Intelligence community actually fielded more than 100 individual warnings about car bombings in Beirut. None of them were fused or passed on to other relevant officials who might have an interest in this.

The U.S. Embassy was actually bombed in the spring of '83; more than 60 people were killed, including most of the CIA station in Beirut. FBI forensic investigators examined the bomb and determined that it revealed evidence of a highly sophisticated terrorist outfit working in Beirut directly targeting American interests.

And a third piece of very telling information, the National Security Agency, the chief electronic eavesdropper in government, intercepted a call from an Iranian official at the Embassy in Damascus to a terrorist operative in Beirut ordering a group there to undertake a “spectacular strike” against the marines in Lebanon. This information was never shared with the commanders at the airport base so that they could fortify their defenses. So Poindexter kind of becomes at this point, along with a number of senior officials in government who go on to have long careers, kind of to run up, I guess you could say, the first contemporary approach at counterterrorism policy in government. They start trying to lash together the systems of the CIA, of the military agencies and commands of the Defense Department, they start trying to put data together, they start trying to form new committees of people who can get together to start planning across government to collaborate on how to respond to terrorist attacks before they occur.

This is something that we recognize as I think a post-9/11 activity, but it is not a phenomenon of those attacks. This, in fact, goes back really to the emergence of suicidal religious terrorism against the United States.

So with that in mind, I kind of, as the narrative began to take shape, saw 9/11 really as a mid point in this discussion, and Poindexter kind of having been there for the beginning in ’83, but it isn’t really until the 9/11 attacks that we start to see this need for security and for better intelligence, start to run head long I think into deeply held notions of privacy and privacy law specifically in this country, and specifically laws around this kind of electronic surveillance itself.

This is the point I think in the narrative where Poindexter kind of finds a parallel or a foil, if you like, in a very similar program that was going on at the time at the National Security Agency, something very similar to total information awareness.

Most of you I think will probably be familiar with the New York Times, a great piece in December of 2005 that exposed the fact that the National Security Agency was engaged in what's known as a warrantless wire tapping program, that's what it colloquially was referred to.

Just to give you a sense of the narrative that leads to this and then how it ties back into Poindexter, because I think this really illustrates this fundamental tension that we're still dealing with right now between security and privacy; it was shortly after 9/11, of course, that the NSA realized that it, too, had missed many of the signals and the warning signals of the attack. And at that time, Michael Hayden was the Director of the Agency, and under his authority, and under existing executive authorities that the Agency has been given years earlier, began to broaden the aperture, as he's later described it, of the kinds of surveillance that NSA was doing. And specifically what they were trying to do was go up on numbers, phone numbers and communications of known or suspected terrorists to try and figure out were they connected to these 19 guys who had just blown up buildings in the United States.

It doesn't take long at this point for Hayden to come to the realization that the kinds of surveillance that NSA is doing is not, in his view, going to cut it, it's not going to be enough to gather the universe of potential intelligence out there and develop an early warning system for terrorism.

So in October of 2001, he briefs the President and the Vice President on the plan to essentially widen this lens even more and to start intercepting the international communications of suspected terrorists both coming into and out of the United States.

And the conditions that were placed on this would be that as long as one participant of the communication was located in a foreign country, not in the United States, and there was some “nexus to terrorism” was the word that was used that was determined by the intelligence agencies, then NSA could do wire tapping, if you like, surveillance for content of the communications, absent a court order from the Foreign Intelligence Surveillance Court, which is normally the body that oversees this process of intelligence gathering through electronic surveillance.

It’s safe to say, I think, that this programs grows very quickly, it morphs actually into something that goes beyond pure wire tapping or monitoring for content of communications and evolves into the collection from telecommunications companies of what is known as meta data, or transactional data about telecommunications.

You see this kind of a report showing up every month in your mailbox as your phone log essentially. What NSA was looking for was information on who is calling who, who is communicating with who, where are they, how long are they talking, what are the patterns of this electronic activity, and can we look at that and try and discern some sort of signal that tells us when terrorists are communicating with each other.

Well, this is very similar to total information awareness. This is essentially the operational version, on a smaller scale, of what Poindexter had been proposing in public, except that NSA, of course, was doing it in secret. The story at this point sort of merges together, and I’ll just take a second to – the interesting narrative twist. TIA was publicly defunded in the summer of 2003. This is after, I should say, that Michael Hayden and John Poindexter had had at least one meeting with each other discussing how they might work together and sort of cautiously viewed the other.

Poindexter had no idea what Hayden was up to behind closed doors; Hayden, of course, knew everything that Poindexter was doing because it was public.

But Congress defunds this program of TIA in the summer of 2003, but leaves essentially a back door in the Defense Appropriations Act for funding to continue in secret in the Intelligence budget.

TIA is broken into component parts, and they are absorbed as a research program by the NSA, by an R&D outfit working for the National Security Agency actually based at Fort Meade in Maryland.

The most significant part of the research, however, that is not picked up by NSA is Poindexter's research into privacy, into what he called a privacy appliance. This would be the thing using the data encryption that I was speaking about earlier. And I think that it is most telling that at a point when this agency that was actually engaged in the kind of work that Poindexter was talking about had an opportunity to pick up not only all of his research and the data collection and the analysis base, but also the privacy research, and essentially said no thanks.

It's what happens next that I think sort of deposits us to the where we are now kind of conclusion, and I'll briefly go through NSA's experience in this sort of nebulous world of data mining that they've been in for several years now.

Once they picked up the TIA program, what they found was that the tools that Poindexter was developing for data analysis were actually not going to be sufficient for their needs.

There was a very telling anecdote that someone told me about when analysts at NSA tried to take some of these experimental data mining technologies and use it secretly with information that they were collecting from the telecommunications companies, they were putting so much data through these systems that they essentially crashed, they fried the circuits, and that's sort of a lay way of putting it. But suffice it to say that NSA was collecting so much information that discreet kinds of technologies to detect patterns were not working on it. They needed some way to sort of massively display information. They kind of became, I think, sorry to say even obsessed with this idea of trying to display connections among this giant universe of information that we're collecting.

There was one technology in particular that analysts became quite enamored of, it's known as a graphic visualization tool. There's a picture of this actually in the book. And what this does is, it takes all of this data that NSA is collecting and it displays it as a series of dots on a graph representing people, places, events, and then tries to show with lines how those dots are connected.

Well, if you look at the photograph, you'll see that there are actually so many dots and lines that it looks like there's this explosion of rays and massive of lines overlapping each other that to, I think, you know, to a lay person would seem almost impenetrable and indecipherable.

Critiques of this approach actually developed a nickname for this technology; they called it the BAG, which stood for the big ass graph. The BAG kind of became the moniker among people who were really suspicious within the NSA circle and technology circle about this approach to trying to swallow all this information and try to find patterns in it. It seems to me that NSA is sort of urged to do it this way as opposed to trying to find discreet patterns in the data, which is what Poindexter was doing. It's really sort of, in part, a bureaucratic instinct. There is certainly an instinct after 9/11 to collect as much information as possible and leave no stone unturned, because what if that one data stream that you weren't looking at becomes the one that had the telling signal about the next attack.

Then it's also fair to say that, in a bureaucracy, information equals power. And NSA, I think, obviously, has probably the most information of any agency and it exercises considerable leverage within the bureaucracy because of that.

This kind of compulsive need to collect and to hoard information is something that, I'm afraid, has spread across the intelligence community today. And what we've arrived at, I think, is a situation where we have created an official regime of surveillance, at least for foreign intelligence purposes, that is very good at collecting dots and really not very good at connecting them. From a policy perspective, there are two big consequences, as I see it, to this over collection and under connection. On over collection, the first, of course, is that you risk a massive invasion of peoples' privacy, that you're monitoring the people who you shouldn't be looking at.

We know that this has happened at least in one case. In January, 2009, it was revealed that NSA, in the course of trying to monitor foreign target email conversations, inadvertently collected the emails of thousands of Americans, who, by law, they were not supposed to be targeting at that point without a warrant.

The failure to connect, though, it seems to me, is one that's also pretty to grasp immediately, it's the risk that you miss or the intelligence agencies miss, as they have in the past, the signals of the next attack.

Briefly, I think we saw this happen on the Christmas Day bombing attempt. As most of you know, of course, on December 25th, Umar Farouk Abdulmutallab, a young Nigerian man, boards an airplane from Amsterdam to Detroit with an underwear bomb strapped to him, tries to blow up the plane, he fails. In the aftermath, we immediately find that, again, there were signals that the government had missed about this event that were never fused together. Abdulmutallab's father had shown up in the U.S. Embassy in Nigeria in Nabooja in November of 2009 saying he was afraid that his son had gone to Yemen to join the ranks of Al Qaeda radicals there. The NSA separately was intercepting the phone calls of Al Qaeda and the Arabian Peninsula operatives mentioning a Nigerian who had been employed for a yet unspecified attack.

And after Abdulmutallab's father went to the Embassy, officials there sent his name, the younger Abdulmutallab's name, to the National Counterterrorism Center outside Washington, where it was added to a data base of known or suspected terrorists. And very little attempt was ever made at that point to determine whether Abdulmutallab had been given a U.S. Visa and was either on his way to the United States or possibly here already.

Here in microcosm I think we see the problem. On the one hand, the analysts at this center who are today responsible for trying to connect the dots of these attacks are literally drowning in information. Officials have told me that they estimate they receive between 4,000 to 8,000 names per day that they're expected to follow up on in some way, names of people who might be connected to terrorist attacks. The master data base to which Abdulmutallab's name was added contains today over 500,000 names or aliases of known or suspected terrorists. I've talked to people who work on these data bases, and even they will tell you that that cannot be an accurate list, that it is too large, and it's simply too large for their purposes, that they're drowning in information today.

There are 28 different data networks to which analysts at the NCTC have access, and within that, over 80 different intelligence streams, they call them, of unique reporting and products of intelligence.

The connection technology, to make sense of all of this, doesn't really exist, at least not in the way I think that it should. There is no Google for intelligence today. You cannot sit at a terminal and type in the name Abdulmutallab and instantly know everything the government has on this individual.

So this is the conundrum that we face, very good at collection, not so good at connection, and this is what I mean when I say we're witnessing the rise in the United States of an American surveillance state. And I use that phrase with some trepidation because I think it conjures up images of DiStasi in East Germany, and that's not what I mean to suggest is happening here. But what we have is a system where it is the default position, I think, of government agencies to collect data on a massive scale and to put off the question, much harder question, of how do we make sense of it. And privacy I think has become something of a secondary concern in this, not out of a disrespect for privacy, but I think perhaps a recognition on the part of the intelligence community that it could slow them down if they try and build in the kinds of protections that Poindexter was talking about and that others have proposed, as well.

I propose in the book that we actually consider perhaps a radical policy change here. It might be time to accept the fact that technically and legally speaking, there are very few impediments to government agencies, or anyone for that matter, collecting any information that they want. That's not 100 percent true in all cases, but broadly speaking, information is obtainable.

And our laws have focused I think excessively, given the current state of the problem, on the acquisition of information, and we have paid relatively little attention to what is done with that information once it is collected. I don't know whether or not John Poindexter had the right solution to this, and we part ways on a number of his ideas and the pursuits that he had, but what I do know is that he courted this debate publicly in a way that I've never seen anyone do then or since, and I think we missed an opportunity there to have these very difficult discussions.

I think that now, in the relative calm between the last great attack and what I think inevitably will be the next one, is the time to have this discussion, to ask these hard questions. And I think that we put off that moment at our peril.

Of all the people I interviewed for the book, and I interviewed hundreds of people in and out of government over the years for this, regardless of where they fell ideologically on the spectrum or their views on this issue, on one point they all agreed, and that was that in the aftermath of another attack like 9/11 in the United States, this question of how do you balance security and privacy, security and liberty, will become an academic discussion.

The government will come down decidedly on the side of security that is exactly what they've done in the past. I think then you will see intelligence gathering that is driven by exigency, by fear, and that you will see perhaps infringements on privacy and liberties that many of us have only imagined or feared could occur at this point. Simply put, if we don't have this discussion now, I think the government will collect first and ask questions later. And if and when that happens, I don't think it should come as a surprise to anyone. Thank you.

MR. TAIPALE: Hi, so a couple things, you know, the best part to start the policy debate, obviously, is with the last thing that you said, Shane, but I'm not going to do that, I'm going to go back and talk a little bit about the narrative first and my own personal reaction to it and go through some of the points and hopefully end up at the same place that you were.

One of the things that struck me when I was reading the book, first I should say, I was at every meeting almost that is in the book, the Cantini meeting, the Syracuse meeting, the Heritage Foundation meeting, I mean all these meetings, and as I was reading the book, actually I guess this was an ego problem, too, as I was reading the book, I kept waiting for my name to pop up, and I was really dreading that actually because I wasn’t sure how that was going to play out, because other books – hasn’t always been pleasant. But I got through the book and it never popped up. And my first reaction was, oh my God, why didn’t he mention it, and then I realized, I represent the radical center, and probably alone represent the radical center in this debate, and part of the problem is that, and I think not just the problem in the debate, but the problem in how it’s played out is that there’s sort of two camps, and one is sort of in charge of what’s happening at one time and then the other and it goes back and forth, and sort of the center of the debate really hasn’t happened in the public. So that was my personal reaction to the whole thing.

I mean I will – just another anecdotal thing on that, so it’s – I testify in Congress occasionally on things like this and on Pfizer reform and stuff, and one of the interesting things is, I sometimes am called as a democratic witness, and then the republicans attack me, and I’m called as a republican witness, and the democrats attack me. They finally caught on to that, so I don’t get invited anymore.

But the point is that you really, you know, the center of the debate is missing, I think, and that really struck me a little bit in the book also. So let me actually get to the issues. And I should also go back, on TIA itself, and I’m in agreement here with you, I actually wrote in 2002/2003, before TIA was defunded, that I thought the defunding of TIA was actually going to be a victory for privacy, that the result of that would actually be that the programs moved into the classified budget, we wouldn’t have the public debate about privacy. That happened in my – from 2003, not the one you mentioned.

There's a footnote, and I actually reference where in the classified budget I thought the programs were going to end and it turns out that's where they ended up.

So one of the – but let's go back and talk about TIA for a second before we put it in the policy context. Although I agree with a lot of what Shane said, you know, and I certainly agree with Poindexter's big idea that drove his interest in participating in the process.

TIA itself was actually a collection of programs that existed within DARPA, and many of them were not controversial, I mean many of them were technology programs aimed at automatic translation of documents, and you know, other things like that that really weren't controversial, and this was the aggregation under which, the sort of big idea under which these programs came together and made sense to sort of manage, just a purely bureaucratic thing. And also it's important to remember, TIA was not a collection program. Although it was driven by this idea that this data existed and somehow we could learn stuff from this data, TIA was intended to develop tools to do the analysis, to actually do the connecting of dots, it was not about collection.

And one of the problems that happened here in this – in sort of the shift that you talk about between TIA and TSP, the Terrorist Surveillance Program that the NSA owned, is that actually the TSP is driven by collection, and TIA was driven by tools and – developing tools for analysis, and that by killing TIA, not only did we lose the ability to have the debate, put the programs in the classified program where they could happen without sort of oversight, but we also really lost the bigger picture of analytical tools, and the analytical tools that were then developed in the classified programs to support the collection business were different than if you had the tools, really what is the intelligence process that you're trying to further, which really is this connecting the dots point.

You know, a word on the privacy thing, you know, again, this was – you’ve got to remember, TIA was a very public project, more public than many other DARPA projects. Poindexter went – this whole thing broke in the public basically when DARPA – I mean when Poindexter went to San Diego in 2002, a DARPA tech, 2002, and made a public speech, and part of the public speech was very specifically to engender the privacy debate.

I mean he brought privacy up, he asked for the privacy – the people that are concerned, you know, the – privacy groups to get involved in the debate, et cetera, et cetera, and that’s what sort of led to this sort of thing, and I think, to some extent, then led to a misunderstanding of what the project really was, and then a demonizing of it because the debate was so polarized and not really a discussion of what was going on and what we needed to do; as we see, we still haven’t done in the sense of not being able to connect the dots in the latest Christmas bombing thing, although I have a word or two to say about that.

The other thing that’s interesting, and again, in a lot of these meetings, these early meetings when Poindexter was presenting this, it was actually very interesting, he had a slide, a slide that I’ve stolen from him and I use actually to illustrate this point, but, you know, he had this sort of vision of the big idea and how things came together and where analysts was done and all this kind of stuff, and then he had a very prominent bubble on this chart that said privacy appliance, and it was right there. And in subsequent conversations, including at the continued reading, Barry Stiffle from the ACLU got up and made a big point, oh my God, you know, this was his view of dealing with privacy; he put a bubble on the thing.

But, you know, if you actually think about that in the context of technology development and everything else, that – from a technologist point of view, and I am a technologist to some extent, from a technologist point of view, that is the privacy answer, put a bubble on the chart and build an architecture that has a place to have the policy debate in it, have an architecture that allows for that debate to happen in the public policy and then it be applied to the technical system. That is actually the way that you do that.

You have a requirements document, you put the thing in, and you put – you label the parts that you want people to put their input into. And so, you know, I saw this very interesting dynamic play out, and particularly in Cantini between Poindexter, you know, the security side of this debate and the privacy side of this debate, where it really came down to this, oh my God, this is horrible, because you haven't filled in the bubble, obviously you're not concerned about privacy. I just think it's very, you know, again, I mean I'm sort of a systems, you know, to the extent that I call myself anything, I'm a social theorist, and I like to watch how people make decisions, and particularly how the bureaucracy in Washington tends to make them poorly, and this was one of them, because people were absolutely seeing this chart in completely different ways.

Every technologist or anybody who understood technology development in the room, and even a lot of the lawyers and stuff, who understand the sort of development process, completely understood that just having the box there was, you know, important, was about having that debate. And on the other side, the people who were concerned about the outcome of that debate couldn't live with a box that didn't have those answers in it.

And I should – a couple other words about that privacy debate, particularly early on. We've come to – and this actually came out in the debate over TIA and some of the other programs that came out of TIA, particularly the terrorist – the future markets, which was this idea that, how do you take crowd sourcing in to sort of make predictions about the future, which we see throughout the economy, people are doing it through everything else, and in this case it was to be applied to national security problems, which also translated into terrorism problems, and obviously, when that became public, the politician's view was, oh, we're going to bet on terrorist events, and that's horrible, and blah, blah, blah.

But actually, and I can't remember who it was, you may know, the Washington Post did an editorial that actually said, you know, this is actually an interesting process, because I mean they were against the whole – and everything, but the point of the editorial was really, you know, before we kill all these programs, we really ought to think about it, this is sort of anti-American, I think was the bottom line of the editorial, that we kill a project because we're not willing to enter into research and development that can't promise zero defects before it actually occurs, and that that's very different than the sort of classic American approach to innovation and sort of taking risks and figuring out how things work.

And I'm not arguing in favor or against these programs, I just – the process is actually one that I find very interesting. I'll mention this anecdote, because you just reminded me of something when you said that, you know, you were – government exec at the time. Two weeks ago – three weeks ago, I gave a talk somewhere, I can't remember now – I think, but I give a talk, and one of the points I made – we were talking about the Christmas bomber thing in particular and the inability to connect the dots, and one of the points I made was that, you know, it's really interesting, because if you read President Obama's tasking order, you know, they did this after action report which is like a six page document, here's what went wrong, and then there's a three page tasking memo to the Secretaries of Defense and intelligence community, et cetera, here's the things I want you to do, and one of his orders in the tasking order, I read it out loud, you know, I read it, and it was about developing the technologies to connect the dots.

I mean it's a long paragraph and it goes through the thing. And I said, you know, it's really curious, because essentially this could be the mission statement for TIA in the tools development side. And I was thinking that it was a positive thing, I was thinking, you know, it's about time we're getting back to the debate about the tools and about applying them. And the question about what data to apply them to is a completely separate thing than developing the tools to be able to actually use data to our advantage.

At some level everybody agrees we should do this. I mean even the ACLU will say we should have the tools to connect the dots in the intelligence data bases. Now, the question of whether you – what data goes into those intelligence data bases is a very important conversation, but it's completely separate from developing the tools.

So I was making this point that, you know, it was really great, I'm glad to see after eight years, you know, the President is finally ordering that we develop and apply these tools. Again, these are foreign intelligence – government exec, the next day, headlined is, security expert says Obama revised controversial Bush program, okay, which actually was sort of great for me because the White House actually had to respond to something that I didn't say, it was great.

So the next day the headline was, you know, Obama Administration says, oh no, we're only doing this in foreign intelligence, not against – but it really illustrates my point. There are two different issues, the development of the tools and capacities and capabilities to do certain things, including the analysis part. Again, I'll talk about collection if you want to as a separate issue, but the analysis part – versus what data you put it against, which is the collection issue.

And I think I agree with your final statement, which is, you know, all of our rules and all of our policies are premised on regulating collection. That battle is over, kids. I mean the data exists. We're not going to live in a world where, under some circumstances, data that is actually relevant to a national security investigation is not going to be – we're just going to arbitrarily say, well, you can't use it, what we have to do is develop the rules under which we can use it.

The data exists out there, it's getting worse and worse, it's not just, you know, IT, and the development is now, and the sort of computers that we think of, you know, the computers issues is actually last year's debate, you know.

I mean the next one is, you know, when people start reading conversations off the vibrations in the wall, I mean not the type of stuff that we do now in real time off of Windows, but come in this room tomorrow and read the nano vibrations on this wall and hear what I said, having been recorded on any device that a man made. We're moving into a world where that's going to be more and more possible. And so information is going to exist. And the question is really, how do we move from a policy matter, from a structure that's premised on collection, where we use the old physics, where we use analog physics, which is basically, look, the way we protect privacy in civil liberties, we use the fact that the real world has friction and it's hard to put stuff together, so we have practical obscurity, we have these things, we have these high hurdles, but we're moving into a world where that's not true, and that – so to have laws and policies that are premised on that physics, in my view, is silly, and we need to move to laws and regulations and policies that understand the new physics, which is that time and space don't exist when you're talking about the virtual worlds.

And most of this data and everything lives in this world where you can't rely on it, which is what creates the problem. I mean, you know, the practical obscurity question is exactly, you know, is, in the old world, data may exist, even public data might exist, but it’s in many, many different places and you can’t pull it together. As soon as you’re able to do that with one click of the button, you’ve incrementally changed both the qualitative nature and the quantitative nature of the problem.

Let me just see if there’s one more point I want to make before I – and there are a couple of things I wanted to say, but let me just – I want to get to the discussion.

Christmas bomber, we can talk about it as a separate issue. Oh, on the use regulation, we’ll plug for another thing, and so – Ben mentioned I’m on the Markle Task Force for National Security. Markle Task Force reports have been out, you know, the first one came out in 2002, I think, then it was 2002, then there was two in ’04 and ’06, one of which became the intelligence report or was incorporated into the Intelligence Reform Act in 2004.

You know, Markle, I think even the first report, but certainly by the second report, the idea that we had to move to a scheme that was premised on authorized use and how you use data rather than collection was a very key part to this. And there’s one other piece I’ll just throw into that, it’s not just this issue that data exists, oh my God, let’s get over it and figure out how to use it. Here’s another problem, all of our laws are premised on the initial collection. In other words, the initial – there’s one – there’s a binary threshold, law enforcement or national security can either collection this stuff or not. Let’s assume they collect stuff completely legitimately, we all agree what the standards should be, they collect it. The way the rules are now, they collect it and can own it forever and do whatever they want with it after the fact.

As we go to these more massive collection programs, which we may or may not have to do given that the data is just there, the issue really moves into this realm of use, and it's really probably the most important thing.

I mean there are two points before we get to the conversation. So I think you're absolutely right, the book is great. I think I need to mention – the – but I do think that the takeaway, which I think is your conclusion in your last chapter, is that we sort of missed the opportunity to have a lot of the debate that we needed to have, the policy debate, and it's unfortunate that this tension between the TIA public program and also focused more on connecting the dots actually was the loser, and the TSP, which is the Terrorist Surveillance Program, the wireless wire tap if you want, program, which is about collection, which is getting more massive data in and then we don't know what to do with it, sort of won, if you – I mean in that sort of tension thing, and that's a problem. And I think, you know, we'll see a shift back now, I hope, and perhaps we'll have this debate where we can come up with the rules, how we're going to live in the future. Anyway, so that's it.

MR. WITTES: Thank you. So I'm going to kick off the conversation which I'd like to go as quickly as possible to questions from the audience, but it seems to me that one of the threads that runs through the book and through a lot of the public discussion of this issue which I'd like to hear both of your thoughts on is this underlying suspicion on the part of a lot of people that technology is a pipedream and doesn't really work.

And so you have this – on the one hand you have this incredible promise of this idea that if you can just process data with perfect efficiency or near perfect efficiency, you can identify the terrorists walking around among us; and on the other hand you have this suspicion that the behavior of terrorists is not actually that different from the behavior of other people until such time as they blow themselves up, and that there is no terrorist behavioral fingerprint that, if you designed the perfect algorithm or set of perfect algorithms, would give you that early warning system. And speaking for myself, I'm a lot more sympathetic to the idea of a kind of master set of analytical tools if I think that there is an underlying behavioral pattern that such a set of tools can actually pinpoint than if I don't think that.

And so I guess the question I want to throw out there is, you know, at the macro level, does it and can it work, or is it, you know, a windmill that we're tilting at, you know, and in what sense is it one or the other?

MR. HARRIS: Well, I'll answer first then. Kim is more I think the technologist than I on this. But my sense is that this has been a fairly elusive kind of dream that hasn't been proven yet.

Now, there are a lot of people who will sort of try and take a critique on this by saying, well, let's look at data mining as sort of a type of analysis here, and let's look at the error rates in things like data mining, and they'll try and sort of make a direct connection between that and what Poindexter was trying to do or what a lot of some of the people in this national security space are talking about. It's not exactly data mining, though. What we're talking about here is more pattern analysis and pattern recognition. So the idea that I think was compelling about what Poindexter had in mind wasn't so much perhaps this, you know, we'll develop a system that will kind of almost, you know, like a minority report, will go out and find exactly and pinpoint who the person is, but rather can we develop series of transactions and patterns of activity that we know match up with terrorist plots that we've seen in the real world or that we might have mattered, and can we train a system to go out and find those signals and detect them.

It’s at that point that I think he envisioned having human beings come in and start doing the real nuts and bolts analysis and the real examination, and it’s almost, you know, the surgical process on this, if you like.

I think any technology system that’s going to be developed in this space, what it cannot become is the end all, be all, it cannot be the first and last stop, it has to be a tool that does heavy lifting for human beings who then come in and look at the information, and using human judgment and calculation, say what does this really mean, should we follow up on it. And at that point, you really can have regulations and laws and policy directed at governing that activity. You know, you might have a passive system that is looking at data and information and sends up red flags before a human being ever touches it, and when they start to touch it, you can really get into the question of use.

I mean you’ll – I think, too, but I think that what you’ll probably see is that if you want to rate how well these kinds of technologies work, there’s going to be sort of an acceptable fail rate.

In other words, maybe these things work 85 percent of the time at spotting suspicious transactions, and then we bring human beings in to verify them, maybe that’s good enough in terms of using technology as sort of a phase one kind of operation on the data.

MR. WITTES: What do you think, Kim?

MR. TAIPALE: Well, I agree with what Shane said, but let me – before I come back to that, talk about your question first. I mean I think one of the problems with this is that we talk about a lot of different technologies and of applications with technology as one thing or the other, so the first level is to sort of, what Shane did, try to move away from this sort of idea, that you just sort of throw all the data out there, and the data is going to tell you patterns, oh my God, these people are doing this and it looks suspicious, so it pops up in this thing. And where Shane was really talking about how – actually, even TIA was much more oriented about red teaming, sort of trying to tease out the kinds of things that we know happened, at least with certain kinds of terrorist spots. I mean you're not always going to get the lone wolf this way, and it was never aimed at that, it was more about looking for those patterns of activity of organization that go into a plot.

And, you know, if you look at people who analyze terrorist things and everything, and then there's a discreet, you know, pattern of how those plans to, and literally you can see, you know, X amount of time is usually spent on this, and I think 40 to 60 percent of time is spent on reconnaissance and, you know, blah, blah, blah, and you can look for weak points in each of those things and say, well, okay, if you were doing that, where would be the flags, what's the avoidance behavior, can you look for avoidance behavior?

So there are patterns clearly at that level, where you're using expert knowledge and you're looking for those. I think the questions then become, what data do you use to generate those patterns and what data do you run those patterns against to look for other things, and that's, obviously, a very important part of the question.

I just want to – now, as a separate thing, though, there's a layer even before you get to those kinds of things that are still the same kinds of technology, but exist maybe even in a realm one step up which aren't even as controversial as that layer, which is, think about the Christmas Day bombing, I mean in a really weird way, the system worked in the Christmas Day bombing, but I don't think in the way that the sort of government officials said it worked.

I think it worked, because if you look at it, in each of the silos where that information – and there were some mistakes, there were the misspelled names and all those kinds of things, which, you know, shouldn't happen, but within the silos themselves, the information actually rose up to the right level where people made decisions, oh, this is not going to the next level.

Now, we can argue about the standards. I mean in some cases, it was the local agent in, I forget now where he was.

MR. WITTES: Nigeria.

MR. TAIPALE: He was in Nigeria, okay, where it didn't go up the next level. There were some other places where, for instance, putting people on the no fly list from the watch list, had a very high, almost legalistic, reasonable, suspicion level that the FBI was insisting on because it came out of the law enforcement sort of – well – so you can argue about the standards, but the system sort of worked.

The information went up each of those silos and then hit the place, and maybe people made bad decisions or not. The technology, though, and the sort of stuff we're talking about, the sort of systems approach to this might give us the ability to have situational awareness across that.

So you could have another layer where people were seeing that these decisions were being made correctly in the silos, but, by the way, the aggregation of all those decisions, maybe it should be bumped up to one more level, and the fact that the same name was popping up in all three of these places meant something. And so it's really this ability to layer in more layers of analysis, which is the reverse sort of the thing that we were talking about there, so there's two – one is, you have patterns that work, and you use that to narrow down the realm in which you need to focus. So maybe it's the 85 percent success rate – and then you focus on that and you get better and better, and you try not to have bad consequences from the error rates.

On the other side, you actually have a system where decisions are being made distributedly, and as they move up the system, you want to actually give people easy access to having situational awareness, to seeing those various independent decisions and maybe making a judgment that – because it's sort of the mosaic side of this problem rather than the pattern side of this problem.

So now all of a sudden the fact that five of these things happened, the same guy's name came up in five different places and got killed at the right level for those silos, but, by the way, oh, ooops, somebody who's seen all five of those says wait a minute, maybe we need to take this up one more layer, so –

MR. WITTES: Yes, wait for the microphone. And when you ask a question, please identify yourself so that the Watchers know who you are.

MR. CHARETTE: Robert Charette with International Investor. A quick comment and then right to my question. I have interviewed a lot of people from former East Germany, their biggest fear was not the state itself, but the neighbors, the people in their community, the people they didn't know who might have been working with intelligence who used information against them to exploit them for their own personal interests.

So here's my question for you; I'm not so concerned about the state collection, what I am concerned about is the tens of thousands of employees who will be answering these agencies, leaving these agencies, and the amount of technology, some of it eavesdropping and other kinds, that will escape the control of these agencies, and will end up collecting data on personal citizens, corporations, and be misused in many other ways; have you looked at that in your book? I haven't read your book yet, sorry, Mr. Harris.

MR. HARRIS: There is a – there's a rather – sort of bizarre chapter, and I say bizarre because of this point where the plot starts taking like these really intricate, you know, improbable twists, where something like this happens; the outcome of it is not an infringement of liberty or a privacy bill, I'll just briefly explain the story. There was a company in New York, and I'm going – it was probably around 2006/2007 timeframe, if I remember correctly, started by a venture capitalist up there who wanted to essentially build a total information awareness like system to look at corporate data and information about new products, changes in corporate hierarchy, new hires, et cetera, micro kind of data, and then use that sort of in the investment space to make bets on companies fortunes and where they were going on a very short microscopic and kind of quick level.

In a series of conversations that this individual who started the company had with people in academia, with people in research, he eventually ran across folks who, at one point, had worked in government and developed the technology that ultimately became that thing I was talking about earlier called the BAG.

So it is the case in research and development that ideas get recycled. And to the degree that people in government are often not just working for a government agency, but are perhaps working for one of the national laboratories, as was the case in this instance, technology will migrate out by different names and find itself suddenly being used for an entirely different application. And this was one of these very strange situations where this technology called the BAG eventually got incorporated into this other system which was called Monitor 110, and it had a very sort of short life – life span.

I actually found emails from people within NSA who were aware of this and would refer to the system as the BAG/Monitor 110. And it became known by other names, as well, based on other programs that were based on the technology that was developed over at NSA.

So I think, you know, that risk is certainly there I suppose of it being used improperly, yes. I mean I don't know of an instance where that has happened, where someone has taken this and spied directly on people.

SPEAKER: Then you’re missing a lot.

MR. HARRIS: Well, then you could give me an example of that where that’s happened.

SPEAKER: We can talk later.

MR. HARRIS: Okay, sure, I’d love to.

SPEAKER: But even within the financial community, this has happened.

MR. HARRIS: And being used on individual citizens, okay.

MR. TAIPALE: Well, can I just – I mean one – can I just follow up on that for a second? You know, look, the reverse of that is also true. I mean the developments are happening in the private sector. I mean, you know, data analysis – data analytics right now is probably the hottest area of D.C. investing right now to the extent that there’s any D.C. investing.

And it’s not just at the level of people trying to get a jump on the market or anything else. I mean, again, you know, the anecdote is great, but that’s the classic sort of – that’s the innovation cycle. He’s the guy with the arrows in his back, that – because he started way before, you know, the technology was ready and the world was ready for that, and he didn’t have the right data bases and the right – tools to actually be able to see those kind of anomalies that were relevant to making investment decisions ahead of the market.

But you see this going on right now. I mean there’s a huge effort right now. Actually, there’s a bill that was just introduced in the – called the Committee to Establish the National Institute of Finance, which is to provide the analytic tools for government to do systemic financial regulation. How are you going to do systemic financial regulation? Everybody is talking about it, watching it. Well, you’re not going to be able to do that unless you have some system awareness across firms. You’re going to have to see what different firms have on their books and how that’s related and figure out what the level of systemic – so this problem is coming up, you know, on that side, and those tools will, you know, people will look for advantage in that and everything else.

But we are going to have to deal with that issue. I mean if we want to have systemic regulation in the financial markets, we’re going to have to find some way to deal with data the same way we’re talking about in these other places. So it’s happening on both sides of the equation, and it will feed back and forth.

MR. WITTES: Yes.

MR. ABRAMSOM: I’m interested in the use to which data is put, and the civil liberties perspective, and the principals we use to trigger security actions or protective actions or further investigations. And I’m going to simplify it down to maybe four different triggers.

MR. WITTES: Can you identify yourself, please?

MR. ABRAMSON: I’m Alan Abramson, I’m just a person not associated with any organization of any kind.

SPEAKER: We’ll have to check that.

MR. ABRAMSON: That was a lie, all right. There’s probable cause, there’s reasonable cause, there’s suspicious associations, and then there are associations. And it seems to me that in the political context since 9/111, we’ve blown past probable cause as quaint and outdated. The Visa apparatus seems to me to work between reasonable cause and suspicious associations in making judgments there.

But the intelligence community tends to lean, as it always has, toward associations. And I’d like to ask for your reactions as to where you think we ought to be in terms of, you know, the risk benefit and the balancing of civil liberties.

MR. WITTES: Just to clarify the question, though, what sort of adverse actions are you – I mean are you asking about – I mean, look, the standard for arrest is very different than the standard for an FBI agent to scratch his head and wonder about whether you should be subject to an investigation. What adverse action are you contemplating when you cite those various standards?

MR. ABRAMSON: I think that's a very good point, and I think I'm deliberately obscuring that and mixing them together, because we've experienced since 9/11 arrests based on sheer association, not even at suspicious levels in a number of cases. We've got people – we had people in Guantanamo who were swept up innocently and incarcerated for many years. So I'm not sure how to discuss that issue since we've been dealing with it on an ad hoc basis. I'd like to maybe just ask what principals we should be using in approaching that issue.

MR. WITTES: That's an excellent question; Shane.

MR. HARRIS: Well, I can tell you – well, first I should say the standards for what triggers let's say somebody going to the next level are often I think rather opaque. I mean you mentioned, for instance, when somebody is on the master watch list, how do they get to the no fly list, and there is sort of a legalistic standard of what they call derogatory information that sort of bumps you to the next level, and there are people making those calls.

What I can tell you is sort of like if you're looking at the sort of – the sort of more basic fundamental issues here around things like, you know, the standards in the Fourth Amendment that became the center of debate under the Terrorist Surveillance Program. I mean, you know, what you found in the aftermath of that program, after it became public, was that there was this great argument over what is reasonable for purposes of seizing information and searching peoples' communications. And there was a great debate even publicly after the program was exposed about whether the Fourth Amendment means you have to have probable cause to go search someone versus a reasonable kind of suspicion.

I know from interviewing officials who were involved in the program that the terminology that was used for when they decide to effectively, you know, zap somebody's communications and grab them was, is there a nexus to terrorism that was the standard.

Now, within NSA and these agencies that are doing that, there are certainly – there are checklists we know that they were going through to check off if what the nexus actually means, and we don't know what those standards were, that's never been revealed.

But I do think it's fair to say that it became more fluid after 9/11. You know, what are the standards that we use to graph this data, and the government was looking for I think, broadly speaking, an argument based more on reasonableness, can we reasonably suspect that if this person in San Francisco is in communication with a suspected terrorist in Karachi, that that person in San Francisco might have a nexus to terrorism, it seems reasonable enough, go get the communications; that's sort of changed.

One other sort of data point in this that I think, though, kind of was very revealing, and I talk about this in the book, about how far this actually gets you, and is it good enough, and how much can we learn from this kind of – these sort of standards and these connections.

In 2006, the agency that – the research and development agency that inherited the TIA programs and then morphed into another name actually put out a proposal for yet another sort of system of systems programs that was going to try and lash together various data analysis operations that were existing in government at the time and kind of develop a new kind of system of systems, and it went by the project name Tangram, it's a public document, you can go look at it.

And there was this very interesting sort of passage in the solicitation for proposals where the researchers talked about how far the state of the art had gone to that point, around 2006. And what they said was that the best that we can come up with now is guilt by association as a standard, that is pretty much where we are, and they said, you know, and they made a point that has held true to this day, which is that when you go to target as an intelligence agency or an investigator, you've got a known target, a known person, or a seed entity they like to call it in this instance, you can find out a lot about that person and how they're connected based on collecting information, you know, even discreetly about that one individual.

It's when you don't have a target that you have to rely on guilt by association. And the researchers in those documents said that's where it starts to break down essentially, we can't get past that, and that is not good enough. And they were looking at this from the standpoint, not as much of a legal standard, but just can we find more information operationally about these people, and they were even saying guilt by association, it's not good enough.

So I mean legally it doesn't raise to the level that I think we're comfortable with, and operationally it's not meeting the match. And I haven't seen anything that suggests that we have kind of leaped beyond that point right now, and I think that's probably from an operational standpoint, very limited.

MR. ABRAMSON: So can I just talk about the legal standard for a second?

MR. WITTES: Let's go to some more questions and – yes, in the back.

MR. SALINGER: Hi, I'm Graham Salinger, I'm a student at American University, and I want to know about – how people in the intelligence community are trained. You talked about Fort Hood and you talked about the Christmas Day bombing, and those are good case studies in terms of connecting the dots and learning and building, in terms of after the fact. I want to know – in the intelligence community, people are – if they have sort of like mock training sessions where they do sort of mock scenarios or if there's anything like that where people are trained to deal with these sort of situational things, where they learn to connect the dots in a non-real world situation.

MR. WITTES: You want to answer that?

MR. TAIPALE: I'll take a stab. Well, I'll make a comment without actually addressing the reality of it. One of the things that one could say if one was being – well, let me say it and then – before I qualify. It's interesting that NSA particularly has a very, very good training program for its analysts, that spends an inordinate amount of time teaching them how not to access U.S. person data, and how to handle U.S. person data, and to deal with the privacy issues, a huge amount. I mean actually as an institution, they do a great job at that.

They actually don't spend as much time teaching them how to be good analysts; you learn that on the job. But the training program is really aimed at dealing with the rules. And it's not a criticism, I'm just – that's the reality of how the bureaucracy responds to things.

MR. HARRIS: And I'll say, too, analysis as a trade craft, I mean it's going to be – it's different in each agency, but I think it's fair to say that in the sort of – if we can sort of crudely draw the line of demarcation here as pre 9/11 and post 9/11, pre 9/11 analysis is sort of you becoming a subject matter expert in a particular issue, and you having your own methodology for how you organized the information, but you essentially becoming an expert on that.

After 9/11, there's this realization that you've got to find – you've got to train analysts to be more all source analysts, that we can't just have, you know, two dozen experts on Nigeria, we have to have people who are, you know, more expert on sub-Saharan Africa, sort of go more broadly. And there are initiatives that are underway now to try and expose analysts in one agency to how they do it in another, such that it's basically not if you want to rise up in promotion in the ranks to the level of the senior intelligence service, you actually have to do stints in other agencies and learn how they do it.

So they're trying to institutionally address this issue by making it essentially a job requirement for promotion that you can't just sit in your silo anymore. I think that's a generational process, though, I think. I mean that's something that, you know, the older generation of senior leaders and officials in the community, you know, don't necessarily see the value of the younger people coming up, you know, it's just being – they're being indoctrinated with it, so over time that will shift, I hope.

MR. TAIPALE: There's one – I mean this is actually an important thing – my earlier answer, but the overall reorganization which Shane is referring to, you know, the model that's being used for that is the joint services model that we use to remake the military, where traditionally we had the four services that were completely separate, but now we have combat – who basically each of the services job is only to provide resources to the commander to, you know, to deal with the problem. And that really was accomplished by having people serve in different places in joint programs, and I think that's the same thing that's now going on in intelligence communities, and it's actually a very valuable thing.

MR. WITTES: Yes.

SPEAKER: My name is – I'm a newspaper editor working with Hearst here in Washington. You mentioned the lack of an intelligence Google as one of the reasons behind this failure with the Christmas bombing attack. Could you go a little bit further on that, and what could it look like, and how could it be developed? Thank you.

MR. HARRIS: Okay. So if I'm king for a day in this, I get to pretend I'm the DNI and what would it look like. I think, and Kim may have a very different view on this, I think it's possible that we should try the radical approach of actually putting agencies on a data diet.

I'm not at all convinced that by collecting information in 80 different streams with 28 networks, that we're making this problem any easier. And I'm not convinced at all that every one of those intelligence streams has value, or not value, that it should be trying to be put on the same level as, you know, things like, you know, electronic intercepts and things that actually might be more telling. I think that to do this, it seems to me there's a technological way to – whether it involves sort of standardizing the way information is put into data bases, or lashing together a legacy system, there are ways that you can mechanically do all this stuff.

It can be very difficult, it can be very expensive. Bureaucratically, it is very hard because agencies collect information different ways, they have sources and methods that they want to protect.

We've been having that conversation, though, I think since 9/11. There was this sort of – at least there was lip service to the idea of doing better information sharing, about tearing down these silos and finding ways to harness these data bases and collect them and put them, you know, their capabilities together.

I think the Christmas Day event showed that we haven't made a lot of progress in that area. So in terms of what it would look like, there actually has been an initiative underway for several years known as the Information Sharing Environment, which I think now is actually no longer housed at the DNI's office, it's actually housed within the Executive Office of the President, I believe. So at this point, I mean I think it's fair to say that what –

SPEAKER: With the program manager?

MR. HARRIS: With the program manager.

SPEAKER: Without a program manager.

MR. HARRIS: Without a program manager; wonderful, there's no one in charge, except nominally the President of the United States. You know, a lot of people that have been talking about this book have said, you know, why not just give this problem to Google, I mean right, I mean like why not just let them solve it, and I mean I think that's sort of maybe, you know, kind of a glib way of saying, yeah, why can't you find a way to standardize this information and sort of break down these barriers, where they exist in these sort of, you know, at this bureaucratic layer.

To do that, what our system looks like, though, we require forceful, persistent, consistent energy from very creative and motivated people. I mean this is not something that you can just issue an executive order for and in two years they'll fix the problem, they tried that, it hasn't worked. So this is going to require people really I think diving down into the bowels here and forcing movement on this issue. I mean – and I don't – those people are rare, and life in general and rare on the government, as well.

MR. TAIPALE: Okay. Let me say something that's obviously going to get misquoted again. First, why don't we address the technical thing? The reason we can't do Google is because what Google does is aggregate all the data, and they have a central data base with all of their stuff, and then they search it.

So it's not they're searching your web site, they've collected your web site and they have everything. You can't do that in government for the very reason we've been talking about. Nobody wants to take those 80 – those 30 data bases, 80 data streams, put them in one place, that's a huge problem.

So actually the way to do that on a technical level is, you need to figure out how to do a distributed search, how can you do a search from one central location into multiple data bases that aren't on the same standards as everything else. That was a key component of TIA that got killed and we saw them solve the problem. Anyway, separate from that, the controversial side of this, which I'm going to say, which I think is actually true, and again, it's part of this policy debate that hasn't taken place, is that who in their right mind would try to solve this problem? Anybody who sticks their head up to solve this problem is going to end up where Poindexter is or anybody else.

Listen, 9/11 failures, Christmas bomber failures, the only person who's ever lost their job in any of this is Poindexter and other people who have tried to solve the problem. I'm not defending John necessarily or the program, but the only people who have ever lost their jobs are people who have tried to solve the problem and have crossed the line, a very important line, of legal policy or someplace else where the privacy issued has killed them and has killed the project.

No one has lost their job for not doing their job, for not connecting the dots. That's an environment that's not going to lead to a lot of innovation, as far as I'm concerned. I mean I'm not arguing, you know, let's let everybody do everything, I'm just saying that's the incentive structure under which people are working, and you're not going to solve these problems until you deal with that.

MR. WITTES: Yes.

MR. SPANOS: Yeah, I'm Ed Spanos, I write for Executive Intelligence Review. I have two questions, one is very simple, maybe, which is what, if anything, has changed since the Obama Administration came in? The second relates to what I think concerns a lot of Americans, particularly those who are politically active, is the fear that this is, you know, under the talk of terrorism, that this will be used domestically for a domestic watch list, things of that sort.

Now, I go back to the – in politics to the 1960's, when that sort of thing was very real. There was a lot of information sharing at the time. Army Intelligence had a huge program, which most people don't know about today, data collection, domestic data collection. This went to the FBI. The FBI collected from CIA, Army Intelligence, Air Force Intelligence, Navy Intelligence, and I've seen it all in my files, you know, they did this stuff.

They had a domestic pick-up list that was known as the administrative index, which was a list of ten – 20,000 people who would be picked up and detained under conditions of a national emergency. I'm not making this up, I mean this is real.

MR. WITTES: Okay. Let's –

MR. SPANOS: Well, the question is, this is – is there a potential, and that's what concerns people about data mining, you may not like the term, but collecting all this data, that this could be used under the pretext of saying we're investigating terrorism as in the 1950's and '60's we were investigating communism, could be used for surveillance and potentially targeting, you know, U.S. citizens under conditions of a national emergency.

MR. WITTES: Okay. So let's – Kim, which of the two questions do you want to address and we'll let Shane address the other one?

MR. TAIPALE: Well, okay.

MR. HARRIS: -- the first one.

MR. WITTES: Well, I mean – okay.

MR. TAIPALE: Is that a theory? Yes. Can that be managed? Yes. And technology actually provides some of the solutions of that. And Shane mentioned it before when he was talking about watching the Watchers. The fact is, one of the problems with the '60's and '70's, which a lot of people who are in this debate are reliving, is that they have this mentality that, you know, that Hoover and the FBI can do stuff and we never know about it. The fact is that that's not true. The anecdote that Shane mentioned before about six months ago finding out that the NSA had over collected a couple thousand and had gotten a couple thousand domestic conversations in this thing – that came because of an audit, right. We live in a world where you can actually audit these systems after the fact.

MR. WITTES: And that has happened repeatedly with respect to national securities matters at the FBI.

MR. TAIPALE: It's happened repeatedly – and everything else, so we do catch these things. Now, is it perfect, would a system that didn't make mistakes in the first place be better? Yes, but we're not going to build that system. So a system that actually has – logging and audit and checks and balances after the fact, in a world where you can't erase those tracks, because those tracks, just like they exist for everybody else with those transactions, exist in these systems from the Watchers.

If I look – if I'm at the IRS and I look at Brittany Spears tax return, it's going to – it is absolutely now possible to figure out if I got there because I was following a lead or because I was doing it because I just looked at, you know, Brad Pitt's. You can make up a lot by the fact that these systems can actually after the fact be audited. That's not a perfect solution, but it goes a long way to addressing those, and that's the debate we should be having. And that was part of, you know, look, the world is different than the '60's. You can't get away with a lot of stuff. I mean – today. I mean it's very hard in this world to live without leaving trails and tracks on both sides.

MR. WITTES: So what about the other question, Shane, is this an area where there's any significant discontinuity between administration or this -- the executive branch is a giant ship heading in one direction and it really doesn't matter if one captain goes to sleep and another captain wakes up and takes over the bridge?

MR. HARRIS: There's a remarkable continuity I think between the kinds of surveillance policies we're talking about now and the Bush Administration and the Obama Administration, the sort of moment where this becomes very publicly quite clear, and I write about this at the end of the book. In 2008, when Obama is still running for the nomination, he opposes a significant rewrite then favored by the administration of the Foreign Intelligence Surveillance Act. And effectively what this rewrite would have done was to make legal a lot of what was being done under the cover of a secret order for the past six or so years, not entirely, but a lot of it, and to grant immunity to any of the telecommunications companies, immunity from lawsuits that had handed over their data ostensibly on the grounds that it was – the Attorney General was saying it's okay if you do this, and the President said it's okay, too, but it wasn't going through the process.

So Obama says I don't support this and its expansion of surveillance authority, it's too much executive power, if these companies were giving over information illegally, they shouldn't be getting off the hook for that, and it's a fairly principal stand, which he completely abandons the closer he gets to securing the democratic nomination for President.

And after, by his own admission, he has conversations with his Intelligence advisors who tell him that the underlying program and the NSA issue was actually useful. Well, my research has led me to conclude that there's only one person on his staff who would have been able to actually tell him that, and it's John Brennan, who is currently his Homeland Security and Counterterrorism Advisor. Brennan was at the NCTCN and the CIA when the program was running and had a view on this, and I think that he probably came to the President and said, look, this is a useful tool, the President looks at it and says it's probably going to be legal, these are executive authorities of surveillance and intelligence gathering, especially on foreign targets in this context that Presidents have enjoyed for many, many – for a generation, so why should I be any different.

And what you see, too, is I think this realization that this is – this is not an issue of partisanship, this is not – democrats don't let surveillance and republicans do, this is a separation of powers issue, this is an executive authority issue.

And one of the reasons why I wanted to go back in history to sort of examine the surveillance policies as they existed over time was to sort of draw these continuous threads one to the other. I mean, you know, I think it upset a lot of people politically that Obama flip flopped on this, but it should absolutely not come as a surprise to anyone who studied the history.

MR. WITTES: We have time for one more question; yes.

MR. GRINDSTAFF: Hugh Grindstaff; did you have a chance to look at New York City, what it's done since 9/11 and see how they've handled, you know, they have a special intelligence squad they sent to Israel to train with Mossad? It's kind of interesting – same question. Is the camera going to take the film he took and do a face recognition for everyone that was here?

MR. HARRIS: I'm not sure it would be very accurate if they did. I didn't look at New York in the book, but there actually is a book that's out now on – specifically on New York's Homeland Security and Intelligence effort. I think in many cases it's fair to say it rivals some of the capabilities of the FBI.

MR. WITTES: Now, New York City, the NYPD has language capacity that operates as surge capacity for the federal government, because they have a lot of capacity. That was a very brief question, so we can take one more. Yes, sir.

MR. FRANKLE: I'm Ed Frankle, I'm a visiting Fellow here at Brookings from the intelligence community, so I wanted to push back a little bit on some of the assertions that have been made, first on this idea of connecting the dots, you know, we're good at collecting, but we're bad at connecting. And I mean, to me, it's a – the phrase – I would like to see the phrase "connect the dots" removed from all the discussions on this because I think it gives people the wrong idea, that the picture was already there, and that's what connect the dots is, right, it's a numbered picture, the picture is already there, there are only the number of dots that are in the completed puzzle, and it gives the idea that this is really easy work, what the intelligence community does, all this stuff gurgles up, we have these pictures, you know, the father comes into the embassy, oh, and there's a communication over there, and therefore, we know this guy is going to blow up a plane.

So I just want to push back on that because I think that phrase gives people the wrong assertions on what's been done, which kind of leads me to my question about the idea of a data diet as the best solution.

I'm wondering how we can justify sort of pulling back on collection when the problem that we have sometimes in being able to connect the dots or bring people up to a point where we can worry about them as having enough information. If you look at the Christmas Day bomber, we had two pieces of information completely unrelated that are really lost sort of in a sea of other things, and only appear clear in hindsight after the bombing attempt fails. And so to say while the solution is let's collect less and that way things will become more clear, I think it's difficult to say because as soon as we identify somebody as a target of interest, the first thing you've got to do is find out more information on them, and having a larger pool of information is going to be the clear way. So I'm wondering how that is a worthwhile solution.

And the last quick point, I know I'm almost out of time, the idea of the intelligence community Google, I think the issue is not the compilation, it's the security issue, and the fact that things are compartmented at different levels, and there's, obviously, you know, the willingness of agencies to want people throughout the intelligence community to see things that are very sensitive for fear of giving away sources of methods, which has happened in the past.

MR. HARRIS: Well – answer that kind of turning it around in the form of another question, too, but okay, so if we've got all this information, but there were only two or three data points of any use on this individual, now, maybe there was no place else that we could get useful information on him, but I think it begs the question then, what about all those other 78 data streams, what are they doing? Now, I don't want to equate all of these together in the same level, I understand that some of this is remote sensor; some of this is actual conversation. I'm just not convinced off of anything that I've seen and people that I've talked to that there has been a real thorough scrubbing of all these sources, or maybe even an attempt to sort of put them into different categories of use.

SPEAKER: Or rank them.

MR. HARRIS: Or rank them; I mean everything I hear from people on the NCTC is that the fire hose has turned on us and everybody is just dumping this stuff on us, because this is now the place where you dump it, and I've done my job as the NSA or the FBI collecting, and handing it off to you guys, and you take it from here.

You know, is connect the dots an over used metaphor? Maybe, but again, I have not seen a rigorous attempt, at least not one that's public, to go through and rank order this stuff and try and filter out the garbage from the useful intelligence.

SPEAKER: Part of that is analytic trade – what you talk about is sort of the skill of becoming a good analyst is learning, you know, what data streams are more important and what data streams are less important, and a lot of that is time on target and experience. And we, you know, at the intelligence communities are very young – inexperienced work force relatively post 9/11.

MR. TAIPALE: But Shane's point that the current bureaucratic response is everything over the – because now you can only lose your job if you didn't share, and it turns out something. Before you could lose your job if you shared and somebody wasn't, you know, if you shared something that you weren't suppose to share; now it's the reverse, so there's a bureaucratic problem.

I think the connect the dots thing, though, actually, not to spend a lot of time on metaphors, but it's actually very important, in my 2003 article, there's a footnote about connect the dots, and I counted the number of times it came up in the 9/11 report and other places, and yeah, it was a – it was a couple dozen. And I did a Google search at the time, and it was – I don't remember, but, you know, tens of thousands. If you do a Google search for connect the dots today, it's like, you know, a zillion whatever kind of thing. What I usually – I usually actually avoid connect the dots and argue that it's much more like a jigsaw puzzle than connect the dots. It's not – here's dot one, here's dot two, dot three, it's a jigsaw puzzle. And the interesting thing about a jigsaw puzzle is that the easiest pieces to put in a jigsaw puzzle are the first few and the last few, and the ones in the middle are the hard ones.

And I know we can go down a whole metaphor, but actually there's the whole thing about analytical process, where that curve is very, very relevant, and that thing means a lot. And the last thing is, I'm not for less collection, I mean I shouldn't say that. I'm not endorsing the idea that data diet is the solution to this problem, I'm endorsing that the tools for better analysis is the solution of the problem.

MR. WITTES: On that note, we'll call it a day. Thank you all for coming.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

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.

/s/Carleton J. Anderson, III

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2012