THE BROOKINGS INSTITUTION

THE FUTURE OF CIVILIAN ROBOTICS

Washington, D.C.

Monday, September 15, 2014

PARTICIPANTS:

Moderator:

BENJAMIN WITTES
Senior Fellow, Governance Studies
The Brookings Institution
Co-Founder and Editor-in-Chief, Lawfare

Panelists:

JOHN VILLASENOR
Professor, Electrical Engineering and Public Policy, UCLA
Nonresident Senior Fellow
The Brookings Institution

WELLS BENNETT
Fellow, Governance Studies
The Brookings Institution
Managing Editor, Lawfare

GREGORY McNEAL
Associate Professor of Law
Pepperdine University School of Law

* * * * *

P R O C E E D I N G S

MR. WITTES: All right. I think we're going to get started. Welcome to the Brookings Institution and to our snazzy new hall. My name is Benjamin Wittes; I'm a Senior Fellow in the Governance Studies program. And I'm joined on my right, your left, by Wells Bennett, and on my left, your right, by Greg McNeal. I'm going to dispense -- well, I hope to be joined shortly in a disembodied presence by John Villasenor. I'm going to dispense with biographies because we've got a lot of stuff to talk about and I'd like to -- you guys have people's bios there.

Before I forget -- which I will do -- the hash tag for this event for those who want to Tweet in questions who are joining us on our webcast is #Robotics and we will have people who will be monitoring that and can route questions as appropriate to me.

So I had my first encounter with regulatory aspects of civilian robotics a couple of years ago when I was admittedly impulsively organizing a very amateur drone fight in connection with a website that Wells and I run called Lawfare. And Lawfare is devoted to national security law and we were interested in sort of the question of proliferation of technologies down to the level of individuals and what people could do with them. And so we thought it would be fun to buy off the shelf drones and see if we could modify them and dog fight them and see what would happen if a bunch of totally untrained people who had no background in robotics tried to have a drone war. It was great fun and you can read all about it on Lawfare, but one of the things that happened while we were preparing for this event is that a gentleman -- I'm not making this up -- decided that it would be an appropriate thing to do from Adams Morgan to take a drone onto his rooftop and fly it directly toward the White House. And the gentleman in question as will happen every now and then, lost control of the drone in question and it

crashed. And so he did what any good citizen would do in this situation is he hung up "lost drone" photos all over his neighborhood and I posted one of them on Lawfare because actually one of the people who works in GS found one on the way to work. And so I posted it up on Lawfare and he actually found his drone which was heartwarming. And he got a call from the Federal Aviation Administration saying, you know, actually you're not allowed to fly a drone in Washington because it's part of a -- there's a flight restricted zone around the DC area and you're not allowed to do that. And we were about to do the Lawfare drone smack down and we thought well this couldn't possibly apply to use because we're flying little things that are, you know, about yay big and that they have, you know, 150 meter radius, you know. These couldn't possibly apply to us, but we took a look at the rule in question and it kind of by its terms if read literally seemed to. So I posted a notice on Lawfare, you know, memo to the FAA saying here's exactly what we're planning to do, here's exactly where we're planning to do it. If you've got a problem with this you'd better let us know. Rather to my surprise I got a call a few days from the FAA that said they regarded the Lawfare drone smack down as illegal. So I asked them well what if we used like, you know, like model helicopters, you know, that are this big that fly, you know, this high? And the answer was well that would be illegal too. And so we actually cancelled the DC appearance of the Lawfare drone smack down. We moved it out. It became the battle of Third Manassas because we had to move it outside of the DC flight restricted zone. And the result of this was that I got interested in this question. We all have these, you know some more than others, but we all have these robots now and they're raising all kinds of amazing issues, difficult issues affecting lots of different areas of life.

So I hear that John Villasenor is now with us. Is that correct? Momentarily? Okay.

So around the same I started talking to John, who will magically appear behind me.

QUESTIONER: Drone John.

MR. WITTES: Drone John. And Wells about sort of organizing a paper series that took a lot at, you know, a broad range of issues in which robotics are kind of making their way into the civilian sector and raising sometimes difficult questions, sometimes just sort of head scratching questions, some of them very immediate that are really upon us right now, and some of them very far off, probably none farther off than the one that I wrote about in my paper with Jane Chong. But we decided to take a broad look at it and we have now released the first six papers of this series and we thought this was kind of a good time to have a little event in which we kind of lay out some of the stuff we've been working on and chew it over a little bit.

So to give you a basic overview of the paper series, John -- who is now -- the disembodied John Villasenor is now behind me -- led it off with a paper on driverless cars and liability issues. So this is actually a really -- I'm going to be very brief about each of these because the people in question will talk about them themselves -- but, you know, we now have cars with a great deal of autonomy driving themselves around in different parts of the country. And it's a really interesting question when one of them crashes into somebody who the drive is for liability purposes and what -- how you want to allocate risk and responsibility there.

The second paper -- and I'm very much regret that she is not able to be here today because -- but I do commend to you both the paper that Heather Knight wrote and also some of her videos that are both on her Marilyn Monrobot site and also the TED talk that she gave. So Heather is a roboticist who works on human-robot interface interactions. And one of the things that she does is she tries to use performance and she

built a little robot comedienne to do standup comedy. And it's a way of kind of engaging what modes of human-robot interactions people are more and less comfortable with and willing to engage than others. And so Heather wrote us a paper about what you might think of as pre-regulatory issues which, you know, when you design things badly such that humans are anxious about the interactions you raise regulatory issues. When you design things so that humans are comfortable with the interactions, you don't. And so she raised a series of questions about how in a long pre-regulatory sense good design and good thinking about the culture of human-robot interactions can alleviate some of the issues that you might otherwise have to regulate in order to address.

So then Greg wrote a paper on -- again I'm going to leave those of us who are here to describe the papers themselves. Both Greg and Wells wrote papers about privacy issues involving drones. Greg, police use of drones and Fourth Amendment issues, and Wells about, you know, privacy in personal interactions. You know, you guys can all go out and buy a drone and take pictures of one another. And that actually raises a set of privacy issues that numerically is much more significant than the issue of police using drones.

So what we're going to do is I think assuming that we can hear him and he can hear us, John is going to lead off by talking a little bit about his paper. Greg will then talk about the cops and Wells will talk about how dangerous you are all to each other and what we should do about it. And then I'm going to finish it up by talking a little bit about the paper that Jane Chong and I wrote about how you all are cyborgs and we need to, you know, regulate you as such.

John?

MR. VILLASENOR: Let me first start by asking if you can hear me?

MR. WITTES: Yes.

MR. VILLASENOR: That's okay. Okay, great. Well, thank you very much. I want to start by thanking not only those -- I can only see the three folks on the stage but I know there's a room full of people so I'd like to thank all of you for taking a few minutes out of your very busy day to come to the this event.

What I looked at in this series was the issue of products liability, or products liability specifically in the context of driverless cars or more formally autonomous vehicles. To put things in context we'll start off with a sobering statistic. Motor vehicle accidents claimed over 33,000 lives in the Unites States in 2012 and that's a number that corresponds to an average of over 90 fatalities every day. And many of these fatalities are directly attributable to a simple unfortunate fact that while most drivers are careful and conscientious some are not and motor vehicle accidents due to mistakes, poor judgment, poor driving skills, or outright criminal negligence exact really an enormous societal toll. So against that backdrop it's important to recognize the incredible safety benefits that properly designed and implemented vehicle automation can bring to the entire motor vehicle industry. And of course all of us are users of motor vehicles. There's often articulated a concern that well, hey, we really shouldn't even begin to let autonomous vehicles out on the roads until we have fully resolved the products liability issues that will accompany them and one of the points I was trying to make or hoping to make in the paper is that we've actually really got a pretty good framework for addressing products liability and there's really no reason to expect that framework won't be able to adapt and then address the inevitable liability questions that will arise as autonomous vehicles become far more common.

Just to kind of give a level setting I'm going to give a three minute overview of products liability. As I think many of you probably already know products liability provides the legal framework for seeing remedies when a defective product or

misrepresentations about a product cause harm to persons or property. And it's a complex and evolving mix of both tort law and contract law. Tort law addresses questions such as negligence, design defects, manufacturing defects, misrepresentation. And while contract law is implicated by the commercial nature of product market and sales which then create explicit or implicit warranties regarding the quality of a product and what it's fit to be used for. And when the product then fails to meet those implied or expressed warranties then the seller could be liable for a breach of warranty. So there's both tort law and contract law.

So if you look at the landscape of products liability law over the last 30, 40, 50 years products liability law has proven to be incredibly adaptive to new technologies. It's been in fact one of the most dynamic fields of law since the middle of the 20th century. And in part this is because the new technologies that have emerged over this period have led Courts to consider a continuing series of initially novel product liability questions and then as case law has built up and there's been some feedback cycles with case law and other legal standards that in general, and of course there are exceptions, but in general the Courts have proven quite capable of addressing these questions. And given this strong record of adaptation to new technologies there's really no reason to suspect that the legal system will be unable to address the products liability questions that are going to arise as vehicles become more autonomous. Of course we already have quite a bit of autonomy in many aspects in vehicles but that's going to change. Vehicles are going to become even more autonomous in the future.

So one of the things I was recommending is, you know, is recognizing the tremendous flexibility and adaptability that product liability has already shown in previous decades. I had also suggested the preemptively resolving liability issues should not be a precondition to commercial roll out of autonomous vehicles for many reasons

including the fact that it is simply impossible to, for example, legislatively anticipate and then address all of the complex products liability questions that are going to arise with relation to autonomous vehicles in the next 20 years. You simply can't possibly do that and that would be an impossible exercise that would simply delay the many benefits of the technology in an impossible attempt to anticipate all the possible things that might go wrong.

Another think I recommended is that Congress should not preempt state tort remedies with respect to autonomous vehicles. And to give context to these tort liability cases and contract cases are the province of State Courts. They're not generally addressed in Federal Court. And there's been some suggestion that autonomous vehicles are so new that we've got to dispense or take away from the States even the right to have State Courts address products liability questions in relation to autonomous vehicles. And I've argued that that is a mistake; that questions of tort law have been in the province of states and while that doesn't meant that every state always gets it perfectly in every case there's no reason to preempt the states in favor of the impossible task of trying to find one overarching Federal framework that would address everything.

So let me stop there. There's many more things that could be said but I want to be respectful of the time. But I think products liability is a fascinating aspect of autonomous vehicles and I look forward to the chance to discuss this further as the program continues.

MR. WITTES: So, John, before I turn to Greg can you just give us a sense of, you know, a very brief sort of state of play of where we are with autonomous vehicles? You know, what is and isn't on the roads and at what state of autonomy and have there been any liability issues that have arisen so far with them?

MR. VILLASENOR: Yeah, a great set of questions. So autonomy is a

continuum and in fact there are some formal definition of different levels of autonomy, but all of us presumably have had experience with cruise control, right, which is a form of autonomy, right. The car does its own driving. There's many cars -- there's -- antilock breaking has been a feature of cars and/or vehicles for, you know, decades now. More recently there's many cars today or motor vehicles today that are sold with what are sometimes called "driver assisted technologies". These will do things like braking, automatic braking to help prevent or to try to prevent or to help mitigate frontal collisions, that is a collision when a vehicle is going to collide with the vehicle in front of it. There's technologies for helping with parallel parking and so on. So basically autonomous vehicles are already in some sense moving into the commercial mainstream. What we don't have of course is the other end of the spectrum where, you know, the sort of science fiction thing where you, you know, get in the car and you don't event sit in the driver's seat, you sit in the passenger's seat and nobody is in the driver's seat and you press some buttons and it whisks you to your destination. The technology to do that or nearly that is in fact being tested in various places but it's not actually -- you can't obviously buy a car that does that. So the issues with getting more autonomous vehicles on the road are the technology itself, and the technology has become remarkably capable and will become even more so in coming years. And there's also the laws. In other words to what extent do states allow autonomous vehicles, however you define that, to be on the road? And an increasing number of states have looked at laws and in some cases have enacted laws that subject to certain restrictions are allowing some level of we call autonomous vehicles or what are more generally called "driverless cars" on the road. But the numbers are still small and the numbers of states that have actually passed legislation is also pretty low.

So with all of that as background I am not aware to date of any actual

Court case that has arisen with respect to autonomous vehicles as we talk about them. There have certainly been Court cases related to antilock braking and things in the past, but the more advanced forms of autonomy that we're talking about I think and for most of the people in this room, I'm not aware of any Court case. That doesn't mean that there hasn't been any and there certainly will be some over the coming years as this technology becomes more common.

MR. WITTES: Thanks. So, Greg, we have lots of controversy about police departments using drones, much more controversy than we actually have police departments using drones . Lay it out for us, what's the problem and what's the solution?

MR. MCNEAL: Well, thanks to all of you for being here today. We have manufactured controversy right now so let me just come out and say it. Many of you are familiar with Senator Feinstein's noted concern that she looked out her window, she saw a drone, as recently as two weeks ago. It was repeated in a *Christian Science Monitor* story that Senator Feinstein was concerned about a drone outside of her window. The drone actually was a fluorescent pink remote controlled helicopter without a camera that you could buy on line for $17.85. It's part of what Code Pink did. You can go on YouTube and you can see the video of Code Pink flying the little fits-in-the-palm-of-your-hand pink drone that flies. It's a helicopter, a remote controlled helicopter. So in part we have a problem with terminology. So the "D" word has been -- I mean the "D" word has been fetishized, the "D" word has been demonized such that if you say "drones" there's no way for us to know whether we're talking about a predator or a reaper from a battlefield armed with hellfire missiles or a fluorescent pink miniature helicopter. So in California for example the Alameda County Sheriff's Department wanted to get a "drone". It was an octocopter, it cost $7,000 for them to purchase. It could fly for 45 minutes, and you could put your regular sort of digital SLR camera on it. This engendered wide spread

controversy by activist groups who said these things will be following us everywhere, subjecting us to massive widespread pervasive surveillance. You need a lot of devices and a lot of people to follow every person with a drone, because every one of those drones that Alameda County Sheriff's Department was thinking about buying requires an operator; not yet capable of autonomous flight. So if you had 1000 people in your city you'd need 1000 to follow them. You'd only be able to follow those 1000 people for 45 minutes and you'd need 1000 operators on the ground to operate each of those drones. Yes, in the future there is the possibility that drones will be able to operate autonomously, create a mass network of surveillance devices, although many of us live in places now, New York City and other places where those cameras already exist, fixed on posts. They have better surveillance capabilities than a drone that would follow you everywhere.

And so the term has been vilified largely as part of a legislative advocacy campaign. I was on a new show with an advocate from the ACLU who admitted that if they were to pursue less technology centric legislation that sought to ban aerial surveillance at large that it wouldn't go anywhere so they need to capitalize on the public's attention with regard to the term "drone" and try and pass some legislation. I think that's the wrong approach. I think legislators should reject it. I think that the approach that legislators should follow should be technology focused -- I mean should be harm focused not technology focused. So if I'm concerned about aerial surveillance from 300 feet in the air from a drone, I should similarly be concerned when the police park a helicopter at 300 feet in the air and look at me. And so I think that that's that harm that we should be concerned about. If we're concerned that the police will follow us from location to location then whether they do that with an autonomous device or whether they do it from a helicopter, that type of persistent surveillance should be the thing that legislators should regulate.

And so I argued that a warrant based approach is both over-inclusive and under-inclusive, to use some forms of legal terminology. But they basically operate as blanket bans that don't address all of the potential surveillance concerns. And they also keep off the table some useful uses, non harmful uses of drones that we otherwise might want. For example documenting a crime scene. Or on another panel where I was pitted with an individual from the ACLU I said would you support the use of a drone at the Boston Marathon and his response was I don't see what the purpose for that would be. Of course my response was to make sure that three year olds aren't killed by improvised explosive devices. But also my response was I don't see what the privacy harm is at a marathon that's televised from the air. I mean there are guys on motorcycles following the runners with cameras; there are cameras everywhere; it's a public place. In many legislatures -- the California bill that's pending right now, a drone at a public event like that would be banned under the current legislation that's before Governor Brown in California and in many other states. I think there's a better solution.

So really I have five parts to my solution. The first part is that we should allow landowners to exclude all form of aerial intrusions from the surface of their land up to 350 feet in the air. What that would do is it would exclude both private operations of drones from that space as well as government operations of drones from that space. The second part is to craft duration based legislation. So when you follow a person for an extended period of time conducting aerial surveillance, whether you do it from a helicopter or from a drone it's the time that you're persistently surveilling the individual that matters, not the platform that matters. We can see in the paper I lay out a few ways to approach that. Then for the fear that the government is going to have a record of us collected over time from these imagery sources, I argue for data retention procedures. Perhaps they say that for the first 30 days you're able to surveil someone and watch that

information. After 30 days expires you'll need a Court Order with reasonable suspicion to be able to access that information. It's moved to a server where government agents can't access it once those 30 days are up. Once you get to 60 or 90 days you would need a warrant premised upon probable cause to believe that there's some information related to a crime about that individual. And then after some period of time, six months, probably five years the maximum, the data gets destroy. It's completely deleted and it's no longer available. And that would apply to all forms of aerial surveillance.

Those are the three core recommendations and then I have two additional recommendations that relates to transparency, and then the next that relates to coding for privacy. And when we're talking about innovation what we've been speaking about here, I think coding for privacy and recognizing the benefits of technology is the most important. And so let me give you an example that I want you to think about. Imagine we send the police out to surveil your backyard at 123 Main Street. The police believe that you're growing a lot of marijuana in your backyard. Under current law if they fly out in a helicopter and they're at 400 feet in that helicopter they can look down and take a photograph of the marijuana that's in your background. If they're in a fixed wing aircraft they can do it from either 500 or 1000 feet depending on the FAA regulations governing at the time. Now imagine that you're pretty neighbor is sunbathing at 125 Main Street. When that aircraft goes out there with all of those men on board looking down to take photographs of the marijuana plant, I'm imagining that those men might not be able to look askance of 125 Main Street. And the woman at 125 Main Street will have her privacy violated, although her Constitutional rights would not have been violated as the Supreme Court interprets it. Now imagine I send a robot out, an aerial robot, a drone, that's coded to only take a picture of 123 Main Street and automatically redact the images at 125 Main Street. This is technologically possible. You know this because

when you go on BlockShopper or Redfin or whatever, the Google map comes up and tells you the exact boundaries of the property that you're looking at and it tells you what that property is worth and the properties next to it. Using a similar coding protocol I could have a drone go out and protect the privacy, the collateral harm, to those around the area that's sought to be surveilled while also ensuring that we gather the information that we need. I can even code so that I could obscure the faces of people until such time as we have a reason to reveal the images of those people. And so this is just one example of how technology could be leveraged to protect privacy. So what I'm hoping for in the paper is to propose a status quo solution that gives the people a right to exclude drones while we figure to whether or not the technology is beneficial and how we can harness the benefits of the technology without having the harms hit us. And I can get into the details in the Q & A. You can see I have a chart that sort of categorizes how the air space rights would operate and I'm happy to talk about that in the question and answer period. Thanks.

MR. WITTES: Thanks, Greg. Before I turn to Wells, where does the number 350 feet come from? I mean that's -- sort off the cuff it sounds sort of arbitrary.

MR. MCNEAL: It's not arbitrary. I guess it is arbitrary; it could have been 349 or 351. Okay. So the Supreme Court in a case called U.S. v Causby established that the Causbys in the facts of their case owned the air space above their land up to 83 feet. The government was flying planes through Causby's air space, making the chickens get scared. The chickens jumped into the walls and they died. And so the Causbys said you're basically taking -- your impacting -- taking my property here. And so the Supreme Court agreed, said the Causbys owned up to 83 feet. From 83 feet up until 400 feet we don't have any FAA regulations. But when we get to 400 feet the FAA says from 400 feet downward model aircraft operators can fly their model aircraft.

At 500 feet in non congested areas the FAA says aircraft can't fly below it unless they are helicopters and they're flying in a way that avoids hazards. And then at 1000 feet above contested areas is the next line that the FAA says aircraft can't fly below. So my thought was that by extending the property rights line to 350 feet and establishing this column of rights for the landowner but also allows a 50 foot area of space in which model aircraft could be able to transit or even a police helicopter might be able to operate. And then when you get to 400 feet that's the ceiling of model aircraft and we'd still have 100 feet of buffer space between the model aircraft operations and the lowest levels at which delivery drones and whatnot would be operating. And so the goal is to balance the potential innovations that are coming down the road against the rights of the property owner.

So somewhat arbitrary but there's a policy reason behind my arbitrary lines.

MR. WITTES: Now I asked the question because I thought it was actually -- thought it was one of the elegant things in the paper that it's really not arbitrary, it's a number that's well thought through and kind of elegant in the needle that it attempts to thread.

So while everybody is worried about police getting drones, Dianne Feinstein is actually right about one thing with respect to drones which is that she probably has more to fear -- she at least has more to fear from Code Pink and their drone assuming --

MR. MCNEAL: Helicopter.

MR. WITTES: Right, assuming --

MR. MCNEAL: A toy.

MR. WITTES: -- that they actually developed a more -- bought a more

sophisticated one. Her privacy is much more likely to be invaded by one of her fellow citizens than by a police department. So, you know, there was a wonderful incident which I think captures most of everything that's important in this discussion. A hunting club in Pennsylvania -- I learned about this from the *Philadelphia Enquirer* -- a hunting club in Pennsylvania was having a pigeon shoot and a local animal rights group called -- I forget what the actual name of it was, but it was engineered so that the abbreviation, the acronym, was SHARK. And SHARK flew a drone over to take pictures of the brutality to pigeons by the club. And of course one thing you shouldn't do if you have a drone is take pictures of a bunch of guys with shotguns because they shot down SHARKS drone and caused, you know, thousands -- and there were these wonderful quotes from the SHARK people about how offended they were that the guns got turned on their poor drone. So this is the subject, not the gun rights side of it, but the privacy invasion side of it that Wells took a look at. What if we are all flying drones all the time, taking pictures of each other all the time? You know, what's the system that we have for, you know, regulating privacy, interpersonally private level privacy between individuals?

MR. WELLS: Thank you, Ben. Before I get into it I want to say I'm very honored to take place in the discussion with -- at least live and in person with two people whose work I admire and a disembodied technological voice of another person whose work I admire.

But as for Senator Feinstein and the SHARK people Greg is exactly right. In the wake of the 2012 law that in so many words told the FAA and a bunch of associated agencies to kind of figure out how to bring more drones into our air space more of the time, on a wider basis, there was this privacy discussion and it had this -- quickly acquired this fever pitch and it was generally about what the cops can do with their drones. So that's starting to change. But I think up until maybe the last couple of

years when we have spoken of privacy and drones we are quickly into the world of Senator Paul and his Freedom From Unwarranted Surveillance Act. You know, these proposals that, you know, Greg mentioned where the cops or CVP have to get a warrant founded on probable cause before they deploy a drone or deploy the surveillance from the drone. And that has sucked a lot of oxygen out of an equally important issue and one that's kind of come to the fore more recently. Those stories in the press about some work at NCIA on this involving commercial operators. And we know Jeff Bezos wants to deliver drones, use drones to deliver his products to your home. So in theory that also kind of raised the profile of surveillance conducted by drones are run by private operators. And so I think there's kind of two ways to think about this and one is this zoomed out 10,000 foot architectural way, and the other one is more at the level of granularity where you talk about crafting of legislative proposals such as Greg has done in the case of public operators, cops.

On the first at the sort of general way I think there's kind of two camps really and you can kind of -- I generalize the paper and I'll generalize even more crudely now. Where you come down about this probably feels -- it depends a little bit on how you feel about the role of the Federal government in regulating privacy generally. And there is one kind of camp immediately after the FAA Authorization Statue was passed, and some people in this room are probably very familiar with this history, but one camp immediately came out and said hey, FAA, we want you in the business of regulating privacy and drones in a big way including privacy with regard to private operators. And the FAA said no and got right out of that. But that's sort of emblematic of that viewpoint or more broadly whether you think -- you know, another privacy context, this has come up, people have called for like a baseline privacy statute that would be in some respects technical, but cut across all kind of sectors and just set standards for how private

individuals -- you know how these things get handled. That's sort of one way to do to it.

And on the other camp, and I'm again generalizing, some scholars, some policy makers who said, you know, no, let's let the states do this and either keep the Federal government, you know, kind of to a dull roar or reserve their regulatory interests to kind of little discreet zones of activity and sort of let the states figure it out. The people in that second camp have said this thing, which I think is kind of important about how we deal with civilian drones and privacy in the granular way, and the first is that there's a lot of law out there that we could use right now. And we don't really know how it's going to hold up. You have state torts and things like that, common law doctrines, common law privacy torts. You also have various specialty statutes, wire taps, and things like that, things that regulate the behavior of the press when they get really egregious, paparazzi and so on.

And then in several jurisdictions -- you know, in the teens now but it's more again I think in recent years, you've seen passage of anti drone laws which actually regulate private actors. And so the sort of more a "statish" camp they've said, you know, look at this and see how this holds up. And they also point out there's not a lot of consensus about what those ought to look like. So if you're in Tennessee it's a misdemeanor essentially to use your drone and drone surveillance to interfere with someone who is lawfully hunting under state law. It's also a misdemeanor to conduct surveillance -- and I'm going to get the statute wrong -- but it's essentially to surveil someone and take their image without their consent or without -- unless you fall into like several exceptions under the law -- to take that information and use it. That becomes a misdemeanor; that's against the law, versus say Wisconsin where now it's prohibited to use a drone to surveil a person in an area where they would have a reasonable expectation to privacy for Fourth Amendment purposes. There's no real accord about

how to do that. Some jurisdictions are drone enthusiastic. I mean there are -- North Dakota we could probably stipulate feels differently about drones than, you know, those -- the small town -- what it is in Idaho where you get to shoot the drone out of the air or something?

QUESTIONER: They pay a bounty.

MR. BENNETT: Yeah, there's the drone bounty jurisdictions where they feel decidedly a different way. So there's a lot of diversity there. And secondly also I think registering in favor of this sort of second camp, and John's talked about this in some of his work too, is you have some of the more unfortunately sweeping regulations tend to butt up against First Amendment limits. At some level the story of American domestic policy going back low to the founding is this struggle again speech and privacy. And anytime you privilege one you tend to sort of elbow out the other. But if for example if you purport to stop private people from conducting some kind of surveillance in public there might be First Amendment problems. And that needs to get resolved through litigation.

And the third thing, and I talk about this a little in the paper, you know, and I think this goes really to Greg's point about the kind of manufactured sort of drone phobia, drone controversy is everywhere and that's gradually coming into the Courts. You know, I mean as Raphael Pirker, you know, I mean he's currently -- he's had his battle. Or, you know the EquuSearch case about search and rescue that's gone on. There is litigation about drone derived evidence in criminal cases. But what there hasn't been yet -- and of course we also know about safety -- I mean there's a drone safety story -- I mean there's a pretty steady clip about "this happened with my UAS or that happened and it was bad, it might have fell down." But what there hasn't been is a wave of lawsuits saying a drone trespassed over the air space above my house and I'm raving

mad and I demand an injunction or money. Or there have not been waves of -- you know, you do have these newly minted anti drone statues regulating these private parties and they're not getting test driven by people who are saying I'm just raving mad at the UAS surveillance that's going on in my neighborhood and my neighbor did it and he was really nosy and stop it.

So all of those things I think really support what the sort of second camp -- which has said, you know -- and there's more than one way to sort of spin it out differently, but letting the states take the lead. The down side of that I think, and it's big or small but I think it's just real is that obviously this iterative process of letting the states figure it out which I think is about the best way to go. And everyone has their own feelings about what an optimal -- again to sort of looking at the granular level -- everyone has their own feelings about what a private drone regulation will look like. And, you know, in that regard I'm actually quite sympathetic to a property rights approach. I think it's a great idea. But everyone else has their own feelings and, you know, sort of let it play out. The down side to this iterative approach, of sort of letting people try things and do it over time is that it presupposes a lot of litigation, a lot of figuring out, and in some respects some privacy violations. And so I think, you know, for the Federal -- in terms of going back to the general 10,000 foot zoom out architectural you could kind of use the Federal government to mitigate the down sides of that as you move through time. And one way to do it, not the only way, a plausible way, and I think it's probably -- I would say it's a contrarian way to do it because -- is to help -- is to use the FAA. The FAA takes a lot of lumps. And one thing if you say to the FAA that they've been sort of -- when they say we're the FAA, we're doing drones and you say well, drones involve privacy, it's sort of lay hands on the Ark of the Covenant. They will say no, we are not a privacy agency, we are a safety agency. We do safety, not privacy. Thank you, sir. But since 2012

they've gradually, either on their own initiative or with instructions from Congress a little bit, gradually have sort of gotten into the privacy game. Not as a regulator. And it's a bad idea I agree; that they should not become a privacy regulator in any respect, but when test sites where drones are currently being looked at to work out some of these regulatory issues, when those weren't being named with sufficient speed people said what's going on. And their agency said among other things hey, you know, this is complicated privacy stuff and we've got to figure this out. And when the time came to award test sites they had very modest privacy rules that operators would have to obey or the regulators in the states disagreed with them the FAA would intervene and say no, you can't do that anymore. Now Congress has also said very quietly to them, you know, you should study this issue and tell us where the gaps in the law are, what you could do to handle it. But there's a little bit of privacy kind of like icing to go along on that safety kick and since -- and I'll stop here -- but I think a lot of people who looked at this would agree that sometimes the line between privacy and safety isn't especially clear and that as we go forward we should be thinking about areas in the Federal government where people have a sense of both privacy and safety. So one way to do it would be to use the FAA licensing scheme to kind of take the punch out of that as integration goes forward and as we figure out what your ideal private privacy, Pink Drone defeating, Senator Feinstein protecting statute ought to look like.

And I will stop there.

MR. WITTES: So before I talk about cyborgs it occurs to me that I actually omitted reference to the sixth paper in the series which is by Ryan Calo, University of Washington. And Ryan has written -- actually it's almost more of a bureaucratic proposal than a regulatory proposal, but it's an argument for a Federal advisory agency to garner expertise on robotics and to advise the many different Federal

agencies that are grappling with different issues and which may not have a lot of internal expertise to think about them. So that paper I should have mentioned when I was listing the other papers but as you can see I don't work with notes and am not a robot myself.

QUESTIONER: Or are you?

MR. WITTES: Or am I?

QUESTIONER: That's the trick.

MR. WITTES: Which is an excellent segue to a conversation that took place about three years ago in this very room involving a gentleman named Tim Wu who has recently become quite famous as the guy who almost won the Democratic primary for Lieutenant Governor in New York in an insurgent campaign with Zephyr Teachout against the incumbent Governor and Lieutenant Governor. Tim Wu in his other life is a law professor at Columbia and a kind of among other things a sort of theoretician of the law of tech futurism. And Jeff Rosen and I had edited a book to which he had contributed and we were talking about privacy and cell phone tracking in light of this recent case that had just then come down, U.S. v. Jones. And Tim made the I thought arresting observation that we debate these issues in terms of privacy as though humans are using tools, but that's a very 20th century way to think about it. And really what's going on is that humans and tools are integrating with one another and we're actually in the offing stages of the development of cyborg law. And if you think about it he said -- and if you read the transcript of the remarks it's a little bit disjointed because he was vamping, but I though the point was very arresting -- that, you know, you and your cell phone are actually not severable. It's not implanted in your brain so nobody noticed it, but you're never separate from it. And in fact there's a human-machine integration there. And the rub is that the biological components of that integration have rights, and the technical components of that integration do not have rights. But the technical components are

subject to easy surveillance and tracking and the biological components are not. I've been thinking about this point ever since. And I don't actually know what political direction it cuts, but I began thinking at the time that the NSA controversies broke that maybe the reason that -- I've been a devotee of sort of the law of FISA and national security surveillance for many years, since the early '90s -- and this was an area that only weird nerds like me cared about until a few years ago when all of the sudden everybody seems to have an opinion about the foreign Intelligence Surveillance Act. And I've always scratched my head and wondered how did that go from being this area where it was really the province of a very small number of people to something that was a matter of passionate front page news day after day after day. Part of the answer to that is Edward Snowden, but it actually began long before Edward Snowden. And I think Tim Wu's point which I tried to develop in this paper that I wrote with Jane Chong who is not here, deserves a lot of -- is a co-author on that paper in the truest sense -- I think part of the answer is that we have actually internalized to a certain degree that the idea of a cyborg is not a binary on-off switch but a spectrum, and that we are somewhat on it. We're further on it than our law which treats humans using tools as very disaggregated things. You may have rights in your use of the tool but the integration has no right, the tool is a slave. We have internalized that to a certain extent and I believe that one of the reasons that we've reacted so strongly as a society to the NSA affair is that we fear that in a world in which we are becoming more cyborgs, we call them in the paper that we're baby cyborgs now and sort of moving toward adolescent cyborgs. We may acquire the rights of the machine along with its capabilities.

So I want to talk very briefly about -- in the paper there we go through a bunch of different areas of law where if you think of us as on the cyborg spectrum our points of law, our doctrines are a little bit head scratching. But there's one that I think in

the surveillance context that really -- the idea of cyborgization kind of opens up in a different light. And that's the so called third party doctrine. Now for those of you who aren't lawyers or Fourth Amendments scholars of one sort or another, the third party doctrine is an idea that developed in the late 1970s in the early years of what we came to call big data, where large aggregations of data about individuals ended up in the hands of companies with which you did business. So the two seminal cases in this area involved your banking records and your telephone metadata actually in a case called Smith v. Maryland. Now it didn't come up in the context of aggregating all telephoning metadata, it came up on the context of, you know, Wells Bennett is suspected of a crime, his name in this case is Smith, Wells Smith. So you send a note to his telephone carrier and you say put a pen trap and trace device on his phone so we can know who he's calling and who he's not and who's calling him. And the Supreme Court says this isn't covered by the Fourth Amendment because you're not searching Wells, you're actually just asking for material that he voluntarily gave to a third party. He made those calls knowing that his phone company was going to retain that data for billing purposes. So he doesn't really have any expectation of privacy in that. Now I want you to think about that. I have been a defender of the NSA since the beginning of this controversy and I make no apologies for it. I believe in espionage and I believe in signals intelligence. But I'm a little bit befuddled by the application of that principle to guy with a pacemaker. Now a pacemaker generates a lot of data and it actually generates a lot of data that can be retrieved from the outside. Now under the third party doctrine you would have to say I think that your pacemaker -- you voluntarily underwent that surgery to have a pacemaker and that pacemaker produces data that is available to the company that makes the pacemaker. Now there may be HIPAA issues about the disclosure of that, but basically it's the same principal as involves your telephone. But somehow when the device is implanted in your

body and when you're depending on it for your life, it feels ridiculous to describe that as a third party doctrine. And I think the more you move the population into a world of infant cyborgs and then juvenile cyborgs and then adolescent cyborgs and then adult cyborgs, the more integrated the technology becomes, the more tracking the device is tracking the person. And your cell phone is a very interesting example of that. You can leave it off, you can leave it at home, but you don't and you won't. And it's not that you're not voluntarily giving that date to third parties, it's that that data is integrated with you in a way that is certainly untrue of the pen/trap device in Smith v. Maryland. The more you think about this in terms of the cyborg and less in terms of the human using tools the more stress you put on that doctrine which is inherent by the way, and deeply, deeply formative in a lot of the activities that law enforcement, intelligence and for that matter other civilian agencies engage in all the time.

I'm going to stop here with a single note that there are eight votes on the Supreme Court as of this term for the proposition that you are partly cyborg. The Supreme Court --having nothing to do with the fact that Jane and I were working on this paper by the way; I'd like to take credit for it but it seems unrelated. The Supreme Court considered a case called Riley v. California. In Riley the confronted the problem of whether the search incident to arrest doctrine allows somebody to go through -- a cop to go through your cell phone when they arrest you. Now this is not really so much a cyborg issue on its face, but eight votes signed the Chief Justice's opinion. And the Chief Justice's opinion begins by saying that the cell phone is so inherent to life in modern society that the proverbial visitor from another planet would not understand that it was not part of the human anatomy. Now eight Justices are on that opinion. I don't think eight Justices would vote for the proposition that they're infant cyborgs, but I would say that they already did.

So I'm going to stop there. And why don't we -- I'm going to sprinkle questions throughout in my other role as moderator, but let's open it up to you guys; you've been very patient. Signal me and wait for the microphone to come around. Please announce your make and model and --

QUESTIONER: If you are a cyborg.

MR. WITTES: -- what organization you represent. Sir?

MR. COLLINS: Hi. I'm Rob Collins of the University of Washington School of Law in Seattle. And I was intrigued by what John said. He said autonomy is a continuum and I think Ben -- if I have it correctly -- you said that the idea of a cyborg is not an on-off switch but something of a spectrum. Along those lines I'd like to ask the following question. In civil and criminal law the law of agency plays a vital role, can you talk about in terms of liability, either criminal or civil, can you talk about how robotics might affect the law of agency, either in a civil or criminal context?

MR. WITTES: John, do you want to address that?

MR. VILLASENOR: Go ahead, you take a start and I'll follow up.

MR. WITTES: Actually there is a person I know who has thought very deeply about this question and I'm afraid I'm not he. The person in question is Ken Anderson who has been ruminating about exactly this for about a year. And I would -- maybe that should be the next paper in the series actually because it's a fascinating issue. What I'll say is this, I think in order to imagine the robot as having agency or the robot as relieving the operator of the robot of agency you have to imagine a degree of self tasking that is -- or sorry, to imagine it as anything other than an agent of the operator. You have to imagine a degree of self tasking that is many jumps ahead of where we are in artificial intelligence. I think the best way to understand, for all the temptations to understand it differently. The best way to understand a robot is as a stick,

as a tool. That may change. And you can imagine the robot over time becoming more of an agent, more of a, you know, even beyond agency sort of self tasking and having its own responsibility at some level. But thing we're very far from that. And I think one of the ways to understand how you should view it for now at least is to think about it in terms of if it were an inanimate object and you hit somebody with it. Who would be -- and somebody got hit with it, who would be responsible? If it were, you know -- I mean John can talk better than I can on the product liability side, but there is a -- you know, one of the questions you're going to confront is whether the driver is liable in certain circumstances or the programmer, the programming entity, the hardware entity, or the software entity is liable. And one of the really good models to think about that is complex machinery that is non robotic in nature, you know, where you have many contributors to the problem and what's the contributory liability of the operator versus the manufacturer, versus -- so I mean that sort of exhausts what I can say on the subject. John I think probably has a lot more to say.

MR. VILLASENOR: Yeah. So I think it's a great question and there's a lot that could be said, but a short -- just to add to what Ben said, I'd say that, you know, while one way to look at it that robots don't make decisions. Another way to look at it is that in fact the people -- that robots in some sense make decisions because they act in ways according to how they programmed during the design process when they're all being manufactured, the code was being written and so on. And so in some sense -- and of course robotics only exists because human beings have actually created the systems and the programs and the hardware and the interfaces and all that to make these devices work. So in some sense there are decisions being made, they just don't happen to be made contemporaneously with the event that you might be looking at. So for example if an autonomous vehicle gets in an accident due at least in part or potentially in part to

some alleged failure of the autonomous aspects of the vehicle then you can start asking the questions of okay, well what part of that vehicle, what aspect may have failed and then what decisions two months ago or two years ago or fifteen years ago, whatever it may be, were made when that was designed that led in some part or contributed in part to that accident. So think the question of agency in part would involve sort of untangling those incredibly complicated decisions that may in contract with -- you know, if you have a car accident involving a non autonomous car to the extent that that exists, then that is the -- many of the factors that relate to that accident are going to be related to decisions that were made at the moments of or immediately preceding the accident, where with autonomous vehicles some of the decisions may have been made far in advance. And of course that isn't new as the person asking the question echoed, you know, if there is an alleged failure of antilock brakes then those decisions were in part made a long time ago. So anyway it's an incredibly important question and I agree with Ben that it is worth a paper or perhaps more on its own. So thank you to the person who asked it.

MR. MCNEAL: So I teach criminal law and I actually think that the criminal law questions are much more difficult to deal with here. You can imagine -- the future exists now where individuals could have prosthetic limbs. So now imagine a prosthetic limb malfunction while I'm holding a knife or while I'm driving a car. If I knew that that type of malfunction might happen it could be analogized to the person who knows they have seizures and shouldn't drive, right. And in that circumstance we might say that that person has a culpable mental state and we might prosecute them. But the first instance that the malfunction on the prosthetic limb happens, it's far more difficult for us to say that that person should be criminally blamed. And then when you get to robots that just do what they're programmed to do -- I'll use a -- this is a reference to Kate Darling although I don't know if she's ever made this reference, she researches sex

robots. So imagine the future where your companion sex robot is left at home and your underage daughter or son not reaching the age of consent shows up and begins to the robot that does what it's programmed to do. Who has committed the crime there? The parent who's left their unattended robot , the child who's using the parent's unattended property, the programmer, the company, and what would such a prosecution look like for that robot? The move AI has this. Jude Law sort of plays this like gigolo robot and it makes you wonder exactly who would be criminally blameworthy there. We laugh, but I have two kids. I would want someone to be punished for that type of thing. So really difficult questions in the criminal law space.

MR. WITTES: One more point on this. I'm not sure this is quite agency but, you know, one of the things in a lot of the robotics areas that where you imagine replacing humans, driverless cars being one of them, but, you know, there are errors that are characteristically human and errors that are characteristically machine. And so it's possible to imagine say reducing the number of traffic fatalities dramatically, that is automating functions that humans perform badly and thus the aggregate number of traffic accidents go down. But at the same time those robots will make errors that humans might not make. And so when you replace large numbers of human drivers with robotic drivers you might be creating a class of accidents that would not happen if you were not replacing it. Now so what happens if the road safety level goes way, way up but you're killed in an accident that no human would have gotten into and that that was predictable, right. So is that an intentional killing? Is that an intentional negligence? And I think there are actually a lot of -- you know, robots and humans are not good at the same things.

Yes?

MR. ROBERTS: Thank you. I'm Dan Roberts. I guess you've got me on half *Guardian* Reporter and half iPhone 5. I just wanted -- which I think you made a

fascinating point about cyborg law and I just wondered if you could flesh it out a little bit -- excuse the pun. What kind of rights do you think this cyborg kind of interaction should have that differ from what we have already? I mean I'm thinking particularly of the GPS data I create by carrying my iPhone around with me. How is that different from the bank account data I create? I mean don't I have the same privacy expectations simply as an individual in creating that data? How does it -- can you give us examples of how a cyborg law would strengthen our collective privacy in those situations?

MR. WITTES: So first of all I'm not necessarily arguing that it would strengthen your collective privacy. You might decide as a society of cyborgs -- cyborgs inherently create data. And you might simply decide as a cyborg society that the mass collection of data about lots of individuals is inconsistent with privacy as we've conventionally understood it. And so we're going to give up on certain aspects of it. My point isn't that it leads to a more privacy protective environment. My point is it leads to a different way of thinking about it. So let me give you an example that we develop in the paper and that I think is illustrative. Right now if you want to call me -- well, notice we still use very telephonic vocabulary here. So you are going to use a tool, your iPhone, and you're going to call my tool, your tool calls my tool. We both hold them up to our heads or to our blue tooth devices and we talk. And in that context it's rather easy to think about, well you have voluntarily given certain information to a third party and I have voluntarily given certain information to a third party. And the third parties in question have collaborated to create a line that can be tapped. And we both make that call aware that we're creating that data and have that conversation aware of the possibility of interception. So now imagine that you go several more generations into cyborgism and you're iPhone 5 is actually biologically controlled -- biologically in your head and my, you know, Samsung is in my head. And you actually don't have to make a conscious

decision to dial a phone number. Wherever you are in the world and wherever I am in the world we can just simply talk to each other just the way we're talking to each other now, only we're not geographically in the same place. And so you might walk down the street and say hey, Ben, I have this thought that I'd like to report in the *Guardian*, what do you have to say about it? And I could say no, you're actually full of beans about that. And we have the same awareness as though we were walking next to each other. But in fact what separates this example from magic is that there is a telephonic device in your head that is doing all the same things that your iPhone 5 is now doing and on my end is the same thing. So I venture the proposition that we would not think of that as two humans using their tools. We would think of that as the two of us having a conversation. And the fact that we are using tools in the course of that would be no different from the fact that we're having a conversation now and we're both wearing clothes. It's just part of the way humans interact. And so my point is not that the law is necessarily more privacy protective, my point is that the human-machine integration necessarily makes you think about communications and other things, not just communications. Also your heartbeat, your prosthetic limb, your use of -- there is one example Jane found and we wrote into the paper of a gentleman who -- he calls it the eyeborg, and the eyeborg is a device -- he has an extreme form of color blindness and the eyeborg allows him -- translates visual color images into sound. And so it allows him to hear color. Now there are a lot of places in the world where you walk in and they say no cameras. Interesting question, does that rule -- would a rule like that legitimately apply to somebody who is using a camera for some biological compensatory function that we consider sort of normatively human?

And so my point is the more we rely on technology integration for things that we think of as essentially human in character, the less we're going to think about

them as human uses of tools and the more you're going to think of it as some kind of cyborg law. And I don't really pretend to know what direction that takes the substantive law. I mean I do think in the case of the third party doctrine you look at it and you say we're going to revisit that one at some point. But I'm not sure -- it doesn't -- I don't think it leads you to a simple and therefore we're going to protect privacy better or and therefore we're all going to have, you know, have laws protecting Google Glass or forbidding Google Glass or that sort of thing.

MR. MCNEAL: Let me add a thought briefly. You could imagine a future where we could eradicate disease by having chips implanted in us that were early warning systems to let us know when disease was going to come about. But for those chips to operate effectively the Center for Disease Control would have to have a way to update the software, just like the software on your phone always updates. Okay, fine. What happens when you fail to update your software though? Under ancient law -- I say ancient, 18th century and 19th century doctrines people who are public health risks could be quarantined. So is a failure to update your public health chip a quarantinable offense? So I started -- but I guess we're all excited about the ability to eliminate disease with early warning, but then I hit you with the other part of it which suggests we're not sure which direction it would go. And so the direction of it is the hard part to figure out. The potential is there. And this is -- everything about what we're talking about is looking at robotic technology a being either wonderful or the dystopian future. And it just depends on who you're sitting with and how many beers you've had, how you come out on it. .

MR. WITTES: Yes?

DR. FINKELSTEIN: On a somewhat different aspect of the topic -- I'm Bob Finkelstein, Robotic Technology, Inc. -- has Brookings looked at the consequence of ubiquitous robotics which will come about well before the end of the century in terms of

intelligent autonomous robots doing all kinds of functions, not only manufacturing but in the service industry and so on? Have you looked at the employment and economic consequences of this? That is in centuries past new technology has inevitably led to certain unemployment in various sectors but new employment as a new consequence of the new technology. But some people think that this is going to be so radically different. Driverless vehicles, cars, trucks, buses, will eliminate millions of jobs. People make a living driving for example. In the near term, in the 2020s. So beyond that have you been looking at the employment, economic consequences and what the potential solutions might be for this?

MR. WITTES: So we haven't so far though it's an area where as you know there's been a lot of work done and of course the estimates are widely divergent, right. Because some people believe you end up replacing a lot of low scale jobs with higher end jobs and some people believe that you basically wipe out large swaths of the employment. It's not an area I've done any work in but, you know, it's certainly an area in future -- the employment ramifications are certainly areas that we should look at in the future iterations of -- future papers in the series.

Have at it.

QUESTIONER: So the first question, after coding -- this is based on the discussion about how you can use programming to basically make a drone not collect sensitive information -- after coding the drone to do only specific things how will you verify that that's what the code actually does? And then there was another question about where does this talk of drones, cyborgs fit into robotic in terms of law, regulation, and Federal agencies.

MR. MCNEAL: So with regard to how do you ensure that the drone's doing what it's doing, outside of my five core recommendations I have a second part of

the paper where I talk about if you reject the five proposals and follow the warrant based approach there are still some things that are necessary to ensure that drones are functioning appropriately. And one thing I suggest is auditing. So if I were constructing the perfect civil liberties protecting approach to drones at the state and local level, when my law enforcement got drones I would also establish an outside review board, I'd probably have like a Rampal libertarian, someone from the local ACLU chapter, you know, to balance that out, to retired police offices. And their job would be to randomly audit the data that had been collected when the drone was used, whether the drone had been coded for privacy or not. And so you could imagine a circumstance where you just have a regular remote control helicopter operated by the police, I would say that the state and local government should have a rule that requires the software to document which officer was using the drone at the time, maybe they swipe a card, where the drone was located, geo-located, and then also what direction the camera was pointed in, and then I would subject that to random auditing. So if I found out at the end of it that the police officer near the university campus always seemed to fly the drone at 9:00 p.m. at night near the sorority house with the camera always pointed towards the sorority house, the audit would catch that and I would say what was the legitimate law enforcement for the police officer doing that? I make reference to this in the paper. It's not an outlandish idea. In the UK the police departments that fly helicopters publish their flight logs. Some of them even Tweet their flight logs and they say the helicopter was dispatched on such and such a date and was looking for a lost elderly woman, or was looking for a stolen motorcycle. The reason they did that was to respond to noise complaints and also the paranoia that people had about why is the drone operating at this time. The law that prompted it was a very aggressive form of a transparency law or freedom of information law in the UK. But you could imagine that being creative up front and forcing this type of

transparency could allow us to the use the technology but also to catch the legitimate concerns about potential wrongdoing.

MR. BENNETT: That's a good example of you can sort of capture, you know -- you don't have to be in a world of Orwellian nightmare. Sort of something really wonderful of technology you can use the technology to mitigate the downsides and get a lot outside.

MR. WITTES: So, I'm sorry, what was the second question?

QUESTIONER: (Off mic)

MR. WITTES: I'm not sure I entirely understand that question.

MR. MCNEAL: I mean I think I envision -- I mean so most of my propel -- so the first portion of my proposal with regard to property rights speaks to what states have to do because states have traditionally been the arbiters of property rights. So you think of your property in two dimensional space. Your property line is like down to the millimeter and if your house encroaches even just a little bit you have to slice off part of your house because you're in your neighbor's property. That's a local type of thing that addresses this. And I've been talking about private property. So what that leaves open is the possibility that over public property you might allow drones to be used. Or you might say above streets adjacent to residential neighborhoods, local zoning laws would come into place that say no, actually you can't go above, you know, above 150 feet because I don't want you to go 400 feet in the air above the street and still be able to look into someone's backyard. So on the property issue I see it as a zoning one.

On the transparency, the persistent surveillance duration limits that I put into place, the data access procedures and warehousing procedures, those are things that I think that Congress could establish rules for how Federal agencies approach that. And by doing it not specific to drones but as to aerial surveillance at large it would

revolutionize the way we think about privacy from aerial surveillance in a way that I think would be more productive than any bill that's out there, any bill that's being advanced by the ACLU or other privacy groups.

MR. WITTES: John, do you have anything to add on Federal agencies or the like?

MR. VILLASENOR: Not on this question, no. We don't have a lot of time left and I want to leave time for some other questions. Thank you.

MR. WITTES: Okay. Yes, sir?

MR. UMANSKY: I'm Vladimir Umansky, University of Wisconsin. I'm curious, everything we heard so far or most definitely I read, where situations where you can separate who does a given action, a human or a robot, even when the operator controls the robot you kind of assume that this is possible. And one reason for that is what you alluded to, you said today it's okay to look at the robot as just a stick, a tool, that's why it's possible. But I really think that today already, definitely very, very soon, we will see a situation involved into some of those where a model could be -- imagine you have a steering wheel of the car and two hands of it and one belongs to a human and the other to the robot. If any given moment all the decisions are done by both and at least definitely no way to separate the two. So to me it sounds like it makes a lot of sense to consider this situation as likely -- I can generalize it, when you have a team of such agents, we're talking about more than two, and again humans do decisions, machines do decisions and you cannot separate when what it done.

MR. WITTES: John, this is you.

MR. VILLASENOR: Yeah. Well, let me get -- so let me -- that's an interesting question. So let me say that -- let me take that analogy and give you one that we already have today which is what is the relationship between the pressure of -- what

determines when a tire, a wheel on a car -- the brakes are applied? Well, we actually already have the situation like you just talked about where well certainly your right foot can be pressed on the brake pedal, but that's not the only thing that controls how much braking is applied. As I think everyone in this room knows there's a whole bunch of very sophisticated computer algorithms that go into deciding on which wheels how much braking pressure will be applied. And so there's already this set of coordinated teamwork one hopes between the human driver and the systems in the car to make sure that the braking applied in the safest manner. And there are many other examples as well. We are already in world where the actions that are taken with respect to a vehicle are in part a combination of specific decisions made by the driver at that time and on this other software. And I will agree -- or to the extent that the question implied or was raising the issue that we need to sort of somehow disentangle that in some cases, that is an important thing and I don't think it's going to be easy but I also don't think it's going to be impossible. That is absolutely a part of the challenges we're going to face in the future. And that ties, you know, actually also to the things that Ben was talking about, about this integration of machines with us, and then as those things become integrated then we have new questions.

I'll just close by saying that in some sense, you know, there is an integration of your right foot and your body controlling the brake, and the automated braking systems of the car that's not as elegant an integration as the mobile phone, you know, sitting in your pocket but it is an integration nonetheless that impacts the physical control of something like a vehicle.

MR. WITTES: Yes?

MR. ERRY: Hi. Malcolm Erry. I'm an independent political and strategy consultant. One interesting thing in the question regarding the sort of the views of the

NSA and how the view of privacy will change as it becomes more automated into our sort of mental functions let's say, isn't it a contradiction there? I mean in terms of where -- at the moment -- let me see how I phrase this. As you say, as it becomes completely automated, as we're no longer sort of divulging data, as we're no longer making a conscious action to call somebody then you would say that that would require a new level of privacy because we are -- the third party doctrine couldn't apply, but at the same time it seems impossible that we wouldn't have the sort of level of data collection that we're currently doing with for example the NSA at that time. So I mean how do you envision that to be in the future? Would we have a heightened level of privacy given that we're not making a conscious action to divulge private data or -- but isn't that impossible? Won't we see that the NSA collection at this time in a few years we'll see that that was nothing compare to what we'll need to have in the future just to have the functions that we'll have? That was unclear.

MR. WITTES: So it's a wonderful question and I'm going to punt it because the honest answer is you're asking here for a prognostication as to what our moral values will be and how we will weigh different interests. That I actually -- I'm a very arrogant guy but I'm humble enough to know that I have no idea what the answer to that question is. I will say the following, here are the constituent components I think of how we're likely to want to evaluate it. One is you're right, we will be producing an enormous quantity of data and we will ask ourselves how much we value the exploitation of that data for various cyborg-y functions. Does the cyborg function well when we exploit that data for a wide raft of purposes? And we will ask ourselves the question of whether the cyborgs human qualities are impeded by doing that. And that will form a set -- you know, a whole complex set of technical capabilities, moral instincts, a sense of why we're doing the things we're doing. You know, one of the things that's driving cyborgization right now

is people enjoying playing, you know, and when you wear Google -- most people aren't wearing Google Glass because they need it, they're wearing Google Glass because it's really fun and the really fun standard is not going to move the NSA. They need it because it innately goes to my humanity in some sense, is going to move the Congress of the United States and is going to move the basic operations of the government in a lot of ways. And so I think, you know, to answer that question you need to know just a huge amount not nearly about what's going to be technically capable, but how we're all going to feel about it. And so I'm just not going to pretend, you know, that I have any idea what the answer to that question that is.

MR. BENNETT: I will mostly punt, but this little addendum. I'm --

QUESTIONER: So arrogant.

MR. BENNETT: If we do get to a point where there is no real third party application that would create a legal exception for surveillance rules my guess -- and it's a hopeful guess -- will be that any surveillance of that information will have to have the permission of a Judge and will not be the kind that can be issued unilaterally. That is what I think, that's my guess for the future. That you'll have to ask for some kind of permission to get into my brain.

MR. WITTES: So just like I think that's exactly right.

MR. BENNETT: You would not get a national security letter for your thoughts.

MR. WITTES: When I read about the eyeborg I have a lot of solicitude for that, you know, for somebody who wants to be an eyeborg for the reasons that he does. When I read about Google, you know -- it's a term that has made the rounds is the "Google Glassholes" and , you know, some of them are really obnoxious. And I don't think we're going to have a lot of solicitude for the people -- there's a lot of great sues of

Google Glass by the way, but there are certain people who use it to film everything that's going on in their lives at the expense of the people around them. And I don't think we're going to have a whole lot of solicitude for that as a society. So I think the pace and utility of cyborgization and what drives it is going to be a real major determinant of how we feel about it which is in turn going to drive the answer to your question.

MR. MCNEAL: And so now I have a thought. I think that what you said about --

MR. WITTES: I can intercept it before you think it.

QUESTIONER: I know.

MR. MCNEAL: But you've got three, you know, a law professor and two Brookings people up here trying to be the arbiters of what would be a good use.

QUESTIONER: Which means we can beat you up if there's two of us.

MR. MCNEAL: But we're not very representative and in fact even the general population wouldn't be representative of a potential beneficial use of always filming what's going on. For example, if I live in Ferguson that's a very good use for a drone or for Google Glass all of the time to document what's going on. And that's a technology I want in the hands of the people. And so I make this point a little bit in the paper, when we demonize technology, when we demonize drones or robots, the end state that we get too often times is that we take away the potential legitimate uses. So if you -- let me circle back to drones, in Ferguson the FAA granted law enforcement a restriction from all aircraft flying except for police aircraft. So that's why we didn't see helicopter footage of what was going on in Ferguson. But that also is sort of a problematic way that we're regulating two power remote controlled helicopters that really were only going to fly 85 feet above the ground to see what's going on. And so we run the risk when we're too fearful of technology that we take it out the hands of the people

for beneficial uses. And I think that's part of a thing we have to look out for in all of these advocacy campaigns where we see the dystopian future and we try and say what a good use is versus a bad use. It's consistent across the board. When cars first came about the laws required someone to walk in front of the car with a red flag to let people know the automobile was coming. And this is our instinctive reaction to technology. Imagine if that were still the rule today. And so I'm optimistic about the future because I'm optimistic about the collective wisdom of the people and I think that knee jerk reactions and fears of a dystopian future are best left to science fiction. We should be concerned somewhat for the negative possibilities but we should also trust that we can use technology to solve problems.

MR. WITTES: On that note we are out of time. Thank you all very much for coming. There are copies of all the papers available on your way out.

(Applause)

* * * * *

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, 2016