THE BROOKINGS INSTITUTION

THE COMING PROLIFERATION OF DOMESTIC DRONES: WHAT WILL BE THE IMPACT ON PRIVACY, SAFETY AND NATIONAL SECURITY?

Washington, D.C.
Wednesday, April 4, 2012

PARTICIPANTS:

Introduction and Moderator:

BENJAMIN WITTES
Senior Fellow
The Brookings Institution

Panelists:

JOHN VILLASENIOR
Nonresident Senior Fellow, The Brookings Institution
Professor, Electrical Engineering, UCLA

PAUL ROSENZWEIG
Visiting Fellow, The Heritage Foundation;
Founder, Red Branch Consulting PLLC

CATHERINE CRUMP
Staff Attorney, Speech, Technology & Privacy Project
American Civil Liberties Union;
Nonresident Fellow, Stanford Center for Internet and Society

KENNETH ANDERSON
Nonresident Senior Fellow, The Brookings Institution
Professor of Law, Washington College of Law
American University

* * * * *

P R O C E E D I N G S

MR. WITTES: My name is Benjamin Wittes. I'm a Senior Fellow in Governance Studies here at Brookings. It's a pleasure to welcome you. It's a great turnout we have for this event and I'm delighted to see you.

As most of you because you're here probably already realize, we're actually on the verge of a kind of revolution in this country and probably beyond. We've seen the revolution already to a great degree in military affairs, but in a provision of law that got little notice at the time but has been creeping up on people, Congress has brought the revolution home. It has instructed the Federal Aviation Administration to promulgate a set of rules that will allow all sorts of unmanned aerial vehicles to operate domestically in the United States. Exactly how it will do that is not yet entirely clear and what will and will not be permitted under what circumstances is not yet entirely clear. But this is very big change, and to give you an idea of how big a change it is, just consider the rules that exist now which is that you can fly essentially model aircraft of one sort or another provided that you do it for noncommercial purposes and provided that you do it under 400 feet. Which is you say you can putter around with increasingly powerful technology, but you can't sell services doing it and you can't get in the way of the big boys.

What the military has shown abroad is that there is just an enormous amount that you can do with this stuff if the regulatory latitude is there to do it. And of course, the most famous applications of this involve surveillance and targeting, but those are not the only applications. To give you a little bit of an idea how far in principle this thing could go, I was talking the other day to a journalist, not the other day, a few weeks ago, named Shane Harris who's spent a lot of time reporting on this and was reflecting -- Shane is a features for "The Washingtonian" and had spent some time writing a paper

imagining and talking to a lot of industry folks about where this technology was and how soon it was going to get there. He'd basically come to the conclusion that there was no good reason anymore for there to be pilots in the domestic air flights that we all take and doesn't really think that that's going to persist for very long. The major barrier in his view to that phasing out is psychological, not technological.

When you think about range of domestic applications from law enforcement to journalism, there was an amazing little episode that happened. I ran across it randomly recently. A guy flying his UAV down I think it was in Texas and starts taking pictures of what appears to be a plant and finds a river of blood flowing out of it. It turns out to be a sort of grotesque animal cruelty situation going on in this facility and he sticks the pictures up. You can imagine a lot of journalist applications with this. You can imagine a lot of malicious applications as well by individuals, by governments, by corporations. And you can imagine revolutionary effects on people's day-to-day lives. So that constellation of issues, the privacy concerns, the promise, the broad range of potential effects, are what we're here to talk about today on the theory that none of you is here to listen to me. I'm going to keep my own role to a minimum. I'm going to introduce our discussants and then duck out and manage conversation flow.

Speaking first is John Villasenior who is a Nonresident Senior Fellow here in Governance Studies at Brookings, but is also a professor of electrical engineering at the University of California in L.A. He has written very extensively about this set of issues across a broad range of the topics that we're going to be discussing today. Speaking next will be to his right Paul Rosenzweig who is the founder of Red Branch Consulting and served in the policy shop at DHS in the last administration. Next will be Catherine Crump who is sitting to my right who is a staff attorney with the ACLU. And finally, Ken Anderson who is also a Nonresident Senior Fellow here at Brookings and

professor at the Washington College of Law at American University and who has written about robotics and law mostly in the international context including a very important paper that he wrote for The Brookings Institution. With that I'm going to turn it over to John, and thank you all for coming.

MR. VILLASENIOR: Thank you very much. I'm going to focus many of my opening comments on a particular class of unmanned aircraft called first-person view or FPV aircraft. An FPV aircraft has a front-facing video camera and transits real-time video to an operator on the ground. The operator looks at the image on a computer screen and sees the view as if he or she were sitting in the cockpit and flies the plane accordingly. When an FPV aircraft isn't visit visible to its operator, this is called non-line of sight operation. In fact, an FPV aircraft can be flown by a pilot many miles or even many thousands of miles away. The use of FPV aircraft in today's domestic airspace raises some significant challenges that touch on all three of the topics of today's forum, safety, privacy and national security.

First, in terms of safety, non-line of sight operation raises well-recognized concerns. For example, if the communication link between the pilot and aircraft fails, then there are obviously challenges involved in bringing the aircraft back to the ground without endangering other aircraft or people on the ground. As the FAA goes through the process of implementing steps in the recently enacted aviation bill, it will be important to be extremely conservative when it comes to the rules regarding non-line of sight operation.

With respect to privacy, FPV aircraft can make it easier to spy. A person who's standing in the street in front of your house and operating an unmanned aircraft over your back yard is much more likely to get caught. But a pilot sitting in a car parked 10 blocks away would be much harder to find. In addition, non-line of sight operation

would make it possible for someone to fly a drone into a fenced-in yard, lower it down to hover directly outside a window facing into the yard and take pictures of the interior of the house. Operation in this manner would be in violation of various aviation rules, but despite those rules, if there are tens of thousands of unmanned aviation systems out there and tens or thousands of people flying them, it will happen. It's important for privacy laws to recognize this possibility and put in appropriate prohibitions and sanctions to address it.

The last area is national security. It would be naive to deny that sufficiently large unmanned aircraft don't create some new risks. It would make no sense at all for a terrorist to attack a shopping center or an office building using a drone. As we saw in Oklahoma City in 1995, a car or truck filled with explosives would be far easier and more deadly. However, sensitive government and military facilities are a different story because of their access restrictions. At these facilities drones could be far harder to detect and stop than a car, truck or small passenger-bearing plant. An unclassified 2005 report issued by the federally funded Institute for Defense Analyses explicitly recognized these types of concerns. That report stated, and I'm quoting here, "A small team could launch a UAV from hiding with a relatively small launch footprint and make their escape before impact." The report also stated that, "There would be little danger of detection and transportation, launch or escape." And that with a precision-guided UAV there is a "high probability of successful execution."

Today I don't believe that smaller unmanned aircraft pose a credit security threat; however, other larger platforms might. Using today's commercial communications technologies, an FPV aircraft large enough to carry a significant explosive payload could be guided to a target well beyond line of sight. GPS guidance is another possibility. I don't think any of us would dispute the existence of this risk. The

harder questions are how big is the risk? Of the many thousands of methods available to someone intent on committing an act of violence against America, does this rank as a legitimate concern? Are there measures that can be effective while minimizing any negative impact on legitimate users of drones who of course are the vast majority? And this last question, are there measures that can be effective while minimizing negative impact on legitimate users of drones? The best solutions are probably technological. Particularly sensitive government facilities could be equipped with systems that jam communications and other systems of an income drone, potentially thwarting an attack. These some technologies could be used to defend our military facilities overseas against armed drones from what the military calls stand-off distance or stand-off range.

I would expect that there are people in our government working on solutions to this. Presumably we're not going to be hearing a lot about the details of that work. One way we can indirectly help, however, is by recognizing the value of these technology solutions and in doing so put those people in our government who are working on them in a better position to develop them. Problems are more likely to get the resources and attention needed to solve them when they are recognized and this concern has not been recognized enough. Of course, the best defense against a drone attack here at home is making sure it never happens in the first place. This will involve new mechanisms for coordination within the government and with the broader community to identify and respond to potential threats, and part of that effort is ensuring that weaponized drones don't fall into the wrong hands.

In closing, the presence of challenges regarding privacy, safety and national security don't mean that we should forego many of the beneficial domestic uses of unmanned aviation systems. They can provide vital life-saving imagery in many different scenarios. Companies in the drone industry some of which have

representatives attending this event are developing amazing technology innovations. People in university research labs and in the hobbyist community are developing equally amazing innovations. These innovations and the jobs they create both now and in the future can help American competitiveness not only within the drone industry, but also more broadly. Thank you.

MR. WITTES: Paul?

MR. ROSENZWEIG: First, thanks for inviting me. It's always a pleasure to come to Brookings. I appreciate the opportunity. It's good that you put me right after John because I'm going to try and give you the bookend of it. Where John has spoken of the threats that come from drone technology and the potential national security threats in particular, I want to flip that around and ask the question about the utility of drones especially in the homeland security and law-enforcement space which would be the principal governmental domestic use of those. In doing that I want to fight the premise of Ben's introduction just a little bit. He says that the introduction of drones is a revolution, and I would say that it's more of an evolution than revolution, that drones in utility might be more pervasive but are in the end not so terribly different than a host of existing aerial uses that law enforcement, border patrol and homeland security use every day. One thinks of helicopters as the paradigmatic example.

In doing that I also want to sound a cautionary note which is that sometimes differences in degree become differences in kind and if history is any lesson, if policymakers within government push too rapidly in the use of drone technology for governmental purposes, they will quickly I think lose the support of the public and very much run the risk of killing the goose that laid the golden egg, of driving the technology over the cliff of public acceptance into a ditch of public dismay. Let me talk about those briefly.

Why do I think that drones are useful? Just think of the border. Our southwest border is essentially a 1,500-mile-long desert punctuated in a few places by large cosmopolitan population, the crossing points. But in between there's nothing. There's nothing at all. That's why there was such a move in about the last 5 or 10 years to think about ideas like fences across the border because it is virtually impossible to imagine a situation in which one could successfully patrol that entire 1,500-mile length of border with anything approaching uniformity. The fences of course have proven both difficult and expensive to construct and relatively easy to evade and thus pretty ineffective. There is a reason that the Department of Homeland Security is so intent on the purchase of new UAVs for the southwest border and it's precisely because it gives a much broader scope of visibility, it allows for deployment of response forces in-depth so that instead of having border patrol at every 30 feet along the border, you can have people in cars who can respond when an intrusion is observed. That is just of course one of many potential positive uses that drone technology could be put to.

When one thinks about that's different, in general I would submit it's unlikely in that context to prove any different from the existing law and the existing uses that we have. The classic case in the Supreme Court is a case involving the use of a helicopter to hover over a Dow Chemical plant and the Supreme Court thee said rightly or wrongly, you can form your own judgment, there is no constitutional limitation on the use of that technology to surveil the open fields inside of a plant. The same law will likely be held to apply at least in the context of law-enforcement uses on the border or in other open field doctrines. I think that John's hypothetical of the small UAV that comes down and looks inside the house is an interesting one that I hadn't thought of before. It would probably fall under a different set of rules because one maintains a reasonable expectation of privacy in one's house and what's happening inside the house.

Having said that, drones are both useful and under the current structures probably lawful, not to say that we should rush headlong into their application. To see that clearly, I want to briefly a short story from the very recent past involving something called the National Applications Office, something that I doubt anybody in the room has heard of because it came and went so quickly that it made barely a blip on America's policy screen. The National Applications Office was an attempt in the last administration to unify the use to which America put its national technical means, that is, the satellites that we have that circle the earth and take really excellent pictures of what's happening on the ground. We of course use those in classified means for spying on Russia or in China or wherever it is that the NGIA wants to look. We also use them in a very overt and unclassified means to follow the tracking of hurricanes and after a hurricane has hit to assess the damage that has happened say to New Orleans after Katrina. There was historically a gap between those two uses, a gap for the law-enforcement and border and homeland security uses of these national technical means. The satellites also pass over the border between the United States and Mexico for example and one could readily imagine using those satellites as a means of surveilling traffic across the border. The National Applications Office was going to be a cross-government office that was going to unify all three of these purposes, the clearly humanitarian, the intelligence and the law enforcement and assign resources based on need and do a kind of racking and stacking of requests for use. In times of a hurricane crisis we would use it for a hurricane, in times of heightened tension we'd be focused on China, et cetera. That to my mind was a totally sensible proposal to use a technology which had no legal limitations for a very new and novel purpose, i.e., examining the southwest border. It crashed and burned. It crashed and burned because it was rolled out without any thought for the obvious privacy and civil liberties concerns that would attend using national technical means for that sort of

surveillance along the border. It crashed and burned because the intelligence community drove the entire development of the proposal. It was presented in a way that was a fait accompli and it was presented in a way that did not involve Congress or the NGOs who have privacy and civil liberties concerns like the ACLU.

The history of that is I think instructive for what we need to think about in terms of drone use going forward. It isn't to my mind that drone use for law-enforcement or homeland security purposes should per se be prohibited. To the contrary. I think there is a great deal of utility to be found in that sort of exposition. But if those uses are just laid on the table as part of the rulemaking in the FAA without thinking about the very legitimate and sensible privacy concerns that people will have about some of the scenarios that John talked about or some of the scenarios that I'm quite sure Catherine is going to talk about in the very next speech. Without giving those concerns, without developing an oversight mechanism for preventing misuse, we won't be able to gain the positive benefits to law enforcement and homeland security that would come from the good use of drones.

MR. WITTES: Catherine?

MS. CRUMP: Thanks for having me here today. I want to pause for a moment at the outset and note how unusual it is that we are having this conversation now. The reason it's unusual is that when a new technology is introduced in the United States, it is generally the case that it is introduced because law enforcement simply purchases and adopts that technology, the public learns about it many years after the fact and then there is potentially some debate about the issue. But because of the FAA's rule for now at least prohibiting the widespread domestic deployment of drones particularly by law enforcement but also for commercial purposes, we have the opportunity to have a real and engaged public debate about the role this technology should play in the United

States and I think that that is a really nice change from how these issues normally play out.

The ACLU is an organization that focuses on a broad variety of issues and drones pose particularly complex problems and opportunities. They raise privacy concerns of course. Some drones are weaponized, but all drones have cameras. They could potentially become a new avenue for surveillance of American life. But they also hold promise, for example, as a tool to hold government accountable. In addition to working on a variety of surveillance issues, I also litigate excessive use of force claims, and one of the best things that can happen in one of those cases is when we have footage of the incident that we can use because it is very helpful in determining what actually took place between law-enforcement agents and private citizens. In addition, drones are unique because they are tools for free speech so that especially when it comes to private uses they need to be regulated in a more sensitive way than your typical technology.

I'm going to focus my remarks primarily today on law-enforcement use of drones and the privacy implications of those. One question that has been raised is what is the big deal about drones? How is this different from what has come before? As Paul put it, is it an evolution or a revolution? I think there are reasons to think of it as a potentially more dramatic change in what Americans experience. It is true that there have been manned aerial surveillance in the United States for a long time, but purchasing a manned aircraft and operating and maintaining that aircraft is an expensive endeavor and that has imposed a natural limit on the amount of aerial surveillance that can be present in American life. A lot of police departments simply cannot afford to purchase an airplane or helicopter for surveillance purposes. Drones will potentially sweep away that limitation and allow smaller law-enforcement agencies that have never had this

technology to adopt aerial surveillance and potentially raise a widespread availability of this type of surveillance. In addition, drones have capabilities which I think have a real impact on privacy that aerial planes that we're used to simply haven't had. For example, as John has written about extensively, they can potentially stay aloft for long periods of time. We're not talking hours. We're talking days, or when certain technologies get discussed such as the possibility of very light aircraft that can float up in the higher reaches of the sky, potentially much longer, months or even years. Unlike a traditional aircraft or helicopter which can be easily detected, drones depending on how they evolve and are regulated could potentially engage in surveillance without being detected by the people who are potentially targets. I think those changes combined with the rapid development of cameras and our ability to analyze video in a way that hasn't previously been possible makes these very potentially very powerful surveillance tools. Everyone today has a smart phone and can snap photos with that. Not everyone. I am actually one of the few who doesn't have a smart phone. But cameras can zoom in to tremendous degrees that weren't previously possible. They can be equipped with night vision. And technology is developing to make it easier and easier to see through opaque surfaces. All of these changes together with the possibility of facial recognition, analytical tools being used to analyze footage, means that it could potentially be possible for example to simply film an area for a long period of time and then go back and reconstruct individuals' movements.

I think there are number of privacy risks associated with government use of this form of surveillance. Prolonged tracking of individuals is one of those. The Supreme Court by the way, and Steve Lacar who argued this case is actually with us today, decided a case called the "United States v. Jones" in which five justices seemed to reach the conclusion that prolonged surveillance of someone's movement in a public

space can become a search under the Fourth Amendment. So I think to the extent drones engage in that type of tracking, they also raise privacy concerns. In addition, drones have a lot of the same privacy implications that cameras have had. Chilling effects are one that people frequently talk about where people simply behave differently when they know they're under surveillance than they do when they have the security of not thinking that they're being observed. The ACLU put out a report on this issue in December in which we issued some recommendations. We are not opposed to the use of drones domestically. I think there is a broad range of valuable ways in which law enforcement can use this technology to meet legitimate law-enforcement needs. At the same time, we are concerned that they not become tools of general or pervasive surveillance so that innocent Americans have to worry about whether or not they're being subject to this kind of monitoring.

In addition, it would be nice, and I think conversations like are a start of it, for there to be a real democratic debate about the rules under which drones are adopted which of course is different from how surveillance technologies are usually adopted. I think there are a bunch of complicated here not just dealing with government surveillance but also with the private use of drones that are very thorny. I know you're planning on talking about private surveillance so I won't touch too much of that.

But I want to mention one other issue that is of concern to the ACLU which is the potential weaponization of drones. The way the public debate about this has evolved in the last few months I've almost found startling. When I first started thinking about the possibility of drones being equipped with nonlethal forms of force and purchased by law-enforcement agencies, I almost thought that was farfetched. But in fact, law-enforcement agents have expressed serious interest in this because it would allow them to for example contain crowds without having to have any officers present. I

personally find that to be a very scary example of the potential use of drones because I think the potential for abuse is too great. But it also gets you thinking about the fact that if any private citizen with enough knowhow can attach a camera to a drone, what else can they attach to a drone and what kinds of regulations are going to need to be put in place to make sure that we're safe from this possibility? One of the things I wonder about is whether drones will become a tool that's available to law-enforcement agents, but the public is severely restricted from using them because of safety and other concerns, raising the possibility that drones become yet another tool that enhances the ability of government to control and monitor citizens but that citizens themselves don't get to take full advantage of.

MR. WITTES: Thank you. Ken?

MR. ANDERSON: Thank you for this opportunity, and I'm going to focus on private party to private party uses of drones and the privacy issues that arise out of this.

I'd like to start with my late saintly mother back in the mid-1960s when she ran the social welfare stuff at our church and she took a gazillion telephone calls a day, and this was in an era long before ordinary people like us had things like answering machines and the ability to screen calls and do all the sorts of stuff we take for granted today, until my father simply stepped in and installed a switch on the telephone that would turn off the ringer. You guys do not look sufficiently shocked at what that meant in 1965. My mother's reaction and the reaction of many of the people who she worked with I, think today sounds almost unimaginable. She had serious qualms that she was actually being dishonest and that she was lying to people about whether she was in fact in the house by having something that turned off the ringer.

I want to fast-forward then from the 1960s to the mid-1980s at a time that

I was on the ACLU's National Free Expression Committee and at a time before you were born, my dear. The Pennsylvania ACLU as with many of the state-level ACLUs was trying to come to grips with new forms of technology available on telephones including things like call waiting, but In particular, caller I.D. The ACLU of Pennsylvania took the position, and this was never taken by the national ACLU, and was quite vigorously supported by important folks in the ACLU at the time, that caller I.D. was an intensely wrong way of denying people free expression because it essentially meant that somebody could not get to you, and that caller I.D. was actually a First Amendment violation that the state telephone regulators should eliminate because it eliminated the First Amendment right you had to reach somebody and communicate speech to them. Ten trillion telemarketer calls later, this attitude is entirely inconceivable to any person in this room and any person listening. That is, our notions of privacy have shifted in remarkable ways including our notions of privacy about person to person, private person to private person.

Let me bring this to the point of drones. How do they fit into this? One is on their own in relation to privacy, and second, as a sort of enabler technology, a leveraging technology in combination with the sensors, the cameras was mentioned, the possibilities of facial recognition, computer-enhanced ways of dealing with the material that is gathered through the sensors. The finally the ability to have something which is constantly out there and then can connected to the web. These technologies I believe, and I'm echoing in part Ryan Callow's views here, I think actually do wind up pushing our existing privacy structures to the breaking point in important ways that go beyond simply government, but go to how we interact with each other and what our social expectations of privacy are and how we believe that those should be embedded in various forms of law. In this obviously we have precisely, as the ACLU pointed out all those decades ago,

tradeoffs and conflicts here between free expression, First Amendment concerns, things like that, the notion of the public and the private, at the same time with also an evolving notion of privacy but in a really complicated way because on the one hand we wind up insisting that we've got the right to essentially turn the world away even at the electronic level, but at the same time we share so much. The point that I'm actually making in starting with privacy is I don't think that we can actually really talk about drones in relation to their impacts on these other areas, particularly their legal regulation between private parties, unless we talk instead about the prior expectations we have about privacy and the ways in which that is socially constructed and evolves in various kinds of ways.

We have to contemplate, and one could give a very long list of scenarios, but the easiest one for private party to private party usages would be that evolving drones will allow you to put a drone up in the air pretty much on a continuous basis and have it looking over into your neighbor's back yard and seeing everything that goes on there which may be nothing, and then stream that live to the web and attach to that computer-enhancement technology that enables it to pick out particular people and set up an entire gallery of everything that they're up to, and simply have that streamed live to the web plus enhanced collection of information stuff that is all just going up there. None of it is commercial. And it may not even be particularly maliciously motivated. But I would suggest that everybody in this room would believe that there is something profoundly wrong about that and that this violates some set of informal and formal notions that we have about the notion of intimacy, privacy, home, even though it's taking place out of doors potentially behind the wall that's not visible from the street.

Ultimately the question becomes in those cases are we going to wind up going beyond the assumption that you could do things like build a wall, you do things like put up a hedge, and that you didn't have all of this sort of stuff that makes everything sort

of instantaneously available to everybody else across the planet? Or are we going to essentially let those changing expectations have to fit in with the existing set of rules that we have or are we going to evolve the rules in various ways? One of the answers to this is very often given at the privacy level. Nobody is actually serious about any of this stuff because if were, nobody would use Facebook the way they do, nobody would use Twitter the way that they do, none of these sorts of existing social technologies would exist in the fashion that we have if people actually cared about their privacy in the way that we've traditionally thought about.

People do not think of intimacy as being private anymore. There is sort of a weird switch would be the argument. On the basis of no data except being the father of a teenager, I don't actually think that that's how it works. I have a strong sense that particularly the younger generations in this have an amazingly sophisticated sense of what their notions of privacy are about and the ways in which they expect that notions of privacy are socially constructed and are in fact fairly close to the bundle of sticks approach to property, that they have a view that what's appropriate in one setting for the use of a photo is not appropriate in another setting across the web for the use of a photo, the ways and places in which one can collect information and images about a person that are appropriate for one use are not appropriate for another use, and I think that actually we have increasingly younger generations that are extremely sophisticated in their views about the ways in which one unbundles the notion of the public and the private and separates it into a whole series of distinctly appropriate or inappropriate usages and they're profoundly naïve whether any of that is reflected in law. I think their expectation is that it ought to be in some way, that that's how we ought to see all these sorts of things, but they're profoundly naïve in thinking that it actually is.

Where this comes back to drones then again is as a leveraging

technology for all the rest of this stuff. You're absolutely right in suggesting that we have a moment to be able to address these things while the technologies are still being set in place and not waiting until effectively they're sort of hardened in some path. When it comes to private to private interactions in these ways, I think there will be a small or should be a small but really very limited realm for the criminal law and this stuff, peeping Tom laws that may have to be updated to take account of new kinds of technologies or stalking laws that wind up taking account of this stuff. But I think by and large most of this is going to fall first of all under state law and that most of this private party to private party stuff will inevitably fall under some form of civil law and nuisance law and the notion of what it means to have the quiet enjoyment of your property would be kind of the classic example. So that I think that we need to think about ways in which we need to update these things as a set of tradeoffs that not all of them run in the direction of protecting privacy. The notion that there is being in public is I think a really powerful notion of the ways in which other people can look, can see, can take photos, can do various kinds of things. But ultimately I think that the best thing that could happen in the private to private interactions would be some form of a model code, model set of laws aimed at states for their adoption in which we had a discussion up front about what the tradeoffs need to be better exposure and privacy.

Finally, and I'll close on this, would be the worst thing in this kind of area would be to allow the law to be driven by a series of really ugly, really bad cases in which we have not thought out the tradeoffs but the public is driven by something that is particularly ugly and then reaches to something that reflects that but nothing else.

MR. WITTES: Thanks very much, Ken. I should have mentioned this at the outset, but this event is being webcast so that we have a group of people who are surveilling this not from a drone, although that thing over there which keeps turning and

sensing is kind of eerily familiar. First of all, let me welcome our virtual participants who will also be tweeting questions to us so that when I go to questions from the audience I'm actually going to alternate between the physical audience and the drone audience who are being monitored. It gets worse and worse the more I say it.

SPEAKER: Voluntarily though.

MR. WITTES: Voluntarily, yes. They're subjecting themselves to monitoring.

So I'm going to start with a few questions for each of the panelists and then we will go to questions from the audience.

John, I wanted to start with you. You talked a bit about the national security side of this and we've had a lot of conversation about the privacy side of this. It seems to me that the part that is going to guide almost all of that is the safety side of it which we actually haven't talked about very much. That is to say, if the FAA on safety grounds allows less rather than more, there is less capacity for the intrusion of privacy, the size of the vehicles will be arguably probably smaller, as a result the concerns that you've articulated are less. So I'm wondering if you can talk a little bit about the safety side of it. How plausible is it that aircraft, how large and how far from the people who are flying them, are going to be flying how high, how soon.

MR. VILLASENIOR: We could have a whole week on that. I think I'll limit my answer to saying that I can't agree more that it's a complex problem. It is almost unimaginably complex to think about how in the world we're going to successfully navigate the safety challenges of having literally potentially tens of thousands of these unmanned aviation systems operated at potentially unconventional locations used for all of these different tasks. By consolation, I think the best minds in the business are on this problem and that's the people at the FAA who I'm sure are working very hard and I think

that will come up with a very reasoned approach, but the sheer mathematics of the numbers means that we're going to have some hiccups along the way and let's hope that they aren't too much.

The other thing I'd say is that the dial that we can turn, it is true that if we reduce to very little the amount of drone activity then the privacy and national security concerns get reduced, but then so does the economic opportunity and the innovation that accompanies them. So I think it's very important to have that perspective and have that balance and to open the skies with drones, to welcome them but obviously with a prudent eye toward the very complex safety issues as well as the national security and privacy issues that we talked about.

MR. WITTES: When you describe the opportunities, when you're thinking about the opportunities that it's important to open the skies to, presumably you're not thinking about the set of things that Catherine and Ken are anxiously wringing their hands about, whether it's peeping Toms or government surveillance of crowds without having to deploy personnel. What are the things that we should be excited about here?

MR. VILLASENIOR: I'll give a couple of examples. There's an enormous amount of commercial opportunities for surveying, for monitoring oil pipelines. Also in the law-enforcement field I think it's very important. There are many small police departments in this country that wouldn't necessarily be able to afford to have their own helicopter, but if they can use drones to monitoring something like a hostage situation, that could provide truly lifesaving information. So there's really a long list of these very, very beneficial commercial things.

The other thing is that, and I alluded to it in my opening remarks, there's a spinoff factor. There's a stunning amount of innovation that's going on in the drone world be it with formal companies some of which as I mentioned before are attending

this, hobbyists, university research labs and that innovation, this is the way it has always worked. In fact, back in the 1960s it was the space program and I would argue that for the 2010s drone are our innovative equivalent of the space program and will generate innovations that will spin out into beneficial ways that we can hardly imagine here. So for all of those reasons I think it's important to encourage them.

MR. WITTES: Catherine, I was struck when you were talking by, it's arguably not a contradiction but it's certainly an anomaly, you're describing the great promise of drones for purposes of government oversight and a great terror of drones in the hands of government. I was trying to think of what the analogy to that is that we've done in the past where we've said what a wonderful technology to use to spy on government and we're really excited about it as long as government doesn't use it to spy on us. I'm curious for your thoughts on that, whether there are analogues to that where we've said we love this technology in the hands of private parties and we don't like it in the hands of government and whether in any other area that's been a sort of sustainable line for us to take.

MS. CRUMP: I think you're right that it is a conundrum what to do about that. I think everyone's ideal solution would be if there were some way to promote all of the good and positive uses of this technology with none of the abusive ones, but of course it's difficult to do that.

I think in some ways this echoes a battle which the ACLU essentially lost about surveillance cameras. The ACLU does not like the fact that it is difficult to walk down the street in many major metropolitan areas without having your image taken by tens if not hundreds of surveillance cameras depending whether you live in Manhattan or somewhere else. And I think that's an example where the ACLU has been a staunch defender of the ability of private citizens to take photography particularly of the police in

public but worries about the capacity of the same technology in the hands of government. I think it's a really difficult issue because if you end up in a situation where every real estate agent is flying a drone for commercial purposes it is going to be extremely difficult to argue that the police who are investigating potentially serious crimes can't take advantage of the same technology. I think the argument that the ACLU and other civil libertarians make is that the police are simply different because they have powers over us that other private individuals do not have, but no one is saying it's an easy question.

MR. WITTES: That's a really interesting example though. For those of you who don't know, there was a real estate agent in Los Angeles who was I'm not sure prosecuted but disciplined for using a drone to take neat aerial photos of the houses that he was trying to sell. Listening to you talk about that, the thing that comes to mind is the anger that people felt toward the restrictions on the FBI using google searches under the old version of the Levy guidelines after 9/11 where the FBI is the one group of people or was under some interpretations in the country who can't google your name and sort of see what comes up. I wonder if you end up in a situation in which, to go to something that Ken said, that you have a sort of very restrictive set of rules on the basis that the police are different until the day something really bad happens and then you really can't sustain them because what you're actually preventing them from doing is what all of us can now do, go to Brookstone, buy a little $300, I almost bought one for this event, thing that you can control with your iPhone, and I wonder about the stability of it in the long run.

MS. CRUMP: The next time you should be beaming this from your drone.

MR. WITTES: Exactly. We will.

SPEAKER: That wouldn't look good on your expense report.

MR. WITTES: I'm not sure whether to direct this question to Ken or Paul,

so I'll direct it to both. You both started your remarks with a cautionary tale, but the cautionary tale seemed to me to pull in exactly opposite directions. Ken's cautionary tale is look how fantastically weird my mother's reaction to caller I.D. was 30 or 40 years ago or to turning off the ringer and how absurd the ACLU's reaction to caller I.D. was 20 years after that. It's just crazy to think we're really going to anticipate the way we feel about this stuff once it's integrated into society. We can't really anticipate it. And Paul's cautionary tale is here's a neat government program that didn't try to anticipate it, didn't try to think this stuff through in advance and it crashes and burns. So my question to you both is, and Ken sort of comes around to Paul's view by the end of this remarks that we've got to think this stuff through in advance, and I'm wondering is it realistic actually to think it through? Is it something that whatever judgments we come to today sitting here in an FAA rulemaking or in Congress, we're going to be your mother and 30 years from now people are going to be saying it's it quaint that they thought that drones X, Y and Z? Paul?

MR. ROSENZWEIG: I guess my answer to you is that there are no new questions, only the same question over and over again. The concept of government abuse of a new technology is as old in the dispute in London about arming the police and probably has antecedents that go back to the first time that anybody put somebody in charge of hurting the tribe or something like that. It seems to me that you can and should anticipate the potential for abuse, but instead of relying on inefficiency and resource limitations which is how we've kind of defaulted to protecting against these abuses, you have to turn that around and do the harder stuff which is training, hiring, oversight and regulation. It's not easy. It changes over time as the technology changes. But we don't disarm the police because of the potential for police abuse of the use of weapons. We try and hire the right guys. We give them good training. We have internal affairs bureaus

that examine every shooting. We discipline the guys who do it badly. We fire the guys who do it badly more than once. And we prosecute the guys who do it badly in ways that violate more important social norms. And that model will apply to the use of drones at least in the government sector. The private sector stuff that Ken is talking about, you have to figure out a different model. But in terms of governmental activity, that model addresses the problem and you just have to invest the resources and figure out what the rules are. Maybe it's that no police force can look in a window without a warrant, but they can fly up 200 feet, between 200 and 400 feet, only. Maybe that's the rule. I don't know the rules yet because I don't know the technology and that will change next week or next year.

MR. WITTES: Ken?

MR. ANDERSON: I think that it's going to be incremental, so going to Ben's question, I think the responses need to incremental as well. But they don't need to be in every case reactive, meaning something happens that basically offends people's notions of either privacy on the one hand, or alternatively, things that people think they ought to be able to do in the public spaces on the other. So I wouldn't want to see a sort of regime develop that develops entirely reactively on account of court cases addressing these sorts of things.

I do think that there is room for trying to think through at least some parts of this on the front end and think about questions that are already starting to arise even on an incremental basis. I am quite committed to the idea that much of this between private parties really exists at the state level and that it exists out of traditional existing bodies of law particularly things that I mentioned such as nuisance or some forms of tort or things like that. We know what happens in these cases. There is some horrific thing that happens that involves something, it involves drones together with cyberstalking

together some young person tosses himself or herself off of a roof in despair and then there's a reaction that enacts a sort of criminal set of sanctions and all sorts of things like that. That I think would be a very bad approach to this. I think that at least to that extent we can anticipate some of those situations on an evolving basis and try to have a discussion up front about what tradeoffs really have to be included.

MR. WITTES: Let's go to questions. I'm going to start with a Twitter question, but when I call on you, wait for the microphone and please start by saying who you are.

SPEAKER: We have our first question from Matthew Shryrer in Urbana, Illinois, and he has a question about using drones as a tool of free speech, how would the argument that journalism has prior restraint versus regulations and privacy play out?

MR. WITTES: Let me take a little bit of a crack at that and others here who do a lot of First Amendment law may have other thoughts on it. It seems to me that the answer to that would have to be that just as with a lot of aspects of journalism, there may be legal limitations on how certain information gets collected including how you would use drones in collecting certain information. It would be very hard I think to argue that once you have obtained certain information barring certain extreme cases that it would be proper even if obtained somehow illegally with a drone that you would enjoin in the publication of it. Do people generally agree with that?

SPEAKER: I think that's exactly right. The press can't beat information out of someone and they can't engage in breaking and entering. It's still a crime even if they are the press. But we have a large body of law that says that if the press receives information even if it is collected in an illegal manner, even if it is leaked in violation of classification rules that have been for years, that we're not going to restrain the press and that would seem to be that this actually plays very much into my mantra which is there's

nothing new under the sun and it's an evolution. I would assume that the same rules go to drones.

MR. WITTES: Sir?

MR. MAGNUSEN: Stew Magnusen, "National Defense" magazine. Can you address the September 30, 2015 deadline maybe first in terms of technology? There are a lot of issues there to be worked out. You mentioned the com link issue. That would maybe require some autonomy onboard these aircraft for them to return safely, also the sense and avoid technology, then also the regulatory part. There are a lot of associations out there, the Pilots Association, Air Traffic Controllers Association, who all say this is going to take a lot of rewriting of the way we do things and a lot of consideration. I guess that's my basic question. Is the congressional mandate realistic?

SPEAKER: I can't answer all of those things. That would be a very long answer and we'd all fall asleep. But for the benefit of those who may be a little less familiar with the legislation, when you came in the room, and for those of you on the webcast I assume we'll be making it available, there's a two-page sheet that was helpfully prepared by Harley Geiger of the Center for Democracy & Technology and he has done us the favor of going into the legislation and doing computations of 270 days after enactment what does that mean? In sum, there are two broad classes that are addressed in this legislation. There's what are called civil unmanned aviation systems so that these are drones operated by commercial enterprises and the like. And then there are public unmanned aviation systems which are operated by police departments, fire departments, national government, state governments and so on. With respect to public unmanned aviation systems or government drones as some people refer to that, May 14 of this year is the date after which or at which there is going to be expedited licensure for the use of those government drones.

With respect to civil unmanned aviation systems, it is November 10, 2012, where there is going to be a comprehensive plan developed and that plan will call for the integration of those drones into the national airspace by September 30, 2015. And there is also sort of an early escape valve in there. On August 12 of this year there is the early integration of safe drones which provide the option but not necessarily the requirement for the FAA to allow certain types of drones at that date. So in addition to that there's about 10 or 15 other complex overlapping headlines and this wouldn't be the forum to go through them all, but it's a complex process.

MR. WITTES: Paul?

MR. ROZENSWEIG: I just wrote Ben a note, only in Washington is 3-plus years not enough time. It is a complex issue and it deserves a great deal of attention, but my own sense is that if the FAA has a will to get it done, it can and should be able to get it done. If it doesn't wish to, it can obviously miss the deadline, but that's the nature of politics. But 3-1/2 years to think this through is not an unreasonable expectation.

MR. WITTES: Anything to add on this end?

MR. DILLON: Ken Dillon -- Press for any of the panelists. What is your thinking on the potential uses that foreign governments might make of drones within the U.S., for instance, to do some major spying? Will that give them an advantage over overhead assets or for instance to track and kill a dissident?

MR. WITTES: Ken, you've given this subject in a slightly different context a lot of thought. For those of you who don't know, Ken has written a great deal about the law of U.S.-targeted killing including but not limited to by drones. What happens when the technology is cheap enough and the airspace is open enough that other governments want to get in on the action here?

MR. ANDERSON: I think when it comes to other governments that everything that I said about private party to private party stuff essentially needing to evolve incrementally and state law stuff and it's basically civil and tort liability and nuisance. None of that do I think applies to foreign governments acting in the United States. I think it's a perfectly appropriate area for the U.S. government simply to come down and say either nobody does this at all or if you do you've got to come and have a long conversation about what you're doing it for and why. And surveillance of individuals is all going to fall under a whole series of national security concerns and all of that. Obviously killing somebody is completely off the map. We regard that as a hostile act possibly leading to war. So in those sorts of settings I think the question is really about surveillance in a sort of practical sense. I don't think that the United States government has any reason to up with surveillance using high-tech means by foreign governments of their citizens or ours. I don't think that any of the things that we've raised here about the uses of these things by various folks would apply to foreign governments at all.

MR. WITTES: We have another Twitter question.

SPEAKER: Yes. We have a question from Amy Stepovich who is Washington, D.C., an attorney with Epic Privacy. She wants to know should there be use limitations to prevent drones bought or licensed for the narrow purpose to be used widely?

MR. WITTES: What an interesting question. This stuff collects, these are platforms, the more sophisticated ones, are just incredible intelligence collection platforms. Let's say you are a weather channel that acquires them for meteorological purposes or for a traffic reporter. These are great for figuring out. What happens to the volume of data that you collect that then has potentially other applications? Whoever wants to jump in on that, it's a great question.

MS. CRUMP: This has come up to some degree already in the context of the Customs and Border Patrol's use of drones. Congress authorized expenditure for Customs and Border Patrol's to buy certain drones to patrol the border, both the southern and the northern borders, and then in December, "The L.A. Times," a reporter named Brian Bennett came out with a fantastic article discussing how CBP was not exactly lending, but putting its drone technology at the assistance of local law-enforcement agencies. Some members of Congress expressed consternation that this technology which had been authorized for one purpose, securing the borders, was now being used for a law-enforcement purpose by I think a local North Dakota law-enforcement agency that they certainly didn't anticipate when they authorized the program. I think in that case at least members of Congress think that that kind of limiting principle would be appropriate.

MR. WITTES: Paul, I imagine you have a different point of view on this, to go back to your earlier point that there are no new issues. This is the classic example of this. Paul when he was in government dealt a lot with issues of data collected for one purpose and the Department of Homeland Security would find out that it would be really good to use passenger manifest data that people give to airlines to use for counterterrorism purposes, and it's really good to know who's on airplanes. You've dealt a lot with this question of when can you reprogram data collected for one purpose for a different purpose. Is it different if it's a private party with a drone or is this just nothing new under the sun?

MR. ROZENSWEIG: I hate being predictable. But nonetheless, you've correctly predicted where I would come down. To my mind, the right way to address this is in the consequences at the end. Think of what we're talking about. We have the CPB and it has a UAV. It's not being used full-time. It's a valuable asset notwithstanding the

fact that they're cheaper than helicopters, they aren't free, it's a very valuable asset. It can be used for another perfectly lawful purpose. If the North Dakota police want to use it to surveil their wives on their shopping trips, that's a different thing. But if the North Dakota police force wants to use it in a hostage situation or to follow a suspected drug dealer, that's obviously a good and lawful purpose in pursuit of a legitimate public end. Why would we begin from a premise of purposefully making ourselves inefficient, purposefully making ourselves limited? I can certainly see in the end saying that that evidence might not be used in court or something like that if you feel really strongly about the particular use, but to my mind the right answer is to define what are the lawful uses, and, no, CBP cannot loan this to North Dakota to go and look in on a political meeting of the North Dakota Tea Party or the North Dakota ACLU. No, they can't use it to surveil in ways and means and for purposes that would be outside the zone of their legitimate law-enforcement concern in the first instance. But if the end is legitimate, it seems to me that we make a mistake in hewing to the purpose limitation, that the right method is the consequence limitation at the other end. How that is used; that evidence shouldn't be used unless it meets a reasonable suspicion standard or some limitation, some gate of some sort, a gate to be determined obviously, as time goes on as the technology gets developed. But I don't believe in enforced self-inefficiency of government.

MR. WITTES: Do you want a brief rejoinder on that?

MS. CRUMP: I'll try to keep it brief because I think we could probably go around and around on this for the rest of the panel. We place limitations on technology like this all the time. For instance, you can't do a Title III wiretap on people in all circumstances. There are specific crimes for which you can use that technology and others for which you cannot so that I think there is a place for these types of restrictions. May I mention one other thing?

MR. WITTES: Sure.

MS. CRUMP: On the ACLU caller I.D. question, it's a side issue, but we actually still don't have caller I.D. on our main switchboard line, and the reason for that is so that people can call us and tell us stuff anonymously and know that they can be secure in doing that.

MR. WITTES: Sometimes the ACLU gets described as outside the mainstream on a variety of issues. I can't imagine that there is a single issue on which that is truer than the one you just described.

SPEAKER: I'm Michael and I'm a private lawyer in private practice here in Washington. The FAA does have this deadline coming up in August where they have to decide what safe drones to allow in the national airspace system and you all have different concerns about safety, national security and privacy. My question is what do you want the FAA to do in August of this year about opening up the system for safe drones? Let me give you some choices to choose from. One is do nothing and have them put off the deadline until 2015. The second choice, to allow commercial drones with line of sight and under 400 feet restrictions so that your California real estate agent could take his pictures of houses. Or sort of adopt the regime of only approving drone operators on a case-by-case basis for showing that it's in the public interest. What do you want them to do?

MR. WITTES: Do you want to address that?

SPEAKER: I'm not going to answer it in full, I don't have all the answers in full, but I think it would be a mistake to rush into allowing people to operate drones over populated areas without due attention to the dangers related to that. I'll just give an example. The Academy of Model Aeronautics which is the national community-based organization that deals with model aircraft hobbyists in this country has long recognized

the importance of not operating platforms in that general size range over populated areas and I think that that is a point of view and set of experiences that needs to be respected, and I frankly don't trust that real estate in August would respect it even if they have the best of intent. So I think we need to be very careful not to rush headlong into that.

MR. WITTES: What is the size cutoff? You can literally go to a hobbyist store and buy model aircraft below a certain size that you can fly at reasonably impressive distance that doesn't raise anybody's alarm bells. Realistically, what's the difference between the sort of thing that nobody is worried about and the sort of thing that raises those concerns?

SPEAKER: One easy answer to that is that the Academy Aeronautics has extremely good safety guidelines and anything that is operated in accordance with their rules I'm not worried about at all. For example, their rules don't allow these first-person view remote unmanned aviation systems that are over 10 pounds. It has to be under 10 pounds. Anything that's compliant with the AMA's rules which in the language of this FAA bill are a national -- let me make sure I get this right. It's a national community-based organization I believe is the phrase. A nationwide community-based organization. Anything operated in accordance with that is absolutely fine. Once we get into the heavier metal, something that weighs 200 pounds or 500 pounds or potentially 50 pounds under certain circumstances that potentially could raise concerns, that's obviously a potential cause for discussion.

MR. WITTES: Does anybody else have thoughts on what the FAA should and shouldn't do by August?

SPEAKER: I don't think that it should actually touch any of the issues that I raised, meaning that I think that the private party to private party stuff isn't really the FAA's area. They're not a privacy agency; they have got a different set of concerns, and

those concerns very clearly from what's been said here are going to be far and away hugely difficult to wind up meeting. I also think that there is a sizable concern among the existing hobbyist community or the model airplane community. These folks are actually very concerned about what happens if you toss aside these kinds of informal standards that have been raised by these folks and open things up to a wild west out there and that it wouldn't take very many safety incidents of a serious kind that could potentially shut the whole thing back down the other way.

MR. WITTES: Yes?

SPEAKER: My name is -- I'm a Japanese scholar working at Johns Hopkins University. I'd like to ask you about -- the most you used the wrong technology in the history of the war is Afghanistan. What is the achievement of drone technology in Afghanistan? I think now you have lots of positive sides but also negative sides such as drone technology stimulated anti-American emotions or hostility of local people or the Taliban.

MR. WITTES: The focus of this event is on the domestic side and not on military applications abroad. That said, this is a subject that when people hear the word drones they don't think of domestic law enforcement or news gathering. They think about predators. Very briefly all of you, how do you assess it and to bring it back to the subject, how does that legacy and origin affect the domestic discussion?

SPEAKER: I'm going to summarize and really reduce it. What I'm going to actually suggest is look at my name in the program and send me a direct email about that and I'd be happy to talk about this at length because I think that is does drag us away from the domestic side a lot. So I'm going to punt in part. But I guess the one thing that I would say about this is that there is an enormous technological feeding back and forth of the development of the technologies in ways that the requirements of the

battlefield and particularly the use of drones as not simply another air platform, weapons platform in conventional war, but the use of drones as being a mechanism both for gathering intelligence and then using force based on the intelligence gathered, puts an enormous amount of pressure on the development not so much of weapons, the weapons themselves are shrinking and getting smaller, but that the real developments that are underway here are in the sensor arrays and in the ability to have software that will wind up processing what's coming through increasingly sophisticated and varied kinds of sensors. That then feeds back into the domestic sphere in all sorts of ways precisely all this stuff that drives the innovation in the commercial sector and all the good things that we're going to wind up seeing in the way of innovations, but you raise the ability to look inside buildings. In Afghanistan and in Pakistan we would like to be able ideally to use drones to be able to get some idea of how many civilians are inside the building. We would like to be able to use drone sensors to be able to get some notion of what the loadbearing impact is of those particular walls in relation to hitting it with a particular kind of weapon and the kind of collateral damage that it's likely to cause, all of which has enormously important and beneficial commercial applications back in the domestic sphere, all of which has got to compound your fears about what it is that government agencies could do with that kind of ability domestically as well. So I think it has to be seen as sort of feeding on one another in ways that are both positive and negative.

MR. WITTES: We have another Twitter question and then in the back.

SPEAKER: We actually have two questions that are related so I'm going to put them out at once. The first one is from Harley Geiger who is an attorney for the Center for Democracy and Technology. His question is, "To what extent does the FAA's mandate include privacy and where should Congress step in?" Then a related question

is from Jason Koebler who is a higher-education reporter for "U.S. News." He asks, "Is there a need for the government to be able to detect and track drones at will and do you think they should be licensed by FAA referring to private or commercial drone?"

MR. WITTES: Who wants to take either of those?

SPEAKER: The one-line answer I have for private-to-private interactions won't surprise anybody by now. I don't think that the FAA should be getting involved in private-to-private privacy issues in this. I think it's got its hands full with everything else that it's correctly trying to do in all of this stuff.

MR. WITTES: Catherine, do you have a sense of to what extent the FAA's mandate, I actually don't, includes any of the privacy issues that you're concerned about?

MS. CRUMP: I think that's a hard question. The FAA's mandate includes protecting people and property on the ground. That has been interpreted as a safety mandate by and large. There are old cases dating back to the 1970s in which the FAA interpreted that mandate more broadly, for example, to include things like dealing with the environmental impacts of air traffic. If its mandate can encompass environmentalism, then perhaps it could also encompass other concerns which arguably impact people on the ground. I am skeptical that the FAA would want to interpret its mandate in that direction. So I imagine this is an area where Congress may need to do something. CDT has suggested at the last the FAA should be conducting a privacy impact assessment to look at privacy questions and I think it is unfortunate that the U.S. is anomalous in now having a federal-level privacy commissioner who systematically evaluates the impact of government actions on privacy.

MR. WITTES: Paul?

MR. ROZENSWEIG: Surprisingly I agree with Catherine, but I would put

it a different way which is I can imagine no worse forum for discussing privacy concerns than the FAA. It's not built for that. It would be like asking the EPA to think about national security concerns or the Department of Commerce to think about education, though they do a little bit. Its apples and clowns even. As I said in my opening remarks, I think that the privacy issues are vital and if you don't think about them you'll get the wrong answer because you'll wind up losing all public support for the programs however they're formulated. But the FAA is great at safety issues, it's great at air-traffic control issues, all of those sorts of things that we well within its zone, but I would want us to have that privacy discussion somewhere else, in an ideal world, in the Privacy and Civil Liberties Oversight Board which Congress authorized in 2007 and still hasn't started.

MR. WITTES: Yes, in the back.

MR. JASON: Carney Jason. I'm a technology analyst. Sometimes we have a habit of throwing out the baby with the bathwater. Here we're talking about privacy issues and all of those sorts of things, but there are times that a lot of this can be used legitimately for rescue purposes and that sort of thing, hovering over with repeaters so fire departments can speak to one another. In New Orleans after Katrina they were not allowed to fly drones with cameras which would have been ideal to help control what was going on. Instead, somebody got clever and they taped them to the skids of the helicopters. Is anything going on now to ensure that these valuable uses are not caught up and tossed overboard because of other concerns?

MR. WITTES: Paul?

MR. ROSENZWEIG: Yes. I agree completely that there is a huge positive value. John has talked about the commercial value; you're talking about the public-safety value. To my mind, the right answer is regulation. We should authorize the good uses and then be very cautious and careful about the bad uses and the fears that

animate people like Catherine. My fear is that by not acknowledging the legitimacy of Catherine's fears, you're now personifying all privacy, Catherine, but by now acknowledging the legitimacy of Catherine's fears up front, we'll wind up in the same place that we were with the NAO which was the exact same thing, we would have had great uses for national technical means in Katrina and we weren't permitted those either precisely because of fears of Big Brotherhood.

MR. WITTES: Stepping out of my role as moderator for minute, there is one thing I would add to that which is that there is something that we're doing to make sure that we don't throw out the baby with the bathwater, which is that Congress stepped in and ordered the FAA to have a set of rulemakings on this subject and that was a very deliberate effort to jumpstart what had been perceived as a sort of stalled set of processes.

MS. TOBIAS: My name is Gloria Tobias and I'm a public school teacher. Do you know of other countries that are grappling with how to regulate domestic use of drones that we could look to as examples or you could direct us to?

SPEAKER: I don't have a full answer to that, but I can say that there have been estimates that as to the drone industry that there will be $100 billion spent on drones over the next decade or by the end of this decade. It's an enormous global industry. Dozens of countries are involved. I understand or I've been told that Australia as some very innovative rules with respect to allowing drone use. Pretty much every country in the world with any kind of a technology infrastructure or industry is getting into the act. We'll see all sorts of flavors, but I don't have the specifics.

MR. LECAR: I'm Steve Lecar and I'm a lawyer in private practice in D.C. Perhaps this would be best directed to Catherine. I find the Center for Democracy & Technology's model legislation to be pretty good, it might be helpful to have private right

of action in there, but what's happening with Congress? Are they doing anything with this or are they having oversight hearings on this?

MS. CRUMP: Privacy wasn't included really as a discussion topic I don't think in the most recent round of legislation that was passed. There have been some interesting developments since then and my other panelists here who actually spend more time in D.C. than I do may have might insight into this. I think there has been an upsurge in concern about privacy. The trade organizations that are looking to promote the use of drones have gotten somewhat concerned about this development and the impact it may have on their industry. They've been approaching various privacy organizations and also congressional staffers to try to see whether there is something they can do preemptively to find some potential common ground here so that this technology can move forward and not be completely stymied by the privacy concerns. I don't know if maybe others know more.

MS. LUCEY: I'm Danielle Lucey with AUVSI's "Unmanned Systems" magazine. I was wondering because of the pervasiveness of privacy issues with the biggest technological advancement in the last 15 years which is the internet what sorts of lessons learned do you think we could bring from that industry into our discussion about privacy and unmanned systems?

MR. WITTES: What a great question. We've already learned the lessons of caller I.D. and turning the ringer off. How does the internet play into this?

SPEAKER: I think one observation, and Ben made this in some sense before, is that who could have known back in 1995 that such a thing as social networks would even exist and the complex privacy issues that have accompanied them? As Ben suggested with drones, I think it would be presumptuous for any of us to sit here and know that 15 years from now we can sit here today and say exactly what those are going

to be. I think humility with respect to technology and what we can't predict is probably important as we move forward.

MR. WITTES: We have about 2 minutes left, so why don't I give each of our panelists a chance to wrap up? Ken, do you want to start?

MR. ANDERSON: I guess the thing that I would emphasize and it actually goes to the last question that was asked here is that when it comes to private person to private person stuff, I've mostly emphasized it as though it's sort of individual to individual, but there will be a whole different layer of large-scale institutions, corporations, nongovernmental but private, and we're going to have a whole series of other questions related to their use of drones in this. Second, the other thing I'd stress would be that although there are certain functions about drones in the private-to-private setting that really are just about drones, where they go, what they watch, how long they're there, all of those kinds of questions, most of the questions that I think will actually drive the privacy concerns this way are going to be the ways in which drone technology is embedded with other technologies and essentially serves as a leveraging platform for things like the web, for other forms of surveillance and the dissemination of all of that. So I think it's the leverage package that ultimately will concern us.

MR. WITTES: Catherine?

MS. CRUMP: I think I'll start where I began and say this is a unique opportunity for us to try to build privacy protections into the regulations that govern drones. We ought to be taking advantage of that. And, again, the ACLU is not opposed to the use of this technology. As others as mentioned, there are many valuable uses. And hopefully if we can think through these things at the outset everyone will be better off.

MR. WITTES: Paul?

MR. ROSENZWEIG: I'd make two points. The first one, picking up on the very last question, is that I think the right answer here is developing the right systems. Static rules about privacy or use will be overtaken by the technology as quickly as the rules about internet usage were. We tried to address internet usage with a kind of concrete set of rules and all of a sudden big data is flooding around the ramparts of privacy protections intensely. I don't know what the answer is going to be in terms of drones because I don't know where the tech is going to go. I'm humble as John says. So the right answer is systems of systems, systems of oversight. The other second point I would just make is, Ken, if you fly your drone over my house, I'm shooting it down. Self-help is the answer.

MR. WITTES: Countermeasures. John?

MR. VILLASENIOR: I think just in closing that drones are like really in many ways any other technology in that the benefits in general far outweigh the downsides and as long as we're attentive to that I have high confidence that it will all work out.

MR. WITTES: 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.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2012