FTC Fall Technology Series: Drones
October 13, 2016
Segment 1
Transcript

[MIXED CONVERSATION]

SPEAKER 1: I'm not sure that this mic's alive. But. Uh-huh. That'll work.

JAMIE HINE: I'm going to put my remarks-- just I'm going to take them.

SPEAKER 1: Oh yeah, yeah. Sorry about that. Yeah, yeah.

JAMIE HINE: Perfect. Everybody's here.

JAMIE HINE: Good afternoon, everybody. And good morning to all of our friends out on the west coast on our webcast. On behalf of my colleagues here at the Federal Trade Commission, I am happy to welcome you to our workshop on drones, which is the second installment in our fall technology series.

My name's Jamie Hine. I'm an attorney in the Division of Privacy and Identity Protection here at the FTC. And my co-organizer for the workshop is Kate White. She's also from the Division of Privacy and Identity Protection.

Before we begin with our program, I have a few administrative details. First, please, if everybody can silence any mobile devices. If you have to use them during the workshop, we ask you please be respectful of the speakers and your fellow audience members.

Second, please be aware that if you leave this building for any reason during the workshop, you'll have to go back through security. So please bear this in mind, and plan ahead, especially if you're participating on a panel, so that we can remain on schedule.

The restrooms are just down the hall outside the auditorium. The Plaza East cafeteria is located inside the building. So you can use it without going through security. And it will close at 3:00 o'clock.

Most of you have receive a lanyard with a plastic FTC event security badge. We do reuse these for multiple events. So when you leave for the day, please make sure to return your badge to event staff.

If an emergency occurs that requires you to leave the conference center, but remain here in the building, follow the instructions that will be provided over the PA system. And if an emergency occurs that requires evacuation of the building, an alarm will sound.

Everyone should leave the building in an orderly manner through the 7th Street exit. You'll be directed to that exit. And after leaving the building, you'll proceed down 7th Street across East

Street to the FTC Emergency Assembly Area. And you'll remain there until your instructor returns to the building. Again there will be someone there to direct you. Hopefully that's not something we have to deal with.

If you notice any suspicious activity, please let one of the staff know. And be advised today that the event is being photographed as it's being webcast. It's being recorded. So by participating in the event today, you're agreeing that your image, and anything you say or submit, may be posted indefinitely at FTC.gov or on one of the Commission's publicly available social media sites.

Now we're happy to welcome all of those who are watching on the webcast today. We'll make the webcast and all the workshop materials available after the event. And we'll have a lasting record for everyone who's interested in these issues. And that should be posted two or three days after the conclusion of the event this afternoon.

For those of you who are on Twitter, FTC staff is live tweeting today the workshop at #dronesftc. #dronesftc. So please participate. Be active.

We have comment cards here in the conference room. Audience members will be able to submit questions, and workshop staff will collect cards and bring them up to the moderators. We will do our best to accommodate as many questions as we can today.

And as a reminder, the public comment period will be open for 30 days after the event, until Monday, November 14th. I urge those who have issues that they'd like to raise to submit those. You can do that at the workshop website at FTC.gov. And again, that's until the 14th of November.

And so aside from some of the folks you'll see today, this program wouldn't be possible without the work of a lot of people behind the scenes, a lot of folks here at the FTC. And so I personally would like to thank Fawn Bouchard, Crystal Peters, and Bruce Jennings, who've done an outstanding job making everything possible today. In addition, I want to thank all of the paralegal support-- Jessica, Amber, Annie, Joseph, Jen, and Bianca.

And in advance, I'd like to thank all the panelists for being here today. We've got a great group of speakers who've come from all across the country. And we are very, very grateful that they're here to participate with us today. And so without further ado, I am pleased to introduce Commissioner Maureen Ohlhausen.

MAUREEN OHLHAUSEN: I always have to make this a little down lower, or jump up or something. But anyway, thank you Jamie. I'm delighted to be here today to open the FTC's workshop on drones and privacy. Thank you to all the participants and attendees. And I hope you find the discussion interesting and educational.

I also want to thank the staff for their considerable efforts in organizing this workshop. As a former head of the FTC's Office of Policy Planning, I know how much work it takes to put together a major workshop like this. And so while my remarks are just my own, and not necessarily those of my colleagues, I'm certain they share with me the gratitude that we have for such hardworking and talented staff.

But let's start with some history. So if you see this picture, this stunning picture of San Francisco was taken from an unmanned aerial system in 1906. This is one of the most famous pictures of the aftermath of the 1906 earthquake, which was the first widely photographed natural disaster.

Photographer George Lawrence strapped a 49-pound custom-built camera to a string of large kites and sent it up 2,000 feet over the San Francisco Bay to get this new perspective on the situation. And Lawrence used cutting-edge technology of his day. Now very few could afford to operate such devices. And today, drones put far more powerful technology into the hands of many.

And as drones grow increasingly accessible to both commercial and hobbyist users, news stories have covered incidents of bad behavior by drone operators. And academic articles have outlined harms, and then posited solutions. And legislators and regulators have offered their own options. So in short, a conversation has begun. And today's workshop will contribute to that.

So my goal today is to quickly zoom up and out, like Lawrence's photo, to provide a very high-level view of this conversation about drones and privacy. Specifically, I want to place this conversation in the context of the much longer conversation about the privacy impacts of new technologies.

Now new technologies often have major social implications, including for privacy. Indeed, it often seems that the more transformative a technology, and the greater its potential benefit, the greater concern about the social implications. As society adapts to new technologies, such concern often generates and drives policy conversations.

These conversations are an important part of the cycle of social adaptation to technological change. In that cycle, a new technology first prompts social resistance, then gradual adoption, and finally assimilation. And through this process, society adapts. And this cycle has occurred over and over again in the area of privacy.

Although society adapts differently to different technologies, such adaptations often include changes to social norms, and then sometimes changes to law or policy. So one terrific example of this cycle is captured in Samuel Warren and Louis Brandeis's influential article titled "The Right to Privacy." They wrote that article in part as a reaction to how reporters and others were using the then new technology of portable cameras. They opined that instantaneous photographs have invaded the sacred precincts of private and domestic life.

Now Warren and Brandeis wrote those words in 1890, 16 years before Lawrence took the photo a San Francisco. Society has long since assimilated the particular wave of photographic technology with which Warren and Brandeis were concerned. In part due to their article, courts developed common law privacy torts, such as intrusion upon seclusion. And states adopted Peeping Tom statutes. And people developed social norms about when and where photographs are acceptable.

Still, Warren and Brandeis's concerns echo today in the words of those worried about how drones will impact privacy. Now perhaps that should not be surprising, given that drones can be used as flying platforms for sensors-- including cameras. In any case, it's clear that we are in a new cycle of technological adoption, and today's workshop is part of the conversation about how we adapt.

But what has been said about drones and privacy before? Or before today? First, many talk about the clear potential of drone technology to benefit consumers and the economy. Drones are already used to quickly and cheaply survey real estate, monitor unsafe areas such as forest fires or construction sites, and gather important news. And new and innovative uses are emerging every day.

In addition, there's been significant news coverage about drones and privacy. Many of these stories cover cases of misbehavior by individual drone operators using their machines in frankly creepy ways, or other people's hostile reaction to being filmed by drones. And some of the stories discuss law enforcement use of drones, and the potential impacts on civil liberties and constitutional rights. And in response, multiple state legislatures have sought to address such concerns by setting restrictions on how law enforcement may use drones.

But on that point, let me note that at the FTC, our enforcement jurisdiction is limited to acts or practices in or affecting commerce, which probably excludes most cases of individual Peeping Toms, and certainly excludes law enforcement or national security uses of drones. So just keep that in mind during today's discussions.

At the federal level, several other agencies have contributed to the conversation about drones and privacy. The Federal Aviation Administration considered, but eventually declined to adopt, specific privacy rules for drones. The Department of Commerce, through the National Telecommunications and Information Administration, hosted a multi-stakeholder process to develop a framework regarding privacy, accountability, and transparency for commercial and private UAS use. And they subsequently issued a set of voluntary best practices. Now today's workshop will build on these efforts and continue the conversation.

Now as you know, the FTC is the primary law and privacy law enforcer in the US. In addition to our enforcement docket, we use a wide range of tools to protect consumer privacy. And I see today's workshop as a continuation of our longstanding effort to educate ourselves and the broader public on the consumer protection implications of emerging technologies.

Now we always strive to get it right when we enforce the law. And we seek to apply the same rigorous approach to our workshops. So we want to hear from all sides. We want to understand the technological trends, the existing and potential benefits, and possible consumer protection issues, and the legal and economic environment.

Today's presenters and panelists will discuss the details of drone technology, consider whether drones raise unique privacy concerns, offer research on consumer perception of drones, and finally debate potential privacy approaches. Now while these panels will focus on these detailed topics, I hope that all participants in the ongoing conversation about drones will keep a sense of perspective. I hope they'll zoom out occasionally, and climb to the 2,000 foot view, and stay aware of the larger cycle of technological assimilation, and the variety of strategies-- including non-governmental-- that society uses to adapt to new technologies. Such awareness will help focus government efforts where they are most needed, and most effective.

So thank you, and I look forward to today's conversation. Thank you, Jamie.

JAMIE HINE: Thank you very much, Commissioner Ohlhausen. And it's now my pleasure to introduce our first presentation, from Joseph Calandrino, Phoebe Rouge, and Chrysm Watson Ross, of the FTC Office of Technology Research and Investigation here at the FTC.

JOE CALANDRINO: Hello, there. Thank you to everybody for making it out, or making it to this today. And I hope that you all are having a good afternoon, and that this will be an enlightening discussion on this afternoon.

I'm Joe Calendrino. I'm the research director of our Office of Technology Research and Investigation here. And over this past summer we had the pleasure of being joined by Phoebe-- Watson Ross, who is a graduate student in computer science at the University of New Mexico. While she was here, she helped us explore some of the privacy implications related to drone technology. So now I'm going to let Phoebe from my office, as well as Chrysm, discuss what they actually did over the course of this summer.

PHOEBE ROUGE: Hello, everyone. So when talking about this, first kind of wanted to set up. So why are we as the Office of Technology, Research and Investigation, looking into drones? So really, many of the same technological forces that are impacting the development of smartphones and other internet of things technologies, are also propelling the development of advancements in drones. So that includes things like component miniaturization, having better and smaller batteries, having very cheap sensors-- including high-resolution video and audio recording.

What this has resulted in. The next slide, there? There we go. Sorry.

So what this has resulted in is an evolution in drones, where even basic and cheap hobbyist drones are essentially becoming flying computers. So essentially what we're seeing is technology that was 10 years ago reserved for large governments or militaries or large corporations is now able to be widely accessible to everyone, including consumers and businesses. And very well in the future this may continue to grow, and become just as ubiquitous as some of the other devices that we have seen. And that includes use of these rather advanced cheap drones in other uses other than just hobbyist uses.

So as I said, any time that you have technology that is novel, and you put it into so many different hands, you're going to end up with a whole bunch of different uses, many of them that you wouldn't have expected. So just a couple of examples here. One, where drones are being used to deliver medical supplies to hard-to-reach areas in Rwanda. But we've also seen reports of, for example, someone using drones in an innovative display of graffiti in New York City on a high building. And I'm sure that there are many other ways that we have just not considered yet.

However with also the new technology being widespread, there's also a set of privacy and security concerns. And many of them are overlapping with some of the other devices, like smartphones and IoT. Unlike smartphones and IoT, very often the drone is not necessarily going to be on all the time, and not always on an individual person.

But drones also have some unique properties. For example they can go places that an individual could not. And they can move independently, and some of them even autonomously.

And then shared by both, there's the questions of any sort of networked or a computer platform, where you have need for authentication, access control, deciding what level of security, versus the ability to actually use the device. What happens when you collect video, audio, and other private information? If there is data being transmitted or stored, how is it encrypted? How is it protected? And then, of course, there's always the risk in the future of some sort of malware affecting that targets any sort of device like this.

So our focus was basically to look at drones from this perspective of network technology that has these various privacy concerns. So what we did is we looked in our case at some three different drones under $200. They're popular in the hobbyist market. Our sample is representing sort of the general population of inexpensive drones that you can just buy off the shelf. And the general privacy principles that we're talking about, though, apply to drones in general. And other researchers have also looked at other drones that are at different price points looking for similar issues.

So to actually talk about the research that was done over the summer, we're going to have Chrysm and Joe come up next.

CHRYSM WATSON ROSS: So we examined a few technical aspects of these three drones. And the findings we found of note, some of the more interesting ones, were, for starters, all three of them acted as Wi-Fi access points. Which means you could connect to them like you do a home router.

But all of them are open access points, which means they required no password to actually connect. And all of them had both video and control signals sent unencrypted, which meant that any observer who was in signal range could capture and review this information. And then two of them allowed root shell access via Telnet, which meant that there's a login to administrative account on the on-board computer. And so people could do administrative control over the drones via this mode.

And then one of those actually allowed this Telnet access without a password. So anyone who's close enough to connect to the drone could actually access its computer and then its operating system through the Telnet.

And then all three of the smartphone apps either had no or inconsistent notification when someone else was connecting to the drone. So that you wouldn't necessarily know if someone else was observing the video signal from the drone. And so now we are going to demonstrate some of these findings in action. Yep.

JOE CALANDRINO: OK. Just give this a moment. Am I coming through the microphone there? Actually, let's just turn these on, and I can do this. All right. Sorry. We're just having a minor mic issue here. But I think that we can handle this just fine.

So we're going to demo two different things here today. The first thing that we're going to show is the ability to connect from an arbitrary device to the camera feed that actually is provided by a drone. The second thing that we're going to demonstrate is the ability to actually interrupt the control feed between a device that's controlling a drone-- like a smartphone. Most of these particular devices have a smartphone application. And the drone itself, disabling the drone, which will cause it to crash.

So for the first part, what I've done, as mentioned earlier, there's an open Wi-Fi access point that's provided by this drone. The Wi-Fi is provided just for standard control. There's nothing wrong with providing Wi-Fi But in this case there's no password that's preventing me from connecting to it and using this particular laptop.

So I've now connected to it. And what I'm doing right now is I'm just running a standard video player on the application. That video player is going to be showing the video feed from the drone itself. Now I'm going to move over to the drone and wave at it. And Chrysm, once you see me in there, there's a little bit of a video delay just in this connection. If you could just turn around the screen.

CHRYSM WATSON ROSS: And there he is. Right.

JOE CALANDRINO: Now the second demonstration is slightly more complicated. But it involves a similar type of concern overall. So I'm remaining connected to the wireless network that's being provided by that drone. But for this particular drone, we can actually directly telnet into it. And by telnetting, you can think of it just as logging into the device.

And once you've logged into the device, you can open and close programs just like you can on any other computer. If I wanted to open and close Microsoft Word on my computer, I can do that. Same type of thing with this drone.

Now the actual controls for this drone, and the way that it interprets commands that are being sent to it, is that it has a program running it. So if from a smartphone you're running the application for that drone, I say fly higher, that program will take that command, and it will actually translate it into the drone itself flying higher.

So what I'm going to do now is type in the command that would actually cause that program to be killed off. So one moment.

OK. So I've typed in the command. But I have yet to hit Enter. Now we're going to have a phone connect to the device. Sorry. This takes just a moment to connect.

And I'm going to hand over the laptop to Chrysm. And I'm going to load the control application, and have the drone fly up. And whenever Chrysm chooses, she's going to be the boss at this point. She can just make it fall back down again.

So now I no longer have any sort of control link to this drone anymore. Strictly from that computer alone, the control has been disabled.

Now we could have done something more sophisticated here. We could have sent commands for it to be able to fly in another direction, or do things like that. But for the simple point, I'm just showing that you have this level of control over the device. I think that this suffices.

So with that, that will conclude the demos. And I'll just pass it back to Phoebe to wrap everything up.

PHOEBE ROUGE: All right. So as we were saying, the same access that you have to other different computers and network devices, we have to this particular drone. And what that's resulted in is that any sort of other privacy concerns that apply to land-based computers can also apply to some of these drones.

So for example, research has shown as far as the collection of MAC addresses. So MAC addresses are unique identifiers for devices. It's very easy for a wireless equipped Wi-Fi equipped drone to collect those MAC addresses if they're being broadcast.

Similarly, Wi-Fi networks, when a phone, for example, let's say last night you stayed at a hotel, that hotel's network is saved on your phone. Later on that phone will then try to probe some probe requests over Wi-Fi looking to see if that network is in range. You can configure Wi-Fi adapters in a certain way such that you can see those probe requests. So in theory you could have a drone flying over a crowd for example, and figuring out that any number of them in aggregate had been staying at a particular hotel last night.

You could also employ facial recognition software along with GPS tracking, where you could actually track individuals. You could figure out that a particular individual is present at a particular location, find out where in the world that is, and then track them over time.

And there are numerous other issues that researchers have explored. So one of the strategies for preventing drones for entering restricted airspace is geofencing, where certain GPS coordinates are off limits. However, our research here has also shown that the GPS signal that the drone is using can also be modified so that the drone thinks it's somewhere else.

Of course, just as with computers, fortunately there's also a large number of mitigation strategies, many of which are already employed and known. So first of all, you can secure the Wi-Fi signal such that the signal is encrypted, and that there is required a password in order to access it. You can encrypt the actual traffic to and from the drone.

You can have access to the drone as a full shell, as they have now, but have an authenticated logon. You can also envision a secure pairing mechanism, where only a particular device is allowed to access the drone. You could also use some sort of custom control signal, rather than Wi-Fi, and many others.

And certainly there's been a lot of movement in this direction by manufacturers, and even by hobbyists, who have had their drone, and decided, well, I do want to secure the Wi-Fi. So they figured out actually how to configure that.

Of course, also there are going to be trade-offs. As with any other security concern, there may be trade-offs in functionality, lower battery life due to the encryption requiring extra processing power, and just general locking it down, restricting the ability of people to actually tinker with it.

Overall though, we just conclude that there are definitely substantial potential benefits to this technology becoming widely available. But like any other new technology, it comes with a set of privacy risks. Some of them are unique to drones. Some of them are ones that we've seen before in other technologies. And essentially, drones, even at a very inexpensive level, are evolving to be essentially flying computers, with many of the similar concerns as other computers-- but also many of the same solutions.

All right. And thank you

[APPLAUSE]

JAMIE HINE: Thank you, Joe, Phoebe, and Chrysm. So I'd like to ask all the panelists for the first panel to please come up to the dais.

So it's now my pleasure to introduce our first panel, addressing the question, "Do drones raise unique privacy concerns?" This panel features to my far left, Dr. Greg McNeil, a professor of law and public policy at Pepperdine University School of Law, and co-founder of AirMap. To his right, Jeramie Scott, a director of the Electronic Privacy Information Center Domestic Surveillance Project. To Jeramie's right, Brendan Schulman, vice president of policy and legal affairs at DJI. And to Brendan's right, Kara Calvert, director of the Drone Manufacturers Alliance.

KATIE WHITE: Before we get started and dive into this, the focus of this panel, which is do drones raise unique privacy concerns, I just wanted to give any of the panelists a moment if they have a response, a point of clarification about the presentation we've just seen?

BRENDAN SCHULMAN: Is this on? Great. Yes, actually I'd appreciate that.

So DJI's the market leader in consumer and commercial unmanned aircraft systems or drones. My colleague Jon Resnick has our Phantom 4 drone down there. It came out earlier this year.

That presentation was interesting, but I do want to be clear that the Parrot AR drone that's on the table is 10-- almost 10 years old. It was released in 2010, and is really not the kind of technology that people are using in commercial recreational activities today.

We've also taken measures just within our own company to address these kinds of concerns. We've encrypted the control link. So the kind of hijacking that you saw, where the drone was turned off remotely by another person, can't be done that way. We've also used signed firmware in our new products to prevent tampering. We've also got methods to prevent GPS tampering. We're not going to tell you what those are in a public forum like this.

And there are other security measures that could be implemented if there were real concerns about hijacking the video feed, and doing things like that. If we saw drones being used in sensitive operations, if the customers came to us and said, look, we really want that feature implemented, I strongly believe that the industry will address those concerns, whether they come from government, or from our users.

And I'd also want to note that ASTM is working on standards to deal with these kinds of security-related issues. So I would just caution everyone watching that presentation to look at the current technology. I think it's very different from what you saw over there. Thank you.

KATIE WHITE: Anyone else? OK. Well let's sort of shift our focus to talk about more commercial use of drones, and the privacy features. But if Brendan, if you could actually set the stage for us with what technologies are available on drones today, and what do we see in the near term-- six to 24 months down the road?

BRENDAN SCHULMAN: Great. I'd be happy to. And thank you again for hosting us. So drones are used in so many applications. I think many of us have heard just the wide range-- and we'll continue to hear today-- of what people are doing with drones-- everything from agriculture to infrastructure inspection, real estate photography. Hollywood cinematography was one of the first uses for the Section 333 exemptions that the FAA issued starting two years ago.

Some of the more fascinating applications I think are the ones that are only starting to emerge because people have access to the technology. They can buy it affordably, and they can use it in a safe and accessible manner.

So for example, just in the past few months we've had someone at a research university used one of our drones to fly behind the spray of a whale, and collect literally whale snot. So they're actually flying through the blowhole without disturbing the animal, without causing a hazard to the animal, to collect a biological sample which could be used to determine whether or not the whale is pregnant, what the gender is of the whale, is it healthy, migratory patterns, literally save the whales. If you had asked me a few months ago or last year what are people using drones for, I would not have guessed that anyone would have come up with that.

We also had a story this past week-- it was in the Washington Post-- of someone in North Carolina using one of our drones to fly around the flooded areas, really was just feeding up the pictures to the Twitter feed as a recreational hobbyist operator. Someone on Twitter who was his follower saw the picture, recognized it was his brother's house, and that his brother was still there. And they sent in a search team and rescued that person and his dog from the flood. They were trapped there.

So this technology in the hands of people, just everyday people-- consumers as sometimes they're called-- is being used for incredible things. And I think as we now finally have a set of commercial rules, and as the technology advances, we're going to see more of the kinds of things that we actually aren't talking about-- not just agriculture and aerial photography, but a whole range of things. And it's very important for regulators and the government at the state, local, and federal level to enable people to use the technology in a reasonable way.

KARA KALVERT: I would just add, I think one of things you also should think about is the ecosystem that this creates, and the platform it creates in terms of technology and the new capabilities. So it's not just that they're going to be using it for new and interesting uses, but people are going to build on top of this technology with new sensors. It really will embody what IoT-- it was mentioned the IoT, the internet of things, as part of the presentation. This is going to be a platform on which people, and whether it's recreational, commercial, civic, humanitarian, they are going to find ways to build on top of the technology, and create really new and interesting use cases, because you're going to have new capabilities.

I think it's difficult for us to know exactly what those look like, just because it's difficult to predict what IoT will look like in a year, or how we're going to go with things like AI and automated vehicles. Those are all kind of developing the same type of technology at the same pace. So innovation will help drive many of these new devices in how they are going to be used.

KATIE WHITE: When we think about drones today, do they resemble other technologies closely enough that when we talk about privacy, we shouldn't segregate them from the other sort of technology devices?

GREG MCNEIL: So I actually think this is one of the more interesting questions to try and wrap our arms around. How people approach this technology oftentimes leads them to the particular legal conclusions that they have about it. And so we saw in the first presentation the analogies to these being flying cameras, or oftentimes flying cell phones, because privacy law and other technology laws are oftentimes balkanized, that would lead us to a series of conclusions about these devices. Whereas if we approached-- those are frankly toys that were hacked. If we approached sort of toy law, consumer protection law, consumer safety law, with regard to those devices, I think we might have a different approach to them.

As another example, one of the questions that was brought up as a thought question for us was about the ability of those devices to pick up various Wi-Fi hotspots. And then we'd be able to trace back the location of that device. That may sound problematic if we analogize these to cell phones, where we'd be concerned about tracking of particular individuals based on their cell phones.

However, if we liken them to aircraft, the FAA's perspective on this is that every aircraft, every manned aircraft, we can look up in the sky, you can point an iPhone app actually at the sky, and you can know the name of the aircraft, it's end number, you can know its location, you can know where it's headed. And so the frame and the lens through which we approach analyzing these issues, I think actually leads us to certain sets of conclusions.

And I think the question that flows from that is are the existing sets of ways of looking at things correct, or might we need to, with these devices in particular, try and find the best aspects of law from a variety of different perspectives. And that might mean that certain elements of aerial surveillance law apply or they don't. Certain elements of IoT law or internet law apply to them. I think those are the challenging issues that we have to wrap our arms around. And so yes, there are a lot of analogies. And where you start from oftentimes determines what conclusion you're going to end up with.

JERAMIE SCOTT: Let me just add onto that. And from EPIC's perspective, yes, drones are unique with respect to their implications for privacy. And that has to do with what was alluded to in the presentation before this, is that they're essentially aerial surveillance platforms that can have a bunch of different types of technology on them.

And what has happened as drones have increased in popularity, they've become more accessible and affordable to the public. And they're also accessible and affordable for companies to have in scale. And what I mean by that is eventually you can imagine, with companies like Amazon and Google, they're delivering packages, them having fleets of drones flying around to deliver packages.

And if you know anything about tech companies, they like to also collect information. So it's not out of the realm of possibility that the technology used to navigate the air space with those drones flying around will also be used to collect information about the environment and the public below.

And I think it's necessary, as we move forward with drones, that there's a level of kind of baseline protections, particularly with respect to transparency, so the public understands the capabilities of drones, how they're being used, what information's being collected, and who it's being shared with, and how long it's being retained.

KARA KALVERT: I would add, I think that as Commissioner Ohlhausen recognized, that the evolving technology creates just a new iteration every time about what is privacy, what is security. There are policy questions that arise in Congress in the regulatory environment every time you see a new type of technology. And I think that there are more similarities than there are differences.

And when you're talking about privacy, that's what we're focused on here, it's really about behavior. It's about how do you maybe invade somebody's privacy, and however you determine what is invading privacy. But we're also talking about things like stalking, harassment.

There are laws on the books that deal with those types of issues. There's a federal statute to make sure that you don't use a drone, or any type of technology, to stalk or harass. And you can go under that federal stalking law, Title 18, to go after somebody.

So there's Title 5 when you want to talk about transparency in terms of commercial operators using certain types of data. How do they use it? How do they collect it? How do they share it? Those types of things are already covered under current law.

So I think the technology is new and different, yes. And it provides some very robust capabilities that I think is really interesting, and presents new questions about how do you collect that data, and how do you use it. But it comes down to behavior. And if you misbehave in using that data, or if you misbehave in using it in a way that you said that you were not going to, there are mechanisms in place currently to deal with that kind of behavior.

JERAMIE SCOTT: Just to follow up on that comment, and I agree, there are some laws on the books that address some of the kind of privacy, invasive behavior that drones can be used for. But you've also got to recognize that it would be very hard to enforce those laws in many instances, because of the nature of drones being kind of aerial platforms that can be controlled remotely.

Actually this past summer, I was on a boat with some friends. And we were driving around this little island. And a drone came around, just was flying, hovering right above us, and just followed us for a while until presumably we were out of range. But I was looking around. I couldn't pinpoint where that drone operator was at all.

Its one of the reasons that EPIC suggested in comments to the FAA when they were doing the registration process for drones that that registration number needs to somehow be more accessible. It just being on the drone itself is not going to cut it, because the chance of you being able to see that are going to be slim.

And in a better world, that information would be broadcasted, the drone registration number. Perhaps also the capabilities of the drone. But at minimal, the drone registration number. So if you do see a drone kind of acting in ways that you thought went against certain laws, you would actually have the ability to track down the person who owned that drone.

JAMIE HINE: Greg, I was going to come to you and see if you could put it in the context of AirMap, and some of the uses that you're facilitating.

GREG MCNEIL: Yeah. So let me try to connect up the two concepts. I think one of the challenges that all emerging technologies face are not only the unique harms that may be raised, or potentially raise, but also how can policymakers actually make accurate judgments where they don't exacerbate problems.

As an example, let's take the hacking that we talked about of the toy drones earlier. The fact that the drone can pick up Wi-Fi hotspots might sound to us like a privacy problem. But also that's a backup mechanism by which the drone itself can geolocate.

And so you all know this. When you walk around with your cell phone, your iPhone tells you that your location sensing capabilities would be enhanced. And it will know that you're on the corner of 1st and Main, not on the corner of 10th and Main, if you turn on Wi-Fi, because it's identifying the Wi-Fi hotspots that have some location-based features associated with them. The IP address is located down to a physical place in the environment. And that actually helps with navigational capabilities on your phone in a complex sort of signal-dense environment. And so if we were to say don't sniff Wi-Fi that's publicly being broadcast, we would actually make the device less accurate.

Similarly, when we say things that we see in the privacy context often times, don't take pictures of people's faces is sort of like the standard reactionary privacy law that we say. Or if you do, make sure that you redact those faces, which is actually pretty computationally intensive for the technology side of things. And if you wanted to do that, the thing that you might lose is something called, SLAM, which is basically our simultaneous location and mapping capabilities.

Imagine that I have a spinning camera on a Google drone, or on a Google driverless car, and I'm constantly taking photos of this area. I'm taking photos of this area and I'm picking up your faces. But those photos are also allowing me to know that some of you are 5'9, and some of you are 6'1, and some of you are 4'11. And knowing that at that moment allows me to then be able to navigate through this complex environment.

So were we to say don't collect this sensor information, or don't collect this visual information, we've now actually made the device less capable of knowing where it is in the environment. And so each one of these incremental attempts at regulation may actually have consequences.

And so here's the big consequence. You can spoof GPS. So if we have an environment where GPS is spoofed, so military GPS is more secure than the civilian GPS you use. If we have an environment where military GPS where the civilian GPS is spoofed, the drone is going to need some ability to be able to know its location and navigate in the absence of GPS. And that's where picking up visual indicia will matter, and picking up additional signals will matter.

And so if the concern is, oh my gosh, someone can hack GPS, and our concern is the privacy concerns, well, what we'll do is we'll end up regulating the device to a place where it's actually not able to advance, without actually really protecting against any cognizable privacy harms. Because the navigational component of gathering your facial information has very little to do with the information that's gathered for other purposes. And so it's very hard to work in this space, I think, without taking account of that.

And so let me turn from sort of that descriptive to a bit of the normative. Probably the best way forward-- and Brendan mentioned this-- is taking a policy stance that recognizes that you define it with pretty good specificity the type of harms that you want to prevent, and then really, if we want to move forward at the pace that the cell phone industry has moved, relying on consensus industry standards to be able to craft the manner in which we mitigate those privacy harms, as opposed to having regulators or Congress being very prescriptive in the types of rules that they're setting for the industry. I think that's how you get the balance. Trying to do this on Capitol Hill through a compromise process, or through a regulatory process, is really a path to lack of innovation, and oftentimes less safety and fewer privacy protections.

BRENDAN SCHULMAN: I think it's really important to try to identify what is the problem we're trying to solve. So Jeramie said drones are unique. And they're aerial surveillance platforms. I strongly disagree. We have seen what people use hundreds of thousands of users use our drones for. And they're not conducting surveillance. They're doing things like Hollywood cinematography. And in many instances, the drone is just being used in place of a railroad track jib with a camera to fly a smooth pattern around the actors. Absolutely not being used for surveillance, and not for any nefarious purpose.

And we don't know what the person was doing out when you were boating, but maybe they were looking for or working with the whales, and doing conservation efforts. So even if you had that broadcast registration number, what would you be enforcing in that context? So first we have to define what the problem is we're trying to solve. And also be very careful about the media reports that we've heard.

There was this report in the Seattle Times I think a year or two ago-- actually I have a copy of it here-- "Regulatory Vacuum Exposed After Peeping Drone Incident." So this was in the Seattle Times newspaper, and then went national. It was about someone flying a drone in Seattle, and someone who was only partly clothed in her apartment saw it out of her window, and assumed, well, it must be peeping, perhaps the way you felt that the drone was following you. She spoke about it to the media. It made national news. The headline was "Regulatory Vacuum."

But is there one? If you actually, as I did, ask the person who was flying the drone what were you taking a picture of, he actually sent it to me. And here it. It is a panorama of the skyscape in Seattle from where the building that he was working on would be built. So this was a construction project. What is my view from the apartment going to look like once the building is done. It's a very common thing that drones do is give you the future view from your apartment.

So there was no peeping. There was no way to peep. This is a wide angle lens, like many cameras, like the Phantom 4. You couldn't even see someone in this picture behind a window.

So let's figure out what the problem is, and then solve it. And also take into account the existing law that is enforceable. There already has been a prosecution in New York State under existing unlawful surveillance law went all the way through trial and a jury verdict-- someone who was flying their drone near a medical facility, and allegedly was peeping into the examination rooms. That made a lot of news and ended up being acquitted, because he actually couldn't see into the rooms. It was a mirrored surface. So let's start by defining what the problem is, and then I think we can all work together on solutions.

JAMIE HINE: I think Jeramie, you had a response.

JERAMIE SCOTT: Yeah. First of all, the story about the boat and the drone, I mean, the drone actually was not far above the boat, and actually followed as I turned the boat. So they were definitely kind of tracking us.

But the real point of it wasn't that they were violating some specific law. The point was, if I thought they were, I wasn't going to be able to identify who was doing that. That was the actually underlying point of that story. And that is an issue. When if a drone does violate a law, or you think it does, it's very hard to identify who's using that drone, or the owner of that drone.

Second the larger concern I have is not so much individuals using drones, but it's commercial use of drones. And I think it's easy to project that drones will be used to collect information. I don't think we should sit on our hands and think and just wait for that to happen without thinking about what type of baseline safeguards could we put in place with something that we know is going to happen.

For drones to navigate autonomously to deliver packages, there's going to have to be a whole bunch of different sensors for them to do that to kind of navigate their environment. And as I mentioned before, companies like Amazon, Google, like to collect information. An example of that is with the Google Street View car, which was not just checking where Wi-Fi networks were, but actually collecting the data on unprotected Wi-Fi networks. And they actually get in trouble for that.

So if we know drones as aerial surveillance platforms can go in a bunch of different places in the future, we see that there potentially may be a bunch of drones flying over populated places, and with capabilities like facial recognition, license plate readers. Your cell phone gives off a unique identifier as it pings cell phone towers that can easily be picked up by drones also. And that was actually tested by a drone company to use it for location-based advertising.

Well I think it's sensible, I think, well the public should understand what drones are being used for. And if it's going to be used for to collect data, if there's sophisticated equipment that's going to be added, surveillance equipment added to these drones, well maybe the public should know about that, so they can actually provide a voice about the use of drones, and what they think the policy should be. And we shouldn't wait until drones are kind of implemented in a way that makes it hard to then, after the fact, kind of implement some type of a policy.

As an example of that, we saw this in the late '90s through 2000 with cookies. Now I'm not talking with the cookies you eat. I'm talking about the cookies on your computer, which were originally used to kind of track your cart as you bought stuff, and maybe track some other little information as you were on a website.

Now people didn't realize, or were kind of unfamiliar with the cookies for a very long time. And a whole kind of advertising structure online developed around it that was based on tracking massive amounts of information on users as they navigated through web pages and websites. And now most people, now that they have a better understanding of the information that's collected-- and even though they probably don't realize the full extent of it-- don't actually like that, and don't feel in control of their information and what happens online. But the structure of that is so ingrained in online advertising, it's very hard to change that at this moment.

But the surveys done by Pew and whatnot, who kind of look into how people feel about the control of their data online-- and a lot of this has to do with online advertising, behavioral advertising-- people feel like they don't have control, but they don't feel like there's much they can do about that. And now we see a technology, technology has similar implications for the public space. We should kind of heed what has happened in the past to be a little bit more proactive about implementing some baseline safeguards that allow for the innovation, but also provide some protections and some transparency.

GREG MCNEIL: So I've listened carefully to Jeramie's concerns. And I think they go back to the initial framing point that I raised earlier, which is about the perspective that you take when you approach this. And I think that a lot of what I heard Jeramie articulate were not concerns that are unique to unmanned aircraft, unique to drones, but instead are concerns that seem to be something bigger about what we need to grapple with as a society when it comes to technology.

So for example, the Google car was sniffing Wi-Fi. I think it was inadvertently misconfigured to be able to pick up the Wi-Fi data, not that that was the intent of the operation. But that's about a car. And so we're using that as an analogy to say, well that's something that a drone might also be able to do.

Well that actually sounds like some technology-enabled devices may be able to have certain types of harms that concern us. And so maybe then the way to approach this as we think about it is not about treating drones as unique or different, and launching off and going after drones as the target, because we're all now comfortable with cell phones, but instead ask ourselves a series of questions about how we feel about location sharing on any connected device, as opposed to just location sharing when it comes to drone.

I think it's hard. And I've spent a lot of time talking about this. Brendan and I have probably talked about this for five or six years. I see my friend Ben in the back, who used to work at a unmanned aircraft association. I think I've been chatting with him for like six years about these issues.

The question is what is unique and special about drones. And I will say that I think there are a few places where drones are unique. And it's not the fact that they can surveil from the air, because lots of devices can surveil from the air. I think there are two probably things that are the hardest for me to grapple with.

The first is the remoteness of the operator, separate from the device, which goes to your point Jeramie, I think, about the accountability mechanisms. And that's probably a fruitful place for us to have a bit of a discussion. And then the second is that there is a little bit of a locational capability with an unmanned aircraft that is unique from a manned aircraft, the ability to get closer into buildings, or people. The ability to perhaps slip in below a tree line. So imagine that you have a canopy in your back yard of trees. A manned aircraft might fly over and not be able to see in, but an unmanned aircraft might be able to come in from the side and be able to see something that otherwise was not observable.

So that's sort of a location-based issue, and a accountability sort of remoteness of the operator issue. I think that's a fruitful place to have a discussion, because those are two issues that are unique to unmanned aircraft. But the other issues I think are really not unique to unmanned aircraft. They're things that we see in other devices.

JAMIE HINE: Kara, to bring you into the conversation, I was going to ask you, are there other types of technologies that you think that raise similar issues?

KARA KALVERT: Well really quickly, I would like to go back just to the issue of the remoteness, and the idea that we just saw Congress pass into law a standard requirement around remote standard identification, and putting together some really thoughtful stakeholders on how you come up with those. As manufacturers, it's very important that we don't have really prescriptive standards, but rather we have what are we trying to accomplish. Again, if you're trying to accomplish the identification from ground to air, or if you're trying to accomplish it from a mile and a half away, those are the types of things that we need have a conversation about, and it needs to be all the stakeholders in the room in a transparent way coming up with those standards. So I think that there are, in my opinion, that's one of again the few unique areas.

Again when you look at the whole range of technologies, when you think about online advertising is a great example of where self-regulation is actually starting to work. It's also a great example of where existing authority actually did put some parameters around some operators online. So again, existing authorities actually covered that.

We think if you think about financial technology, if you think about the new artificial intelligence, if you think about some of these new capabilities, I think what we really need to be cautious in doing is we need to approach it from an innovation standpoint rather than a regulatory standpoint. Because when you start to neuter the capabilities by regulation, you actually neuter not only the ability to deal with some of these whatever the perceived problems are, but you also neuter the solutions. And when we think about safety and whether it's remote identification, technology is going to lead to how you actually accomplish that. You're not going to be able to do it by slapping a sticker on the side of it. So there are going to be things that technology needs to do to actually achieve those.

If you think about financial technology, technology led to a better authentication process. So those are the types of things that we need to be thinking about. And then use, I think again, the existing statutory authority of many agencies-- of this agency in particular-- but again state and locals who are also looking at the privacy concerns.

I would know, as we're talking about state and locals-- actually I would know two more things. But the state and local issue, as you think about drones, it's important to think if you're trying to do things in the name of privacy, specifically altitude restrictions, or flight limitations, that starts to impede the national airspace, and you actually start to deal with safety. And you impede safety.

So we have to be very cautious again on what are the problems we're trying to solve. Not just say, oh we have a privacy concern, and therefore we need to create an entirely new siloed regulatory structure. So I think those are very important things.

The other issue I would just go back to on remote identification. We actually have to have be cautious of the privacy of those operators. Just because you're flying a drone doesn't mean that you have just given up all your right to privacy.

We've seen this in the conversation around the registration, and what is publicly available information, information about the operator. We do have to be cautious about how does the operator, what kind of rights does the operator have? What kind of information needs to be given? What are they doing? What are their technologies? What are their capabilities?

I think that raises really interesting questions. And very sensitive information that you're asking to just be spewn about, whether or not it's on the internet, or by app. I think we have to be very cautious in protecting everybody's privacy-- not just a perceived privacy problem.

JAMIE HINE: So do you have any thoughts about what that balance might be? Sort of balancing the transparency of sort of going back to Jeramie's example, the consumer saw the drone over the boat. I'm presuming it was a hobbyist that was operating the drone. But if there were a mechanism to use an identification number to try and understand what are the capabilities, what is that drone doing? Is it delivering a package? Or is there a secondary type of collection? What would that balance be about having the ability for a consumer to learn more about the capabilities, versus protecting that user?

KARA KALVERT: It's a great question. I think it's the million dollar question, actually, what the balance is. I think it's also a matter of adaptation and evolution in how people become comfortable with drones, and how people see them being used.

Whether or not if somebody sees a drone in the air right now, I think the perception is, well, are they using it to surveil me? Oftentimes if you're in a rural area-- I'm from Wyoming-- when I see a drone up, I don't think that they're trying to surveil me. I think they're trying to look at their crops.

Or when I went home for an August, my cousin had a drone. And he went out and surveilled how many thousands of acres of our land had been killed by wildfire. So I think that there's a perception issue.

And what is the balance? Again I think it's very nascent. And to come in and have a very structured regulatory environment I think will actually cause more harm than good.

JAMIE HINE: So maybe Jeramie you can address this. But if we can talk a little bit about this perception issue. And sort of again going back to your example.

So I mean, we do have this perception issue that many consumers are encountering these devices in the hobbyist context. And that's very different from a commercial use. And so some have posited that there is this perception problem that if a consumer notices that it's being used to spy on a neighbor, or sort of, in your case, sort of hover over the boat without identifying itself, that that's the first encounter that a consumer has. It's not necessarily with a delivery, or knowing that their next door neighbor is using it for crop surveillance. So how much of a problem is that? And how are manufactures and commercial operators addressing that issue?

JERAMIE SCOTT: Well it's actually an issue we've pointed out before in comments to the FAA in terms of why we thought addressing the issue up front was important. I know Pew did a survey a couple years ago on the perception of drones in the US. Actually wasn't that great. Over a majority, like 64% said it would be bad if drones were allowed to fly around the US airspace.

And I actually don't I say agree with that. But I do agree with the idea that there needs to be some protections put in place. And that needs to be transparent to the public, because they need to understand that there are protections in place so they can feel more comfortable with drones being integrated into the airspace. That's why we constantly advocate for the transparency aspect of it, in terms of drone capabilities, the information collected, how it's used, who it's shared with, how long it's retained. Because that is going to give kind of the public a little bit more comfort that they can find this information.

And with respect to actually drone users. When we sent comments to the FAA about their drone registration process, we actually advocated for the privacy of the drone users, saying that their personal information shouldn't be readily available. What needs to be readily available is the drone registration number on the drone. That's what we thought should be broadcast. And then after you show there's a legitimate reason to kind of have the information to contact the user of that drone, then maybe you can get it.

But it shouldn't just be readily available to the public to look up when and wherever they want without any type of legitimate reason to do so. So I think we'll see a pushback against integration of drones unless we're more proactive about kind of implementing a certain baseline safeguards that help with it.

And with respect to the innovation kind of argument, from my perspective, if you can't innovate around some baseline protections, you're not being very innovative.

BRENDAN SCHULMAN: Jamie if I would just ask a question. You suggested that hobbyist use is very different from a commercial use. I would like to know what you meant by that in particular. Because the examples we've heard so far about what drones might do that might invade your privacy are analogies to things like cookies, and street mapping, and online advertising, and Wi-Fi sniffing, all of which are commercial applications where someone had a financial incentive to collect information and exploit it. So if I'm sensing a heightened concern over recreational hobbyist use. I'd like to know why. And why you might, if you are thinking of giving the commercial user some advantage, or a free pass in terms of a privacy regime, why that would be?

JAMIE HINE: So I wasn't intending to imply that there was a vast difference. I really was sort of going back to the example that Jeramie highlighted in sort of personal experience as well, where often I find that my first encounter with a drone many years ago, and people that I know, doesn't tend to be necessarily a positive one if they're not operating the drone itself. It's an unusual technology. It tends to hover. It tends to be doing something. And I don't know what it's doing, but it may be following me.

One of our colleagues in the office talked about he was walking home from work, and the sort of drone was sort of over his head. And as he sort of continued to walk down the street it followed him for a while. And then it eventually went away.

But it sort of had him thinking, what was it doing? Why was it following me? Was it taking a photograph of me?

And so I simply was using that. And it may not be a great example. But I think for many, many consumers who have never encountered the technology, it's not necessarily one where they understand. They have more questions than answers about what the capabilities are.

GREG MCNEIL: So I think your examples, Jamie, actually bring up, these examples always sound so stark. The drone was following me. So every time I come to DC, if I get in a little early, I go on a walk, and I just kind of clear my mind. I used to live here. And so I kind of check out my old neighborhood, where I used to live.

And I was walking through the neighborhood. And I swear the guy behind me was following me. So I stopped and I read a menu. And he just walked right by. But it was like the person was heading in the same direction as me.

There were people in the mall who were taking photographs with cameras with zoom lenses. Some people had GoPros. A GoPro camera with GoPro's new drone can be taken from your hand and affixed to the drone. Is it now a different privacy harm the moment it's one inch above the hands and affixed to the drone? I think not. Is it following someone because it's up in the air?

If we believe that all those things are true, those harms, then all these people in the mall should be wearing T-shirts that identify-- maybe arm bands, that identify the purpose for which they are gathering information. I have a right to know why people are taking photographs. I mean that's the logical extension of this.

Which then begins to lead us-- and this is the slippery slope of privacy law-- which you guys know really well. As soon as you start to get into these areas, the path of privacy law protections eventually leads to a conflict with the First Amendment, my right to freely associate; my right to freely gather information, not just for journalists and news gathering organizations, but for any person who wants to engage in that protected speech, of which photography is a protected form of speech.

And I don't see how it changes when we take the camera, and we put it on the drone, unless of course-- so now I'm going to get into our analogies-- unless of course we say that it's different, because these are aircraft. In which case every aircraft has to identify itself. Pilots, if you can look up any pilot and their certifications on the airman's registry at the FAA website, you can look up the home address, if someone is dumb enough to put it in, for their aircraft that is actually registered. So when you see that aircraft flying overhead, it has an N-Number. And you can look that up and trace it back to the person.

I'm not sure that we want that in the drone context, where the operator is on the ground, and they're in a neighborhood. Which again goes to the locational capabilities of this. Someone doing real estate photography in a neighborhood is potentially different than a helicopter flying overhead. And so we have these moments where this is just I say we as an industry, where we want to say, well we're very different. But then in other circumstances, we want to say, well actually we're very same. And the challenge we have in emerging technology fields is which things can you pick and choose from? Which parts of privacy law versus aviation law and others might we be able to pick and choose from?

On the question that the statement Jeramie made, though, about I don't think it's that hard to innovate around baseline standards, I just fundamentally disagree with that notion. The idea that every drone, if some congressional mandate or regulatory mandate, every drone would have to broadcast in some way, is actually a substantial burden on industry. You're talking about hundreds, perhaps thousands of dollars of costs-- perhaps to the point where the technology itself is simply unable to be operated.

And so then we get into a cost benefit analysis, where the FAA's economic analysis report on unmanned aircraft stated clearly that even if one unmanned aircraft was used, and one life was saved, the benefits of unmanned aircraft would outweigh their costs. And if we then say to ourselves, well, all of these devices should have to transmit, well how far? How powerful is the transmitter? Must that transmission also be encrypted-- which requires greater processing power, it requires greater battery power.

These are all trade-offs that manufacturers face in having to broadcast these types of things. Which might then mean that that one unmanned aircraft is not used, and instead a person's climbing a pole, and that person is going to statistically a person will climb a pole and die instead of us putting an unmanned aircraft there to see the exact same type of thing. And so we have these types of trade-offs that we need to work through.

Now if we instead take the approach that I talked about before, where we recognize the harms, we define what those harms are, and then we allow industry to innovate, to be able to address those harms, we get to a very different place. And I'll give you three examples.

The first example. Unmanned aircraft by law were generally required to provide notice to airports before flying within five miles of an airport. But Congress never defined how notice would work. My company AirMap got together with 125 airports. So LAX, Denver international, Houston Intercontinental, all the way down to municipal airports. And we created a solution that allows you to push a button on your iPhone and let the airport know that you're operating there. Call it remote identification for the airport. That is deployed today to 125 airports-- not because someone told us specifically how to do it, but because the law generally said that there was a harm out there.

Two years ago, when my co-founder and I went to the major manufacturers to talk to them about what AirMap could provide, we said, you know what? You're going to need to know something about wildfires, temporary flight restrictions, stadium flight restrictions. And initially this was a little earlier in the industry. And people sort of looked at us and said I don't know that we really need that.

Three weeks later, drones started flying into wildfires. Nobody mandated that we put that information about wildfires in unmanned aircraft. But we rapidly innovated. We figured out a cloud-based solution to provide that through an API. And now millions of end users get information about temporary flight restrictions, presidential movements. They get information about stadiums.

Then just three months ago, the Department of Interior came to us and said there are wildfires that don't get temporary flight restrictions. What can you guys do? No regulatory mandate.

We crashed on the problem for a couple months. They provided us a data set. And within 24 hours of providing us a data set, we turned to DJI. We said here it is. It's available to you. It's live. And the second that DOI becomes aware of a wildfire, a button is pushed at DOI, and it is deployed to millions of end users almost instantaneously. Again allowing innovation to move very quickly, rather than have these prescriptions that come from well-intentioned-- I'm not picking on anyone-- but well-intentioned prescriptions that actually slow innovation down, and slow industry down.

I am convinced that within the next two years, most privacy problems and most safety problems will be addressed in such a way by this industry that people will say, wow, those devices are the way we should be going. Why isn't manned aviation doing the types of things that unmanned aviation is doing? I think we're going to find the same type of thing happening in privacy. But it can't be prescriptive-- certainly not from DC in a country as diverse as this.

JAMIE HINE: So I just want to interject. So I did get a question. I know there were some question cards. And we have some available if folks have them. If you do a question, just raise it up in the air, and one of our assistants will come by and grab them.

So I don't know if the question was actually written a few minutes ago, or it was after the question that was posed to me. But the question asked, it's easiest to assume the worst about uses of drones, as we've seen in this panel. How or what role is there for a government to bring to light the good uses? We are the moderators. And I will pose that question to--

BRENDAN SCHULMAN: Well we just did a great event last week in collaboration with 4H. They do a National Youth Science Day. And they picked drone discovery as the theme this year. So 100,000 young students, middle school students approximately, got together on one day, and learned about drone technology, and presumably had a great experience, and then took what they learned back to their families and said, hey, I had a great time with drones. And I learned about all the things you can do with them. And I got to see one fly. And I got to build sort of a replica of a drone-- a Styrofoam airplane. That was an announcement that we put into the White House fact sheet that went out about two months ago.

So you can do a lot in government to encourage and to get out the word on the positive use cases-- education, science and technology. Don't forget that, as Kara put it, there are young people using the technology. If you do remote identification, you're going to have to think about whether you would identify a teenager in a backyard or not, how you do it responsibly. But those are also the people who can then go out and develop new things with the technology.

We currently have a pilot shortage in the United States, airline pilots. I think I saw an article a few days ago about Alaska running out of pilots up there. We want to inspire young people to learn about robotics and aviation and programming. And I think that there's a huge amount that the government do.

KARA KALVERT: Yeah, I think there are many opportunities to talk about how drones can improve, I think, particularly the education space is a really interesting one to consider. When you think about kids, and how they're learning to not only adopt and use technology in the classroom, but more importantly, how to build on top of the technology. And as I was saying earlier, about startups, about innovative young companies, many kids are starting these types of ideas and projects in their garages. And then they come up with a really innovative way to use the drone.

So I think in terms of government, how do we ensure that our educational system is, one, producing scientists and engineers and folks who want to use these devices? But also, is there curriculum? Are there other things that we can be doing to make sure that classrooms have this kind of capability, this kind of technology? And how do they use it, and how do they build upon it?

BRENDAN SCHULMAN: I have one specific thought to follow up. So I'm at the wrong agency. But I think it would be extremely useful if others, and with FAA, were to try to verify that the pilot sightings, the reports that we hear about drones near or at either at airports, or seen by airline pilots. Because it's very difficult for us and our partners to come up with solutions, like five-mile geofencing or other things, or height limitations, if we don't have verified, credible reports of what people are seeing.

And if you look through the so-called hundreds of reports that the FAA has compiled, that they're just people calling in. In some cases, those are not airline pilots, the people on the ground at homeowner association saying I saw a drone, and I assumed the worst. And I called the FAA. And now it's one of the, whatever, 100 sightings or purported near misses. So we need better data from things like that in order to build the features that help address the problems.

JAMIE HINE: I wanted to come back actually to Greg's point. So on the one hand, you were talking before about how we needed to define the harms. And then you made this comment about how in the next two or three years, we're going to see a lot of these privacy problems addressed through innovation technology. So I guess one of the questions to you is what are some of the technologies that are developing right now? And that's sort of presupposing that the industry's already defined what the harms are.

GREG MCNEIL: Yeah. So as an example, go back to the airport example, when we first decided to roll out the notification system for airports, I got a little bit of resistance from my friends in the industry, who said listen, if you give these airports a tool, they're going to say no. If you push these tools down to the most sort of local level, they're going to say no.

And actually what has happened across all 125 airports is that instead of a big red circle, the airspace around the airport has been basically tiny little triangles in the runway area. And so when a person files notice within that five mile area, it's oftentimes just the message is received, and then their immediate response is, thanks for letting us know. And that's because the airports we're dealing with people who are just calling on the phone and saying, it's Bob, I'm 4 1/2 miles from the airport near the 7-Eleven. And the airport doesn't know what 7-Eleven it is, who's Bob. And all of a sudden we have this challenge that technology solves.

So next thing coming down the pipe that we'll see, and this is largely because the FAA has shifted from a prescriptive we know best approach, and we're going to pick one of the DC beltway bandit contractors to build a five year, $5 billion technology solution based on the set of requirements that they came up with first.

Instead the FAA has shifted. So in the area of getting access to controlled airspace near airports-- that is to say, contacting the air traffic control tower, the FAA instead sent out a request for information. And what we've heard them say in some public presentations lately is they're looking for multiple vendor industry solutions. That is to say, to keep the competition in the marketplace, so people are rapidly innovating to try and make a better airspace system.

I think we'll start to see the same type of thing happen even in privacy. So you could imagine a circumstance where-- and there were like 49 vendors that bid on that RFI. And so that's 49 companies who have some way of connecting end users to air traffic control towers.

So let's take a city like New York City. New York City has very unique concerns-- large buildings, micro-scale wind, privacy implications of flying drones adjacent to windows at the 20th floor of a building where someone heretofore had never expected a device to be next to that window. And so New York's approach has largely been, we're just not going to allow these drones to operate.

You can imagine that a year or two from now, when this air traffic control authorization system is rolled out by the FAA, that instead now people using drones in New York City might be able to let New York City know that there are NYPD, or the Port Authority or whoever it is, let them know that they're operating there, in the same way that when you want to film the Batman movie in downtown New York, you simply just can't decide to start filming. But instead you're pulling a film permit, or something like that.

Now that's New York. New York probably needs something like that with the density of people that are in New York City. But if you tried to roll that type of solution out in suburbia from the Amazon distribution facility out to suburbia, or in agricultural areas, before one of PercisionHawk's drones is flying to do precision agriculture. That to me seems like it's a bit of overkill.

And so what we want is technology solutions that are customized to the particular area based on a risk assessment, which might include the privacy harm. Because privacy is very different in Montana than it is in New York City-- just the expectations of privacy, the number of cameras in New York City. I think that changes based on geography. And we want to ensure that we have sort of extensible solutions that can be customized based on the particular areas in which the operations are taking place.

So that's me projecting forward a little bit there. Which is not drone industry doctrinaire. I recognize some elements of it. Some people in the audience are giving me dirty looks. But I can see technology solving a lot of the types of safety and privacy harms that we're concerned about in the future.

KATIE WHITE: We have a couple questions that have come from the audience. First is, how would you feel about legislation setting forth use restrictions? Surely we can agree that drone operators should not market to people based on their behavior as observed by drones, for example. So do you have any thoughts on that?

JERAMIE SCOTT: I'll start, since I'm probably the only one that would support that up here. But yeah, EPIC would support use restrictions depending on what they are.

The drones do have some capabilities to collect PII-- personally identifiable information. There should probably be some use restrictions on that. But probably not on collecting information in the environment that's necessary for the drone to actually navigate, particularly when we get more autonomous drones flying. They obviously need to collect some information to navigate the airspace. But I think we'd be silly not to recognize that drones will have the capability to collect information that we might not want them to collect without consent.

KATIE WHITE: Would it be dangerous or problematic to have a set of rules around drone collection, and then sort of spend all the political capital on coming up with those sorts of rules, and sort of leaving other people, others using the same technologies, without those same rules? Is that a concern.

KARA KALVERT: I think that's exactly the concern. The data collected by a drone, while you may have a more robust collection capability because of where it can go and what it can do, generally it's no different than other data that's being collected, whether you're talking about an aerial shot, whether you're talking about photography, or a Wi-Fi or a MAC address, those are the same types of data that can be collected by other devices.

And to create one set of rules, imagine if you're a business operator, and you've got a security camera. You've got people taking cameras up on bridges for inspection purposes. And you've got drones. And now all of a sudden you have to have a privacy policy that recognizes all these different types of technology, how they're going to be used, and how that data may be shared in different ways. That's going to make it impossible for people to start to think about how do you use these in exciting ways, in ways that will solve problems.

So to create different use limitations or different privacy requirements just because the way the data is collected actually will certainly make the process, it will make it more difficult for operators to actually use and benefit from these devices. And I think at the end of the day, instead of the privacy concerns killing off the innovation, it's going to be the regulations that kill off the innovation.

BRENDAN SCHULMAN: I'm very supportive of problem-solving regulation legislation. So identify the problem, and then let's work together and address it. So if for example the use case concern is persistent surveillance. Let's deal with that as a society, and with a set of rules and law-- but not specific to drones. Any technology that you use to invade someone's privacy because you are persistently sort of doing surveillance is, I think, a societal problem we have to deal with without regard to which technology.

JERAMIE SCOTT: Yeah, I agree. There's obviously other technologies that can be used to kind of invade people's privacy. I do still contend that drones are unique, just because of the fact that they're aerial, the mobility of them. And the price point to do aerial surveillance drops significantly with drones.

So when we do have, as drones get integrated, and we do have companies who can send out kind of mass collection of drones over a population and collect data in mass, I think that we need to think about that ahead of time. Although I would advocate in place of that, a consumer privacy bill of rights, which would be great. That would cover more than just drones. But barring that, the uniqueness of drones and their capabilities I think would warrant some type of baseline protections.

KATIE WHITE: Is industry at all concerned that if privacy, or privacy issues that consumers perceive, like the things they're worried about aren't addressed, that adoption will be slow to come, or maybe not at all?

KARA KALVERT: So I think what we've seen is if you look at the Section 333 exemptions, and how that has taken off over the last couple of years in terms of commercial operators really wanting to take advantage, you can see that people are getting out there and using them, and in exciting ways. Part 107, that was just established by the FAA, is just now going into effect. I think we will see more and more data about how those are being used, and how many people are up in the air, and what they're using it for.

Again, while we've been talking about this for five or six years, some of the folks who were early, this is still fairly nascent. And to make a decision on right now whether or not people are adopting based on a perception I think might be premature.

BRENDAN SCHULMAN: I think some of the proposals we've seen this year and previously to try to address some of the concerns could have that effect. In fact, they probably will. So what we've seen on the state front, there have been over 280 state bills relating to drones this year alone. And many of them are about privacy, or purport to be about privacy. And the proposals in them sometimes include asking permission, or notifying the people that you're taking images of with the drone-- specifically with the drone.

And the problem with that is it's really impractical. If you have to reach the owner of the real estate, that can be really tough to do in any practical way-- especially if you have an apartment building, and everyone's a tenant. How do you possibly figure out who owns and who doesn't? Airbnb, in the Airbnb area, you might reach the temporary resident, and never the owner.

And also trying to get permission is one step higher than that. And so let's address the harms, as Greg put it, but not with proposals that impose so much of a burden that really you almost couldn't operate.

JAMIE HINE: So you think existing laws in local jurisdictions are too complex?

BRENDAN SCHULMAN: No. I think they work well. We've seen, as I said, a prosecution in New York State under existing unlawful surveillance laws, which are not specific to drones. They apply to anything you used to unlawfully surveil someone.

We've seen in various other jurisdictions, they have a different flavor. So maybe it's intrusion upon seclusion. Or it's sort of a anti-stalking or surveillance type of statute. And I think that does work well.

KARA KALVERT: The one issue, again, in the name of privacy, some locals are proposing legislation that would limit very specifically the use of drones, and limit how they're operated, when, how high, by whom. And that's actually when you start to get into a patchwork of laws and regulations that actually could not only hurt safety, but really and truly hurt the safety implications that the FAA is working so hard to ensure as drones are integrated into the air space.

So privacy and perceptions and whatever the problems are around privacy do need to be addressed. Whatever those questions are. But it's very important that we think about it in a way that again maximizes safety in the name of integration.

GREG MCNEIL: Yeah, so what's interesting, I think that we've observed for a long time now on this is how something starts, with a privacy implication type of thing. Oftentimes the way the legislation moves in the states, for a while it was moving where it was a concern about the police and what the police were doing with their drones. And then the police are very well organized. And so they come back and they say, well if you're going to limit our use of drones, then you need to limit other people's use of drones.

And then as the bill moves through, the police are very well organized. And the police part drops out. And then all you're left with is the bill about restricting the use of the commercial use, or the-- I'm sorry-- the civil use of unmanned aircraft.

I actually think the commercial recreational distinction is oftentimes a really difficult one to make. The person who flies an unmanned aircraft today to take pictures with his kids tomorrow does it for real estate photography. It's sort of like is that a recreational use of a hammer, or a commercial use of a hammer is not really a very useful I think distinction for us. But we start to see those types of issues coming up.

And then the privacy issue drives into safety issues, as Kara mentioned, either undermining some safety rules, making them confusing, or making the local officials believe they need to take some action about some things related to safety. And then we start to get into all these questions about airspace, which are still somewhat undefined for us, it's easy at 500 feet to say that local authorities shouldn't say anything about that. I think it's actually very hard to say what local authorities can say about two feet above a sidewalk, or two feet adjacent to your third-floor window-- even if not camera equipped.

And so if I strip the privacy part out, and I strip the nuisance part out, and let's take a non-drone example. You live on the sixth floor of an apartment building. You have a balcony. You have a great view of the ocean. The guy on the seventh floor is wanting to make America great again. And he hangs a Donald Trump mannequin in front of your window blocking your view.

Whose air space is that? And who do you call? I don't know. Everybody's having nightmares. It's not Halloween yet. Sorry. One guy's not having nightmares. Keep going buddy.

So that once I take the mannequin off the string, and the mannequin is now just a hovering Donald Trump drone, like has our analysis changed at all? Or are the harms that that person experiences there separate and apart from the privacy, something that probably needs to be addressed? And then the question is by whom. And I think that's going back to these first principles of addressing the harm. And I just really wanted to use a Donald Trump analogy, and so there it is.

JERAMIE SCOTT: I think nuisance law might take care of that one, personally.

GREG MCNEIL: So I think, Jeramie, that's a good first impression, right? That nuisance law might do it. Or privacy law, or Peeping Tom laws.

But a lot of these laws are tied to is there a noise? So a lot of nuisance law is about noise measured in decibels. That's how it is in many municipal law sort of contexts. Or the Peeping Tom laws are oftentimes about whether or not a person trespassed to gather the image, which then brings us back to I get what a trespass is if I step on the land. But if I'm a millimeter above the land, have I trespassed? These are some areas where I think having a little bit of harmony in the state law approaches might help us to resolve some of these issues.

KATIE WHITE: Is there a way short of regulations that the government can help incentivize companies to adopt strong privacy sort of protections in their products?

GREG MCNEIL: Threaten to do something, but don't actually do it, which compels industry to act. But then once it falls apart, we've sort of acted, solved the problem, and now we don't have to deal with prescriptive regulations. That's I'm being very serious. I'm just being a little too blunt.

BRENDAN SCHULMAN: I actually think we're doing it on our own. We put in GPS-based geofencing over three years ago. No one asked us to do that. So we've got protection for airports. We added prisons, nuclear power plants.

We added temporary flight restrictions, the DOI wildfire information from their system. Nobody asked us to do that. We've got a height limitation. We've got automatic return to home on the battery, so it doesn't just fall out of the sky. It comes back and lands itself.

I do think that even in the absence of a regulatory push or a threat, these things will be solved by us. We have an interest in good community relations, and having the technology be welcome by everyone, and used by everyone. So it may be helpful, but I think not necessary to have that push.

GREG MCNEIL: You left out sense and avoid, too, and the advances there.

BRENDAN SCHULMAN: Thank you, Greg. The new Phantom 4 has computer vision-based sense and avoid. If you fly it towards a wall or a person it will stop and hover instead of colliding.

KARA KALVERT: As manufactures I think our incentives align, in the idea that we want people and consumers, educators, commercial operation, we want everybody to be comfortable with these types of devices. And so our incentive is there to make sure that you implement and use the same type of technology to help them be comfortable, not only flying that, but having it flown above them. So our incentive is there. I think that's often why, as manufacturers, we're pushing the limits on what we can do with technology-- how small we can make it, how robust we can make it, and how we can address some of these concerns, and actually solve for the problems, not perceptions.

JERAMIE SCOTT: I'm somewhat skeptical, obviously. Although maybe the fact that kind of drones are a kind of topic that has some staying power in terms of the public's attention span on it, maybe it will be the kind of impetus to the industry to kind of address the privacy issues. But I also think we may end up in a situation where they address some of them, the ones they feel like they need to, but maybe others kind of fall to the wayside that don't get as much attention from the public.

And it's kind of why I like, at minimal, transparency I think really helps with this issue. Because it informs the public of what's going on. And then in turn the public can put pressure on industry to make the changes necessary to respect their privacy as the public sees it.

And one of the kind of things I'm looking at in the future, and something I think we'll have to struggle with, not just with drones, but drones I think may push this forward more than other technology, is just the idea of mass public surveillance. So we see this with license plate readers. We've kind of integrated into many, many cities without the public's kind of understanding or knowledge of it until after the fact. And we have to start struggling with what kind of level of privacy do we want in public. How do we integrate these new technologies in a way that kind of respects that, where it allows them to do kind of the things that would be useful for not just companies, but the public also?

JAMIE HINE: So last call for questions, if there are any questions for the panelists, I'm going to wrap up in a few minutes.

KATIE WHITE: That's it. We're taking up one question for Jeramie. It says, do you and EPIC believe that people have a reasonable expectation of privacy when they are in a public space?

JERAMIE SCOTT: Yeah, absolutely. Now it's not an absolute expectation of privacy. Your picture can be taken. But where we really see that kind of come to the forefront in terms of the expectation of privacy is with the kind of mass surveillance, and mass collection of information in public. So it's one thing for an individual to take your picture, or you happen to be in the background someone taking a picture of something. It's another thing where there's a mass aggregation of information in which information around you is in a database, and can be tracked, and we can aggregate that information in terms of where you were at, and figure out what you were doing, and things of that nature. So that's kind of the difference, is when we start getting into that mass aggregation of data, we have to start thinking, OK, about the privacy implications of that. And that applies in the public space.

BRENDAN SCHULMAN: So I agree. But we have case law on those things-- photography in a public space, and also the tracking surveillance. The one thing you didn't mention in your answer was the word drone. So yes, let's address the surveillance issue, that people being followed even in public, without regard to what you're using to conduct that potentially misconduct offensive conduct.

JERAMIE SCOTT: Well, my suggestion is that drones might push this forward in a way that they may need to be addressed specifically. But I would be completely open and happy to have a law that was, say, technology agnostic, and address the mass collection of information in public [INAUDIBLE] technology.

JAMIE HINE: So we have come to the end of the first panel. Are there any closing thoughts? Anybody? We have a minute.

Actually we'll end early. We'll take that [INAUDIBLE].

So please join me in a round of applause for our first panel. Thank you Greg, Jeramie, Brendan, and Kara. So at this time, we are headed into a break. And we have a 20-minute break. So please be back just around 3:00 o'clock.

KATIE WHITE: Thank you so much.