FTC Fall Technology Series: Drones
October 13, 2016
Segment 2
Transcript

JAMIE HINE: Welcome back, everybody. Our second presentation of the day is from Professor Yang Wang, from the School of Information Studies at Syracuse University. Professor Wang will discuss his research on consumer perceptions of drones. I'll turn the floor over to you.

YANG WANG: All right,

JAMIE HINE: Thank you very much.

YANG WANG: Thank you, Jamie, for the introduction. And hi, everybody. My name is Yang Wang. I'm from the School of Information Studies at Syracuse. We just heard a great panel sort of touching on the issues of privacy in the context of drones. And I'm very pleased to share some of our empirical research on this topic.

So most of what I will talk about today is based on a paper we published early this year at Privacy Enhancing Technologies. I showed up the paper info there. It's available online, so if you google it, you should be able to find it. This is a joint work with my colleagues, Huichuan Xia, Yaxing Yao and Yun Huang. We are all from Syracuse University.

I would also like to thank DJI, their generous drone donations for this research. This research was also supported by an internal research grant from Syracuse University, and also a great supporter from my school.

OK. So there are a few takeaways from my talk. The first one is consumers, they do raise many different privacy concerns, which I'll describe later. And they also identify key differences between drones from other tracking and recording technologies. For example, camera phones and CCTV.

We also did a study on drone controllers, so these are people who actually own or have operated drones. They have quite different views on the privacy issues on drones. Overall, they feel that the privacy issues on drones are mostly exaggerated.

And then lastly, we discovered a sense of distrust between the drone bystanders. So these are people who have never used drones, but they could be present when someone else is flying a drone. And I believe that this lack of trust between bystanders and controllers is really a key challenge moving forward in terms of privacy protection for drones.

Our empirical research started with interviews. So we interviewed ordinary citizens. These are people who have never had experience with drones. We did 60 interviews in the area of Syracuse. This was done last summer. You see that there's a picture of a DJI Phantom 2 that was one of the donations from DJI. Last year, it was, I guess, a popular model on the consumer market.

So in these interviews, we first show these interviewees this model, this physical drone. And we flew the drone. We showed them the live video feed from the drone camera. This is a way to give them kind of a better taste of what a drone will look like, because most of them didn't have any experience with drones.

These interviewees have pretty wide age range and backgrounds. Overall, these interviewees have mixed feelings about drones. They identify many potential benefits and innovative applications about drones which we have heard in the last panel. For example, using drones in crisis response scenarios. But they also raised a number of safety, security and privacy concerns. And for the remainder of my talk, I'm going to focus on the privacy aspect.

When they talk about privacy, I really want to highlight three things. One is the way they talk about public versus private space. And they also raised concern about peeking, stalking. The drone can be used to record people's lives, and then who knows what's going to happen with these recordings.

All right, so first off, public versus private space. So in these interviews, we provided detailed drone usage scenarios. So for example, there's a scenario where you're going to a mall with a friend. And the mall owners will fly a drone and take pictures and videos of people shopping in the mall.

And then we asked the interviewees, under this scenario, imagine you were there, do you accept this drone usage or not? And one major factor people considered is this question, whether the drone is operating in a public versus a private space. However, their definitions of what counts as public versus private space differ significantly.

So overall, there were three factors that surfaced from people's reasoning. The first one is ownership. This has to do with who owns that space. Like, for example, if you're talking about someone's house, of course, that's private space, because they own it, right?

The second factor is the sensitivity of the space. So one example is schools. Many participants consider schools as private space because they're children.

And the third factor, which is perhaps the most interesting one, is the nature of activity in the space. So here I have a quote from one participant, and you can read it. Basically, this person was saying that he would consider a public space only when he's in a public area, plus he's conducting some public event, some public activity.

In another scenario-- the shopping mall scenario I told you-- some participants actually believe shopping malls are private spaces if they are shopping with a close friend. So the interesting part is that the nature of the space is characterized by the social relationship within it. So the fact that this person is shopping with a close friend, that close personal relationship signifies the space to be a private space, and they reject the drone usage.

And I would also note that this kind of social definition of public space seems to be not covered by the regulations. And I think that could potentially be a point for conflict.

Moving on, people are also concerned about that drones can be used for peeking and stalking. And we heard some concern from the earlier panel. The first quote basically was saying that they're concerned that the drones could fly near somebody's window, and peek through the window, and see what people are doing within their house.

The second quote, I guess, is slightly more negative. This participant was saying, there are some very emotionally unstable individuals out there. So to have everybody able to own a drone, and that I could have some crazy person watching me, yeah, that's a problem. So this speaks to, I think, early on again in the panel, the fact that drones are getting cheaper. It's widely available, so you really don't know who's behind these drones. And so people have these concerns.

Because drones have cameras and other sensors, they have capabilities for recording. So people are concerned about drones can capture them. In this first quote, this participant is saying that people can't tell it's there. And they would not be aware that they were being watched by such a tiny drone. And the footage by a drone may be used for whatever purposes without their consent or knowledge.

So again, this speaks to the fact that the drones might not be visible to the drone bystanders. And the controllers-- we talk about the [INAUDIBLE] of the controllers. People might not see where the controllers are.

And the second quote is basically saying that if I don't know who's the controller, I want to make sure that the person who controls the drone is someone who is reliable or it's someone I know. But how do you know that controller is someone who's reliable? These are some of the sources why people have these concerns.

I think, in particular, the second quote alludes to this concept which I call the duality of drones. So imagine that you're out in a public park and somebody is flying a drone. You're not only dealing with the physical drones. You're also indirectly dealing with the people who's behind the drone. So that's the duality of drones.

And I think this quote is particularly telling. This participant said, "You wouldn't like to know who's behind this?" And I think this is kind of an important point to raise because people fear what they don't know. So if they don't know who's steering it, that raises some concerns. So again, this goes back to the hidden controllers. We need to know who are the people behind this.

Most of our interviewees have no experience with drones. So to help us to gauge their perception of drones, sort of unfamiliar technologies, we asked them to compare drones with other particularly-- technologies they're already familiar with.

We asked them to compare drones with camera phones. Everybody, I guess, knows camera phones. And here, there is one example quote which the participant said, "It would be a lot further away with a drone, and they are hidden away but still get a really good shot. So I feel like there's that kind of not knowing this is happening, as opposed to a cell phone, where you get a much larger chance of seeing that person taking the photo of you.

So what this means in practice is that, let's say somebody is using their camera phone to take a picture of you. It's pretty likely you'll be able to spot that person, and then you can walk to the person and say, hey, are you taking a picture with me? Or can you please delete it? I mean, at least that's a plausible-- that's a practical thing that you could do, as a privacy-enhancing mechanism.

But this mechanism might not be easy to achieve if you're-- in the context of drones, because again, drones are small. They can identify them. The controllers are hidden. They can't really approach them. So that's one of the key differences between these two technologies.

Another technology we asked them to compare with is CCTV, because again, people are pretty familiar with this tracking and recording technology. And one obvious difference is that a CCTV camera is fixed in one location. They don't move. Drones fly around. They can go into various places.

But the other more interesting difference is the fact that drones can fly into people's space, whereas CCTV is kind of-- they're sitting there, waiting for people to come to be monitored. So I think this quote really tells a good story of this concern.

"A security camera is put in a place where it's very visible." Again, so visibility is the key. "Usually, a place will post some sort of sign that says there is a security camera. And so there is that disclosure that you understand if you step into that space, you're going to be recorded. But I think a drone has the ability to enter someone's space, rather than the person going into a space, and then not having that disclosure that they're being monitored or recorded."

So again, there is this idea that the drone actively flies into people's space. Also, what's alluded to here is the lack of disclosure about the presence of drones, but also the purpose of the drone usage.

So I would just quickly summarize the major issues faced by consumers with regard to drones. First, it's not easy that they can identify drones, whether there is a drone present in their-- nearby, because they're small. They're flying high in the air.

And related to that, it might be more difficult for them to even identify or approach controllers to see what they're doing. Even if they can identify the drones, there's really no easy way of telling what the drone is doing. So is the drone recording? Am I being captured in the recording, and how the recording will be used. They really have no idea about that. And really, there is really no easy way for the consumers or the bystanders to opt out of a drone recording.

So to mitigate these concerns, these consumers talked about their expected notice and consent from the drone controllers. They say that they would hope that the drone controllers would notify them if there are nearby drones. And they would expect explicit permissions from the drone controllers if the drone controllers want to take pictures or videos that would capture them, especially if the recording captured their face, and they wanted to post these online.

In a later study with drone controllers, we did find that posting these drone recordings online is a common practice. So the drone user student, they do do this.

So, so far, I've talked about just briefly what bystanders or general citizens think about drones. And now I want to briefly switch to the drone controllers. We did a follow-up study interviewing drone users. So these are people who either own or have operated drones.

Overall, not surprisingly, they have a much more positive view on drones. They love the technology. They have great fun with it. They see many, many potential innovative applications. They also reported that safety is their highest priority when they're operating drones, which is a good thing, right? It's understandable.

But they believe the privacy issues of drones are exaggerated. And this is in part because they feel like the general public's perception of drones were misguided by the popular press media's coverage of either controversial or problematic drone use-- a drone crashing in the White House, where somebody shoots down a drone over their backyard. So these public media really frame or misguide the public's perception about drones.

They also reported that they do use their common sense to operate drones. They do this properly. They're being reasonable. But they also said they know that other drone controllers, not themselves, do crazy things. They will fly their drone over schools, over prisons, over other people's houses, and they really hate that. They feel like these other drone controllers really spoil the public image of drone controllers as a whole.

We did a follow-up survey study. We surveyed hundreds of both drone bystanders and controllers. And this graph basically shows there's a big discrepancy in terms of how these two groups perceive the same technology.

So the blue bars represent the controllers. So you see that over about 80% of controller respondents in our study view drones as very positive. Compare this with about 40% of the bystanders holding a positive view. And again, it's very obvious that there is a big discrepancy in how they view this technology.

I don't have time. I see the clock is ticking. I don't have time to go into the detailed results of this drone controller study. But here, I show you some of the interesting and representative quotes from our drone controller participants. The first quote is basically saying that hey, forget it, you have no privacy expectation in public space.

And second, they believe that even though they might not be a professional photographer, they believe that they have constitutional rights to do essentially whatever they want with drones as long as they're in a public space. However, remember early on, I talked about different definitions of public space? For the controllers, their view is that they used ownership criteria. So who owns this? If it's owned by the public, then that's a public space, and then they can do whatever they want.

And the third quote is perhaps even more debatable. This participant said, if you don't want your indoor interactivity to be reviewed because there is a drone outside of your window, I'm sorry, you just have to put a curtain down. I'm not sure how most citizens will feel about this.

And lastly, just very, very briefly, we did another follow-up study on how bystanders and controllers would perceive different privacy-enhancing mechanisms for drones. So these mechanisms include, for example, the drone owner registration required by FAA, face blurring, no fly zone, geofencing, a number of mechanisms.

Overall, what we found is this level of distrust between the two groups. So for the bystanders-- you know, most of the mechanisms are voluntary, except for the owner registration required by FAA. So the bystanders, they just doubt. They doubt the controllers would adopt these voluntary practices. NTIA released a best practices document. They just doubt people would actually adopt these.

From the controllers' side, they also have some distrust about the bystanders. They believe that some of these mechanisms will be abused by the bystanders so that essentially that will curb their capabilities to fly their drones. So we see that. There is a big gap in terms of their trust.

When we ask the respondents to evaluate individual mechanisms, the top two mechanisms that are accepted by both groups are the owner registration. Again, it's required. People feel like there is an institution behind it, so that helped the accountability of the controllers. So they liked it.

They also really liked the face blurring mechanism. So what it is, is once you have the drone recording, you can automatically identify people's faces and blur it. This is a technology that has already been implemented in the Google Street View, which we heard about in the first panel.

And lastly, when we give them specific drone usage scenarios, they told us they want multiple mechanisms. Not a single one, because multiple mechanisms would cover different aspects of privacy.

So I think my time is up. I will stop here and thank you for your attention. And we'll keep doing follow-up studies. And if you're interested, I'll be happy to chat offline. Thank you.

[APPLAUSE]

JAMIE HINE: Thank you. That was perfect. Thank you so much, Mr Wang. So I know that he alluded to several different studies. One of the studies is available on the event website. It was submitted as a comment. I know some of the other pieces are in pre-publication and should become public sometime final. You can also check out the professor's website, and there are links to the materials there.

So I'd like to ask the panelists for our second panel to please step up to the desk. It's a little bit cozier this time. Kristine, are you OK on the end there? Good. [CHUCKLES]

DIANA COOPER: We're a tight-knit industry, as you can see.

JAMIE HINE: Yes, yes, intimate conversation forthcoming. So let's introduce the second panel, addressing the question of how should privacy concerns raised by drones be addressed? The panel features, to Kate's left, Margot Kaminski, assistant professor of law, Moritz College of Law, the Ohio State University. To Margot's left, Dr. Jeremy Gillula, senior staff technologist at the Electronic Frontier Foundation.

On Jeremy's left, Diana Cooper, vice president of legal and policy affairs at PrecisionHawk. And to Diana's left, Mark Aitken, director of government relations at AUVSI. To Mark's left, Michael Drobac, representing the Small UAV Coalition and Akin Gump Strauss Hauer and Feld. And to Michael's left-- last, but certainly not least-- Kristine Gloria, privacy research fellow at the Startup Policy Lab.

So in the interest of fairness, we provided the panelists on the first panel to react to the first presentation by Otek. And I'd like to make that opportunity available to anyone here on the panel.

DIANA COOPER: Sure, I'd like to start.

JAMIE HINE: Of course.

DIANA COOPER: There were a few quotes that were put up on the screen that were quite inflammatory, and I think not well representative of the drone industry-- the hobbyist or the commercial side. I think most people would know that they are not exercising their First Amendment rights when they're engaging in aerial photography. So I think it's important not to take one-off comments and extrapolate those into an entire industry that's quite diverse and mature and responsible.

JAMIE HINE: Thank you, Diana. Michael.

MICHAEL DROBAC: So I just have to say that, one, I want to thank you both. So Jamie and Kate, you've both been extremely accessible and have been wonderful to work with on this. And so I appreciate the time you've given to, at least, I know to me with my concerns around the research.

And I think the main thing that we've talked about as a community-- I think that Greg McNeal did a very good job of addressing it, which is, you're really looking at unsophisticated toys, and that was really what the research was. And it does a great disservice to this industry, largely because they also didn't discuss the innumerable technologies and countermeasures that can be applied, the platforms that can help to protect from any kind of device tampering, from any kind of technology that can be utilized in a way that would-- for the device to be used in a way it wasn't intended.

So to me, again, I think it was said on the last panel, but it's important to really emphasize this, is that this discussion is at a much higher level now than that research would indicate. And I hope that going forward, if there is research-- because when I got the call about the research studies, I

was looking forward to constructive research that would help the industry to move forward, and that wasn't it.

JAMIE HINE: Margot, please.

MARGOT KAMINSKI: So I just wanted to add, actually, positive feedback to the presentation, which I found fascinating. So thank you. One of the things that was most interesting to me about it was the conversation we did not hear in the discussion of drone exceptionalism on the first panel about the presence of the operator.

So I know that Professor McNeal had raised the presence of the operator or remoteness of the operator from a perspective of being concerned over tracking. One of the things that seemed to come up in the presentation we just saw was an awareness of the lack of availability of the operator with respect to being able to socially sanction the behavior. So if somebody is standing in front of you with a cell phone, taking a picture of something you don't want them to take a picture of, you can stare at them until they feel uncomfortable and walk away. But if somebody is hovering their drone, to use a massively overused example, over a person who is sunbathing, then it's harder to socially shame them away from that kind of behavior.

JAMIE HINE: Is there anyone else?

JEREMY GILLULA: I just wanted to add to that. I think it's also important that the difference really seems to be for me that with the drone, you can't tell what it's looking at. If I'm standing on the ground, I don't know if it's targeting me, or the guy-- the person operating it-- is actually just interested in something else.

Whereas, if I'm looking at a person on the street with a cell phone camera, or even a security camera, I can see what it's targeting. And so I can see that, oh, as I walk along, they're not constantly looking at me with their cell phone cam. I just happened to be in the frame. And I think that's another important thing to understand why people sometimes have this sort of privacy fear of drones. It's because you can't-- there's no way to understand the intention of the operator currently.

JAMIE HINE: OK. I think that's it. So we thank everyone, and let's shift into our second panel.

KATE WHITE: Sorry. So thinking about the concerns that consumers have started to raise, like they're a little wary about some of the technologies, because they're not sure who's operating it. They're not sure whether it's collecting it, who's collecting information about them, what information they're collecting. And so they have these concerns.

And so the question we want to really talk about now is, how can we address these concerns? And so, I think my first question is, actually, are there any places where attempts to address these concerns have started to pop up? Are there any jurisdictions where they're making attempts? And what do those consist of? And how are they working? And Kristine, if you'd like to start for us.

KRISTINE GLORIA: Yeah, let me-- is that on? OK. So a little bit of background on what we've done is that we've actually been working with the City of San Francisco to figure out their municipal drone policy. And in that, I guess you could say that we have, in some cases, some of these questions and answers pretty much laid out because we know who will be in charge of the recording. It would be the city and its departments. And we should know the uses in which they want to use these drones, and we should be able to formulate the harms and potential risks.

With this project, we found this to be actually very difficult, to have the departments come to us with use cases in which they could give us enough detail in both the data collection and their use. Most of it was fairly broad. It was just we'd like all the data possible, all the collected data raw. And we said, well, OK, we would like a little bit more detail into that.

And then also, in deciding, well, how do we tell the public exactly what we're going to do with the drone data that we're collecting? And here we had some recommendations of using preexisting information architectures, like the city's 311 and San Francisco's Open Data Portal to give some sort of transparency and ability for the public to have access to this data. And what I'm trying to point out is here that, while we are working with a government entity, I think some of these questions-- this is a really good use case of how these questions can be really difficult department by department.

And we originally had started with almost all the departments of the City of San Francisco. Towards the end of the project, we now have five, excluding the law enforcement, because it became a really difficult task. There was not enough expertise and bodies and manpower for each department to come up with what we needed them to really consider in terms of the entire selection from the drone, to the data collection, to the processing, to the retention. All these questions required a lot more operational and processing expertise that city governments didn't have.

So from a local level, there are questions that are popping up. And from our work, we've had other municipalities engage us on these discussions. And we do have-- this is an internal use of drones, and not necessarily going after, well, how do we go after-- how do we regulate consumers, and hobbyists, and things like that?

So I just I do want to point that out, that that is the distinction on the work that we're doing. But it is certainly a good use case of how difficult it is for departments to go through this discussion, even when we can walk them through the points.

MICHAEL DROBAC: So to answer the question more broadly-- I think that was an excellent description of one area. But to say where it's happening, in jurisdictions where it's happening, I'd point to the United States after the presidential memorandum in February of last year, when it convened a multistakeholder process for the community to come together and come up with industry self-regulation.

And Kara Calvert reasonably pointed out the fact that online advertising, in the way that the description that was used by the gentleman from Epic about how consumers hate it, well, they're not disabling cookies. And there's a bunch of issues there that the FTC knows very well. But she

referenced how the DAA, Digital Advertising Alliance, has been making a lot of progress in their self-regulation related to online behavior advertising and advertising, generally.

So the NTIA stakeholder process was a very successful one in which industry came together and outlined a whole series of things that would be the expectations for those who are using the UAS, both commercially and recreationally. So I would say this. In terms if you want to look to a jurisdiction where there's been a considerable amount of effort and time spent toward a process of identifying the issues, identifying how good stewards of the technology will work, look no further than the Department of Commerce and the NTIA, based on a presidential recommendation that we come up with standards.

So I think the US is probably leading in the privacy standards. And I'd also add one thing, which is the inefficacy of the FAA to come up with the commercial rule that was nine months late. And the lack of clarity about what's to be had in terms of the technology and where we're going with this industry has created also some of the problem itself. But industry didn't wait for the rule. In fact, industry came across with this consensus, a [INAUDIBLE] graph. So I'd say that there's a really good outline and platform for us to work from.

JAMIE HINE: Margot.

MARGOT KAMINSKI: Yeah.

JAMIE HINE: Jeremy, if we can come back. Margot, I understand you've written about the NTIA and its multistakeholder process. And so--

MARGOT KAMINSKI: Yeah. So I've also written about a different area where drone privacy policy is happening, which is on the state levels. There are various states around the country that have enacted drone privacy laws, both in the context of law enforcement and in the context of private actors. These, when they're dealing with private actors, range from the absurd to the potentially mildly useful. So, for example, Texas has a law that says that you cannot use a drone to take a picture of a person or of private property and then lists around 25 exceptions that are all very specifically carved out for the particular industries who were there at the table when they negotiated the law. Wisconsin has a slightly better one, but anyway.

With respect to the NTIA process, I just wanted to flag that there were a number of consumer protection groups-- I think, Electronic Frontier Foundation, Access, and the ACLU-- that all expressed serious concerns about the actual substantive outcome of that process.

In large part, just some background, a number of these groups did not participate in the process until very late in the game, because they experienced great frustration over negotiating at the NTIA during the facial recognition negotiating process, which resulted in a consumer protection walkout.

And if when you look at the actual substance of the NTIA best practices, I think you can read them either way. There's certainly restrictions or suggestions about informing people about use

of drones, restricting your collection practices, restricting your sharing practices, and making sure that you have good security practices in place.

On the other hand, nearly every single one of these suggested best practices has some sort of exception, including when you're using drones for a compelling purpose, or when you are using drones for the purpose for which they are being used, or in compliance with FAA guidelines, which suggests that FAA guidelines are the privacy baseline, as opposed to privacy best practices. So there are multiple ways of reading these. I also think it would be just interesting to see whether they, in fact, get adopted by industry.

JAMIE HINE: Jeremy, I-- you were going to [INAUDIBLE].

JEREMY GILLULA: Sure thing. So I just wanted to second what Margot was saying. EFF, more or less, did not participate in the NTIA process, because although I personally wasn't involved in it, we had found these sort of processes basically useless, particularly in the facial recognition example.

But I wanted to jump back to something that Mike said that, while I agree about the FAA lagging behind on rules, I sure hope no one up here is thinking that the online advertising industry is a good example of self-regulation. People do block cookies all the time. I'm probably the only person on this panel from an organization that works, as well as drones, on online software, online tracking and advertising. And we actually put out a product explicitly to help people protect their privacy online, because people are fed up with being tracked online.

So I would say that industry self-regulation definitely isn't working there, given that we've got people who are basically saying, we don't want it anymore. So I just don't think it's a good example. That's neither here nor there, with respect to drones.

DIANA COOPER: I'll just jump in. I want to respond to one of Margot's comments on the NTIA process. So although we didn't have every public interest group like EFF join onto the principles, we did have the Center for Democracy & Technology, and then groups like FPF, and then larger groups like CTIA, AUVSI Small UAV Coalition. So we had very broad support for the document.

And I think there are quite a few members and companies that are actually doing things to incorporate the principles. I can speak for our company, PrecisionHawk. We've implemented high-level privacy guidelines into our operator manual. So anytime someone purchases one of our drones, they open up the operator manual. They see their instructions. They also see some guidelines in terms of privacy in there.

So I do think you're going to see industry commitment and uptake from a lot of the members that have signed on. And hopefully, that will spread across the industry.

MARK AITKEN: Yeah. So from an industry perspective, and kind of echoing my colleagues up here, I mean, you had a process through the NTIA multistakeholder initiated form there which, in

reality, that was an eight-month process. Eight months, right? And you have the ability for folks to come into the room, at whatever point, to interject their comments on this.

And whenever you have the likes of AUVSI, the Center for Democracy & Technology, and FPF standing shoulder to shoulder behind a document at the end, it's something that I think, as an industry, we should be proud of and being embracing. I mean, we are actually getting ahead, I think, of any of these potential concerns, or as I should use the president's words in his memorandum, "potential implications," right? Because we're talking about what perhaps might be out there as an implication for privacy.

And I think, as an industry, we should be commended for coming forward and putting forward voluntary best practices which, especially with new entrants into this-- especially from the commercial side, this is a framework for guidance. We're not saying it's the be all, end all. But we're saying that, as you come forward within the commercial environment, there are some things out there that you need to be considering whenever it comes to privacy policies.

But at the same time, as you-- looking at some of the other supporters of this document-- Amazon, Intel, PrecisionHawk, specific companies that have broader privacy and data policies in place-- by no means are we saying that this NTIA voluntary best practices should trump that, because they're already handling bigger issues whenever it comes to broader data collection.

And I just kind of-- I would point out in terms of industry adoption of these, again, we're doing our best effort to educate people about this. You can go on the AUVSI website right now, and you'll see that it's front and center on this. We joined with the Center for Democracy & Technology and did a joint op-ed actually saluting the effort that was put into this from industry and civil liberties groups. So I think that we're already going the extra mile right now to really educate people about what it is, as an industry, we're trying to be mindful of.

MARGOT KAMINSKI: I just had two short responses to Diana. The first is that it's very encouraging that you are intending to adopt the practices or have adopted them.

One of the concerns about the best practices as a basis for any kind of policy movement forward is that it doesn't capture what will happen with smaller bad actors, right? So if you're a larger company, and there are potential pressures on you from consumers to behave as a good actor, then you might be more likely to adopt best practices. If you're a smaller company, or you're a less permanent company, those kinds of pressures aren't necessarily there.

The second point is that this, again, did not get raised in the first panel when we were talking about drones and technological exceptionalism. There is a particular type of privacy problem with drones that escapes the model-- my apologies-- with which the FTC operates. And a colleague, or friend of mine, has referred to this-- Meg Jones at Georgetown-- as the "Internet of Other People's Things problem."

When your governing the privacy issues online, you are largely governing an interaction between the supplier of a product and the person who's consuming that product. When you're governing drones and privacy, you are governing an interaction between the consumer of your product and

a third party. So even if you have drone manufacturers who adopt the best possible privacy practices with respect to their sale of that technology to an individual, that doesn't mitigate some of the privacy concerns of that individual's then use of the drone upon their environment.

JAMIE HINE: So just to go back to this issue, one of the issues on the first panel was this idea of identifying the harms. And a criticism that I've read about the NTIA process was that it was a solution in search of a problem. And so this idea that, was it appropriate at this point to develop the series of best practices? Or go back. Have we defined the harms that the best practices should be addressing if, in fact, those best practices is an effective self-regulatory effort to avert potential regulation?

MARK AITKEN: So I'll just step in here and say, I mean, if the President of the United States is directing this, obviously, they're trying to get ahead of something. And I think that's been the resounding message that we've heard from certain groups. It's we're trying to get ahead of the game.

So I would submit that again, given the open process that the NTIA had through its multistakeholder agreements to actually come out with a consensus best standards. I don't think that it was premature at all. I mean, if anything, it's out there. And it's, again, guidance. And there's something to be said there with it being voluntary and not mandatory.

I would also submit too that, as commercial stakeholders really start coming into the mix of using this technology, there's an economic incentive there for them to have these best practices already in place. To think that someone is going to go out there-- let's use insurance, for instance. I mean, the FAA doesn't mandate liability insurance. But you could submit that as a commercial operator that's going to want to be respected across the community and its industry, they're most likely going to carry their own insurance, even though it's not mandated.

So again, with the nascent industry, which I think is becoming a little bit more than just nascent, given the number of commercial operators out there, I think we're starting to see the industry coalesce around these standards, especially within the commercial community, that other types of businesses already have their place that are just adopting it. Because at the end of the day, a drone is a business tool, and it's an evolution of the tools that businesses have at their disposal. So I think for us, the NTIA best practices is definitely a tool for someone to look at and use for guidance.

MICHAEL DROBAC: So-- may I?

JAMIE HINE: Please.

MICHAEL DROBAC: So I would say that one of the things that I heard that disappoints me, and I think it's unfortunate, is that in the NTIA process, a number of consumer groups either didn't come or came at the end to oppose. Based on previous bad experiences with NTIA, that's too bad, because I think there was an opportunity to have a real thoughtful discussion. So to some extent, I'd say that that's on them for not coming, because there was a very good discussion.

The other thing is, to say that this is premature, the 2012 FAA Reauthorization put very clearly what was going to happen in terms of commercial use and made very clear that it would be a prohibition on the FAA problem getting rules related to recreational use. And so the idea that this is new and that we're talking about this in advance of the industry, in fact, it's not new at all. We're talking about something that's been in the offing for a decade. We have millions, potentially, of recreational vehicles in use currently, and I have a number of them which I love.

So the idea that we're talking about something that is going to be very scary. And there's going to be a lot of invasions. And I recognize that's a pretty easy one to talk about, which is easier to say, be careful, because your privacy is going to be invaded.

It's harder to say that, in fact, these vehicles have been on the market for quite some time. People have been using them. And what we're doing is we're seeing a pedestrian unsophisticated model from the demos about how this technology can be manipulated.

What we're not seeing is the real life examples, at least not as prevalently as many would suggest. I think what we're seeing is, there's a lot of excitement around this. And I think the reality is there's going to be immeasurable and ubiquitous use of this technology across every industry and for entertainment purposes, which does mean that beginning a discussion around self-regulation, beginning a discussion around standards that industry should be looking at.

And Congress already mandated in the FAA Reauthorization or Extension this year that there should be a two-year investigation into how you do remote identification of vehicles, which was a discussion on the last panel. So how can we decide which vehicle is where?

Beyond what Gregory McNeal is doing with AirMap, you have a company called Airways, which is coming up with different ways for vehicles to immediately be taken from one airspace which is maybe restricted to non-restricted.

They have alerts that are coming up, where they can alert local law enforcement as to where vehicles are, who the vehicle's owners are. So there's not only identification of the operator, but also the vehicle, and where the vehicle is. All of the same technology that you all demonstrated in terms of how these vehicles can be manipulated, can also be used in terms of identifying the operators, identifying where this vehicle is.

And my question is, why aren't more of the consumer groups that didn't show up to the NTIA process saying, technology can be used in the other way? And the reason, partly, that it hasn't been is because this industry, based on the FAA's attempt to become more knowledgeable before they move forward with rules, what we have is the officials that are supposed to be regulating this don't understand it.

And so the reality is, what they're trying to do is get a sense of what's going to be necessary. And technology is going faster than it will ever go, which is not just in terms of the creation of problems, that people can stand up and say, the technology is bad. The reality is, the very technology that concerns us is the very technology that will also be able to protect us.

JAMIE HINE: So we had an early question from the audience, and it sort of does dovetail with this discussion of NTIA. So it says, "Industries rallied behind the NTIA document. Why don't responsible members of industry make irresponsible operators fall in line by making NTIA something binding as a matter of state and federal law?"

DIANA COOPER: As my colleagues on the earlier panel and this one alluded to, it's not like there's a gap of laws in place to deal with drones. We already have strong frameworks in terms of criminal laws, tort laws, trespass nuisance, intrusion upon seclusion. So I don't think that there's this vacuum that requires specific legislation dealing with the harms or perceived harms associated with drones, specifically. Nor do I think that drones should be treated differently than other technologies that raise similar concerns.

And I think if regulators start to regulate individual technologies, as opposed to the uses of any type of technology that can create the same harm, then we're really going down a wrong path. And you'll never be able to keep up with the technology in terms of drafting rules.

And you've already seen companies like DJI implement fantastic safety measures that regulators didn't even think about. That wasn't imposed on these companies, but everyone's really doing their part to try to create a safe space for people to operate in.

MARGOT KAMINSKI: Look, the problem with the continued criticism of technology-specific regulation with drones is that we don't have adequate privacy law with respect to almost any of the technologies that you keep referring to-- you, not being specifically you, Diana.

The other thing I take issue with is this idea that there aren't gaps in the laws. As Greg mentioned on the last panel, when you talk about some of the state laws that get raised when we talk about drone privacy violations, they end up, when you look in the devil's in the details, not being able to apply to drones for various reasons.

One example that Greg raised was that when you talk about various peeping Tom laws, there's often a trespass requirement. There's the question of whether aerial trespass is trespass within the understanding of that statute. There are also often requirements that involve peeping in through physical windows. And there's a question of whether if you are remotely peeping in through the window using a zoom technology, you are in fact peeping into the window under state laws.

So I just wanted to take a moment to debunk both the conversation around drones are just like cell phone cameras, and so we don't need drone-specific regulation. We just need regulation, period, and also, to push back a little bit on this idea that there aren't legal vacuums here.

MICHAEL DROBAC: I mean, the question, though, for the panel, I think, does get into this idea of, so we were saying they're not similar to mobile devices. They're not similar to desktop devices. They're not similar to cookies and the portfolios we create on individuals. All of that sounds like, OK, I accept it.

But then the question becomes, is there anything unique about UAS technology? And one is that it's in the airspace. And so, we then get into a question of the state and local regulation, where it becomes really a viable question as to, is it established yet who has jurisdiction here?

And I think we're suggesting that we're going to do something with San Francisco. So how does that impact Atherton? How does it impact Palo Alto? Because the reality is that I don't think it's necessarily-- I don't think anyone, even if they're on the consumer side of the fence or on the industry side, is going to say that we don't have an interesting juxtaposition here, where you have communities that are very close. And we can't have disparate treatment of the same technology when they'll be spanning the border there.

I think the reality becomes-- and this is one where I do think there is a question here-- is what jurisdiction does the FAA have, and is it exclusive? And if so, then how do we handle that? It's clear within the FAA Extension. When they're saying, begin to identify how we can do remote identification of vehicles, they are looking at this because that was privacy-related.

MARK AITKEN: Yeah, I mean, I guess I would look at this from a perspective of, what is it that-- I mean, just because we're inside of the FTC here, I mean, what is it that the FTC is trying to get at with this? I mean, as you look at the FAA, the FAA was very adamant in the fact that drones are considered aircraft whenever it comes to regulation because of the way that they're congressionally defined.

So I guess, in order to have a more constructive conversation on this, it would be helpful to, I think, understand perhaps where the FTC and other agencies that think that they have jurisdiction in this come out. Would Section 5 of the FTC Act-- would that not cover any sort of privacy implications or concerns that-- from a commercial operator's perspective, with their privacy policy, would the FTC not have the authority to come in under that enforcement action under Section 5? Would they need to go further than what was in the NTIA best practices?

Again, this is just kind of posing the question the other way around. But as we're having a constructive dialogue, I think especially with other government agencies and departments, this is what's needed.

KATE WHITE: So the FTC, we've always put out guidance for wide-- across industries about privacy. And I think one of the things we'd like to talk to this panel about is that we put out guidance. In the past, some of our guidance has been to employ notice and choice for consumers whenever possible. Is it possible to employ notice and choice with drones? And if so, how? And if not, why not?

MICHAEL DROBAC: I'm happy to tackle from the beginning, but I'd love to have Diana's thoughts as well, largely because one of the areas we're going to-- and I think it was referenced that this is still nascent, and I think, countering my previous argument that's been around for a long time, it's nascent to the extent that we're not seeing ubiquity across every industry yet.

And yet, to do that, we're going to have to have the right command and control, communications systems in place. Do you need dedicated bands of spectrum for certain communication? Do you

need a license for others? That's a big question. And a lot of it is centered around what's happening at NASA with PK and NASA's leadership on an Unmanned Traffic Management system.

In a commercial context, certainly, one of the things we're talking about is, can you do sense and avoid technology? Is there geofencing that can be utilized, such that you can actually have this at scale, and do so safely? And that's going to depend on a very sophisticated Unmanned Traffic Management system that may in fact have registries of where these vehicles are flying, at what times, and by whom.

So I'll let Diana go into it more, but this is not something where industry and any willing consumer groups that will attend couldn't be a part of a discussion at NASA with PK around an Unmanned Traffic Management system.

DIANA COOPER: Sure. Prior to the discussion on UTM, I'll just mention that I am aware of operators that actually do provide notice and choice. I know of certain operators that have done videography over construction over strip mall-like sites that are partially built.

There might be a restaurant on the other end of the parking lot. They go to the restaurant on the other side that's in operation. They ask the owner to post signs. They post signs around the property with the time of their operation, the name of the company, and contact information.

So I think there are things that you can do in certain contexts to provide notice and some level of choice, as well as transparency and accountability. And I do think just raising awareness of these possibilities will help in terms of adoption.

JAMIE HINE: So do you think that's an effective model? I mean, that's an isolated incident, and that works well. But is that a model for commercial operators? Is it a realistic one?

MARGOT KAMINSKI: I mean, it depends on the scope and type of your operation. If you're talking about commercial operations generically, not a lot of them actually take place in places where there are private individuals. For example, our company does services for a lot of Fortune 500 clients, operating in oil and gas, agriculture. In those types of operations, generally, there's no one that's present in the area of interest. So I think there's a misconception that there always is a privacy interest in a specific operation. Often there isn't when you're talking about commercial operations.

JAMIE HINE: So, I mean, just to sort of push on that, let's talk about what-- if consumers are thinking about a consumer use, they're probably thinking about package delivery. Let's just say that a company figures out how to deliver whatever you want at any time by drone. And it's going to traverse through your neighborhood, and it's potentially going to collect images, because it doesn't want to run into a tree, or a neighbor's house. And there may be different types of information it's collecting along the way. Is that a realistic use situation for providing notice? And how would one do that?

MICHAEL DROBAC: So I think the question itself is probably not entirely right, which is, that's not the foremost consumer use, which is delivery. I wouldn't subscribe to that. That's the most titillating use.

JAMIE HINE: I'm just positing an example that I think if you ask consumers about a potential future use, I think one of the responses would be something will be delivered. A drone will be doing delivery.

MICHAEL DROBAC: Right. And that's largely-- but I mean, as we know, and again, I'm not an anti-media person, but much of this discussion is driven about the close calls with the airports, which oftentimes turn out to be plastic bags, or something unrelated to the drone industry altogether. Or they tend to be delivery, and how close are we to delivery?

And there's always this kind of description of this as being sci-fi. And the reality is, is it a realistic approach? And again, this gets back to an Unmanned Traffic Management system. There is going to have to be infrastructure in place, such that we can ensure that these vehicles are able to fly in a way that is consistent and reasonable for consumers. And that does entail a discussion.

And I think a conclusion of the discussion is, who's got jurisdiction over the airspace? That one's going to-- that discussion, in many people's minds, has already been established. And Brendan Schulman in front of me, can go into some description about his work on this, and I think, remarkable work, in many respects.

But the other part is that, absolutely, you're going to have a system in place where you have to have a system where vehicles are able to know where other vehicles are going to be. Vehicles can communicate with each other. Vehicles can communicate with the ground. That this is not something where a vehicle that is making a delivery won't have a system by which it's working through and with. And it won't solely be a privacy policy.

But this concept that we're going to have vehicles that are-- where the privacy policy will be the entirety of what is necessary, I mean, it seems to me that that could be an acceptable response to this, because it's how we work in so many different capacities in life now.

But I think the interesting part of this is industry has never said that it's not willing to explore, as did the FAA Reauthorization, the ability for identification of the vehicles and reasonable restrictions on the amount of data that's collected, for how long it's kept. But the concept that you can't have cameras, and cameras-- there's a technology also to prohibit certain cameras from taking certain photos in certain areas. I mean, all this technology exists. The concept, though, that we can't have these technologies working together in a way where you're going to be able to protect individuals and allow these operations is just absurd.

MARK AITKEN: Well, and I just want to add to that, which I think was brought up on the last panel. I think that this really comes down to public perception. And it's a matter of getting those good news stories out there for people to understand. And I have two specific examples of this.

So again, from the White House itself, I mean, the White House held its first ever drone event to talk about some of those good use cases across the federal government. Specifically, I think that it would behoove everyone to look at the work that NOAA is doing with drones. I mean, especially coming off of the horrible hurricane down South, Hurricane Matthew. Look at the work that NOAA is doing, which is flying their drones to gather information about hurricanes-- simple data weather data out there.

As opposed to flying a P-3, a manned aircraft with a crew of 5 to 10 people on board, they're able to fly a drone remotely and actually get the long endurance and the data that's needed in a much more timely real time fashion, in order to better educate emergency management scenarios.

Second to that, I think really the public is going to start to understand the benefits of this technology with the news themselves, right? You have the news gatherers out there that are going to be able to use this to get that real time information and the images for local news stories that they wouldn't have at their disposal unless having a helicopter.

And then you're starting to look at, again, just the safety of flying a helicopter, and the cost and the maintenance to operate a helicopter. So I think as we start seeing really these use cases coming forward, I think the transition across public opinion is going to transition as well.

MARGOT KAMINSKI: So-- sorry, Jeremy first.

JEREMY GILLULA: So I actually agree that getting news out about positive uses would do a lot to help improve public perception. I feel like there will still be scenarios where people will see the drone, and even though they know that, oh, NOAA does these wonderful things with hurricanes, I don't know what that drone is doing.

So a question I want to pose to the folks from industry on the panel is, what if we took one of the security flaws that was in the first presentation of the day and actually made it a feature, where if I see a drone, and the owner is OK with it, I could just bring up an app on my phone, and I could see what the drone is seeing? So that I could say, oh look, he's not actually targeting me. It's just flying by. Or obviously, that thing is looking at real estate pictures, doing real estate photography.

And of course, this would be an optional thing. Not everyone is going to want their drone video to be broadcast. But I feel like this would be one way that people could get--

MICHAEL DROBAC: Would you be able to strip search me too, or come up and frisk me if you thought maybe-- I mean, the reality is, do you see what you're saying about--

JEREMY GILLULA: No, I'm saying it's a voluntary thing, that if you want to promote people saying-- if I'm a commercial operator, and I want to promote that, hey look, I've got nothing to hide here, I'm just doing my commercial job.

MARGOT KAMINSKI: The potential problem with that model is that it doesn't take into account privacy interests of third parties. So coming back again to the issue of there are the people who are being observed who don't have any kind of connection to the drone. The person who is filming things, like filming real estate, might be totally OK with letting another person look in on the feed. But the people who are being filmed might still see some sort of privacy violation.

JEREMY GILLULA: And so I guess the question is, by being able to see what the drone is filming, do those people get--

MARGOT KAMINSKI: That reintroduces the shaming.

JEREMY GILLULA: Well, it reintroduces the shaming, or if I can see what the drone is seeing, and I don't have a-- and I have a problem with it, then do I have some way of getting out of the frame, or something like that? Do I get more knowledge and the ability to make a choice by knowing what they're going to do with it.

MICHAEL DROBAC: It sounds like you're actually violating the very thing you think you're protecting, which is-- what you're saying is that if I give you access voluntarily to whatever my camera is seeing on my vehicle, and what my family is seeing is my entire extended family in my backyard, and someone is somewhat in another yard, then I'm saying, yes, you can have access to that. And then everyone in my family and everyone that's visiting my house would then be being viewed by a third party.

JEREMY GILLULA: So I guess the question is, why should I trust you, if that's what you're taking the footage of over a third party?

MICHAEL DROBAC: Hey, look, the reality is, first of all, I don't think the issue is why you should trust me. I think what I'm failing to understand is this concept of the reasonable expectations of privacy, where you're suggesting that you believe-- and these stories that I found, even the gentleman from Epic, when he was on a boat. And the drone was following him.

I mean, some of these are just-- they're wonderful. I've never had a drone follow me, but the reality is, why should you trust me versus the third party? It's not about whether you should trust me or the third party. It's about the fact that we're not going to set up a system that allows for a violation of someone's expectations of privacy.

You're saying that the drone does. And therefore, that's why there's a process that took place at NTIA, which many of you didn't attend, to address how do you cover this information? How do you dispose of it? How do you-- how is it collected? When is it not collected? That's where we had that whole process.

Now those who didn't attend, I can understand why they don't know what was discussed. But the reality is--

JEREMY GILLULA: So I did observe the process. I know what was discussed.

MICHAEL DROBAC: You did. Not you. I said those. But I'm saying that people who have a problem with this, the answer isn't to expand it to allow other people to get access to the person's camera data, or to what the-- I mean, that to me, even if you had that app available, what you're saying is that everyone would then be able to access whatever images are on the drone. That actually seems to be a deterioration of privacy.

DIANA COOPER: I mean, one of the problems that I have with that model, besides not respecting the privacy of the operator, is if you're an operator that chooses not to share your feed, then is there some sort of implication that you're engaging in wrongdoing just because you want to protect your own privacy? I mean, how would you address that?

JEREMY GILLULA: So I don't see what this has to do with the privacy of the operator. I'm not saying that you even necessarily need to show who the operator is. I'm just saying you show what the drone is seeing. So unless the operator is doing it to film themselves, in which case, I think it'll probably be pretty clear. Here I am. I'm a guy with a drone, and there's the drone looking at me.

DIANA COOPER: But now you're talking about getting the data from the feed. You've got a registration that potentially gives you a lot of details about the operator. We're talking about big data of the people that are being watched, potentially. What about the big data collected about the operator?

JEREMY GILLULA: No, I still don't see what you're talking about, because--

MARGOT KAMINSKI: Can I intervene to return to the initial question about notice and choice? Everybody's OK with that? So the hypothetical, Jamie, that you proposed about drones and delivery, taking it solely as a hypothetical and not as something that's actually one of the foreseeables soon to come use cases, does highlight a lot of the notice and choice problems.

So first, you have a more traditional consumer relationship between the person who has ordered the package and the company that is doing the delivery, right? Because that's the kind of thing where you could have-- you probably do have-- a EULA, an End User License Agreement, and a contract between the person who ordered the object and the company that's doing the delivery. So that's no problem. That person can have notice.

The issue is when you deal with, again, all the third parties who are in the physical environment that the drone is following through-- is flying through. And when that drone flies through that physical environment, there's a question of what constitutes adequate notice of the information that it's gathering.

And when you look at a number of state privacy laws, there is a conversation over notice versus surreptitious. So it may be the case that the person who's walking in the street and sees the drone knows in some way they're being subject to surveillance, right? It's not surreptitious surveillance.

But the question is whether they're given adequate notice about the type of surveillance they're being subjected to and where that information is then going to be shared. And that, I think, is an

extraordinarily difficult problem. It's very hard to tell people who are walking in the street under the drone that the drone is collecting thermal imaging information in order to figure out what their energy uses are in their houses.

KATE WHITE: So if notice and choice is difficult, should there be rules around collection of data by drones? Or should there be rules around the use of data collected by drones?

MARK AITKEN: So I would argue, why does it matter if it's collected by a drone or something else? I mean, data is data, and how you collect it-- there shouldn't be a distinction between the tool that you are collecting that data from. So to single out drones over some other technology out there, I think it would be a disservice for the entire privacy conversation as a whole, quite frankly.

MICHAEL DROBAC: I mean, and the other interesting point about this is that, again, talking about notice and choice and the idea that I think it's right there are EULAS, and there is going to be disclosures to consumers. But there's another issue that gets back to one of my earlier points about who's got jurisdiction here? Because FedEx and UPS and USPS, they're going on public roads to get to consumers to deliver packages. And we're fine with that, even though they may be passing my house and looking at me and seeing whatever they may see.

Then there's another question, like how far up is this vehicle? Supreme Court jurisdiction is beginning to demonstrate that, in fact, the airspace is maintained for the public, and that you don't have a private right in certain areas within your own private property with airspace.

And so there's a question here as to whether we're actually talking about just simply the notice and choice and the collection of data, or whether we're having a larger discussion about what is-- how the FTC or any government agency views this technology, in particular. Because again, there's no question but that other technologies are far more invasive in terms of a person's expectations of privacy in the portfolios and the knowledge that can be developed on a person than a drone. And yet--

JAMIE HINE: What are some of those technologies? I mean, and what are the similar issues?

MICHAEL DROBAC: So we talked about it before, and I think the point was made when I brought up this industry self-regulation on advertising. We were saying that that was a complete failure, and that nobody likes it, and people don't like be tracked. And the reality is, I don't have really an opinion on whether people like it or don't like it or whether it's helping to function.

JAMIE HINE: So Mark, I want to challenge you on that.

MICHAEL DROBAC: Yeah, good.

JAMIE HINE: So I go to a website. Let's go to my-- I go to a news site. And I'm there, and that first party drops a cookie, says, this user has come here. And at the same time, 120 other cookies are dropped by a bunch of third parties that are working on behalf of that company, or are simply being paid or allowed to drop a cookie, collect information about what you do across the web.

Why is-- what is unique or different? I, as a consumer, am going to the news site. I may know that--

MICHAEL DROBAC: What's unique or different between that and drones?

JAMIE HINE: Yeah, what is the difference between them?

MICHAEL DROBAC: So I would say that the amount of information, theoretically, in your example, where there's 180 cookies being dropped, or however many, which is fairly extreme, but I'll go there, is that the amount of information that you can glean from my activity on a website, or across various websites over time, provided that I'm not a good steward, and I'm not using ad blocking technology, or disabling cookies, or removing my cache, that information is far more of a statement about how I live and what I do than whatever can be captured by a drone in a rare instance.

So the reality is, is it possible for a drone to catch a picture of me through a window where I'm not clothed? Yeah, theoretically, it's possible. Is it possible for my entire history online to be captured, my loc-- I mean, look at the Uber app which I love. It not only knows my credit card information. It knows where I am and where I'm going.

The reality is, do you think there's a difference between that and a snapshot of a photo or data that's collected by a drone? I do. I think that the kind of dossiers, the kind of profiles that could be collected through different technologies are far more insidious than what we're talking about here.

But the focus here isn't because of the actual technology. It's because it's titillating. To say that drones somehow represent a unique threat is much more interesting than to address the things that the government hasn't done a thing about for decades. And I hope it doesn't, because what we're seeing is a continuation of development of technology and innovation that is providing consumers with easier use of services such as Uber, such as Airbnb, such as what drones are going to provide across every sector of the economy.

The problem is that you have to actually have this discussion. And I appreciate it, but you're having a discussion where you're actually having to defend why your technology is less invasive than another one which, in fact, has provided massive benefits to the society. So I'm having to throw another technology under the bus to protect a technology that's far less invasive?

This is the problem is that all of the technologies that are referenced in terms of cookies that are tracking websites. I mean, the reality is-- and the consumer groups, it's a difficult one, because to actually employ a system where you're tracking who's tracking you and not tracking you, you've got to drop a cookie.

So the reality is that there's-- and when you talk about working with cities and having them be the help on the data issue, the biggest breaches of data have happened by the federal government or by state and local governments. So the reality is, if we want to have a thoughtful discussion

about this, you start with the fact that the government has been the biggest problem in terms of the release of consumer data.

How many letters do I get indicating that every single cover position I had in the past, I'm breached. They have my social security number. They have all my information, because the government released it. And yet, private industry is being called to respond to this issue that every single new technology that consumers love is creating some expectation, or it's diminishing our privacy. When the fact is, the government is doing it more so than anything.

So any project around San Francisco, I'm worried about San Francisco having my data. I'm worried about the federal government having the data. I can't control that. But the reality is that to have this discussion about whether one technology is more invasive than the other-- I think it is, no question. But I also think it's leading to more innovation, which is always a positive thing.

MARGOT KAMINSKI: So it's just-- sorry, very quick response to that. We're back to the technology-specific versus technology neutral regulation question. And we're back to this argument that drones are not different from other kinds of technology, and therefore, we should regulate them in the same way. Which fails to acknowledge that, in large part, we don't regulate technologies for privacy protection in the United States-- apologies to the FTC-- in really particularly effective ways.

So all that's arguing for is a significantly lower ceiling, as opposed to-- and I think there are actually great reasons, and to say this publicly, for not regulating on a tech-specific basis, because you do have overlapping problems in different areas. But what's happening right now is that you are having zero regulation in most of these places, as opposed to effective regulation of anyone.

MICHAEL DROBAC: I completely subscribe to those views, which is that there is a problem, which is there have not been very many thoughtful actors addressing the general technology environment. And it doesn't just address the fact that we have existing technology where there hasn't even been an assessment of it.

But we also have a lot of privacy laws on the books that are outdated. They were a part of the world when we had Blockbusters. And so they're still looking at things that are completely anachronistic to how we live.

Having a comprehensive look at this in a thoughtful discussion about technology generally is fine. Isolating one technology and saying that it somehow is uniquely invasive of a consumer's privacy, yeah, it's not true. And the reality is that there is. It's ripe for a discussion, though, about technology regulation and a consideration of, how do we move forward?

MARGOT KAMINSKI: So one way to tie this technology-specific conversation back into the question, which was about data collection versus sharing and use, is that one way in which, again, drones are different from your behavioral advertising online, is that the collection takes place in a physical environment and involves third parties who clearly have not consented to that collection.

So that suggests that there is some sort of governance space there around collection that as long as you agree with me that there are governance gaps with a lot of the imagined use cases for drone privacy violations, collection is a place where some sort of governance is probably necessary.

MICHAEL DROBAC: So are we suggesting that, in fact, drones are the only ones that can collect data on third parties?

KATE WHITE: No, absolutely not. And in fact, taking it for the moment as totally technology neutral, my more general question is, when we're talking as we go forward-- and a lot of these technologies raise the same questions besides just drones, but I'm interested in how you think about this question, which is, should there be rules surrounding the collection of personal data, whether it be in direct relationships or passively in technologies that have the ability to maybe passively collect some information from people? Or should the rules be focused on use of data, and if anyone has any thoughts on that.

MARGOT KAMINSKI: I mean, I can say, at the NTIA negotiations, most of the focus, at least from the industry proposals that were put on the table, were on use, as opposed to on collection. The final product, which did incorporate a number of those CDT-proposed best practices, did have suggestions that there be restrictions on collection. But when you looked at the negotiating process, it looked as though the primary industry focus was, let's forget about the collection problem and talk primarily about use and sharing.

DIANA COOPER: I think we need to break apart the collection problem. If you're talking about an area where you're collecting data where there clearly is a reasonable expectation of privacy versus in public space, which is generally where most hobbyists and commercial operators might be operating in, if there's no reasonable expectation of privacy, as determined by courts in those public spaces when you're collecting data about people or their images or videos of them by any other means, should there now be that type of restriction just because you're using a drone to do the same thing?

JAMIE HINE: So we have a question. I just want to throw this in as well, and it may take us in a different direction. But the question-- and I'm going to paraphrase it-- says, how would this whole notice idea apply to drone journalism by, say, television networks? And then there are several examples, riots, Thanksgiving Day parades, floodings. And would regulations on these be constitutional? So--

MARGOT KAMINSKI: This is an extraordinarily thorny issue. I've spent around four years trying to sort it out. The, I think, key takeaways are, one, there's clearly some sort of First Amendment protection for a right to record what exactly the scope of that protection is is currently being litigated in the courts of appeals around the country.

Two, just because there is a First Amendment protection for rights to record does not mean that it obviates all privacy interests. And journalists and news gatherers who are not professional journalists can still be subject to privacy torts. And so how that applies to the notice issue, which

on the one hand, is a disclosure which might be permissible, on the other hand, it could be considered compelled speech is an extraordinarily thorny question. That's the academic's answer.

JAMIE HINE: If someone else wants to--

MICHAEL DROBAC: I mean, I'll just say that as part of the NTIA process, there was a clear carveout for the First Amendment. And I think, while it's thorny, yes, the concept of a journalist or a news gatherer is moving as well.

We live in an era where the platforms for the dissemination of information and for news no longer fit neatly into this concept of journalism. And so-- and I hate to create even more thorns, I guess, but the reality is that the First Amendment, I think, on this topic is going to be absolutely impacted and will maintain. It will be strong, because the reality is that you're using a technology which makes possible something that was not possible in the past.

It's happening all over the world, not here as much, because of what I consider to be relatively youthful regulation we have here. But I do think that we'll see the use of UAS for news gathering ubiquitously. And I think the reality is that the First Amendment will protect it.

JAMIE HINE: So Kristine-- unless, Diana, you wanted to--

DIANA COOPER: Jamie, yeah, you asked, how do you give notice in something-- in a case like a riot? I think, riots in general, people know that the media tends to show up and videotape what they're doing. Sometimes they hope that they will do that. So I don't know that that's necessarily one of the cases where people wouldn't expect that kind of activity to be going on in the area. So we also need to be careful not to impose unnecessarily restrictive barriers on legitimate commercial activity that people are generally aware and quite OK with.

MARK AITKEN: And I think it's also just worth taking a moment here to actually applaud the news gathering industry, because I know there are specific members of it that actually go above and beyond, especially whenever it comes to the safety side. So, I mean, they are taking the extra precautions out there, just recognizing that they're-- while it's another tool in their tool box, they want to make sure that everyone is comfortable with it. So again, I think that they should be applauded for not only their engagement in the NTIA process, which was definitely critical in getting that document to where it was, but also, just its utilization of the technology, I think, to just further enhance that public perception.

JAMIE HINE: So Kristine, I wanted to pivot to you. We've had some discussion about these issues of notice and choice, or potentially an alternative framework that we might use for a particular technology, or more generally for technologies that engage in similar ways. And I'm wondering if you can add some perspective to this. And obviously, working with the City of San Francisco, I imagine that you've grappled with some of these issues.

KRISTINE GLORIA: Right. And so I appreciate the overall discussion that we've been having. And when we look at local, particularly municipalities, again, like I mentioned, resources are

scarce. And so we look to guidance from state, from the federal level, in order to help inform what we have.

And so when we consider, again, data collection, data use, we're not-- these conversations came up because we understand the implications across a technology neutral kind of way. But because drones are inevitably going to be part of how the city plans on addressing emergency use cases and for different departments, there needed to be a proactive discussion about, well, where do we need to have limitations on collection and use?

And I think that's at least a starting point. And from our progress, we've not gotten to a consensus, per se, about what that might be, even between departments, let alone the city in and of itself. And I'm not-- and I don't think that it's going specifically after the drone technology. But it certainly is in part because we understand we can now use this data to also be combined with other things through other departments. So there needs to be some understanding there in terms of how and whether there needs to be limitations.

And also, because it's in a unique position that it is a government entity, the trust between the citizen and the government, again, needs to be carefully addressed, right? Because right now, we attempt to do this by being as transparent as possible with our decisions on collection and decisions on use. But whether or not that is sufficient for a citizen is yet to-- is the next part of where the project needs to go.

But I think I don't-- in trying to apply-- in trying to make this an applicable process for particularly government entities, it's been a challenge. And I don't think it's a bad challenge. I think it is a discussion that needs to be had, and it's difficult only because of resource limitations and operational limitations. So the more that the guidance can come from bigger entities in which we can then position within our own contacts would be certainly very helpful. But for the time being, it's still fairly limited on the municipal level.

JAMIE HINE: Jeremy, I know you know a lot about laws in California. Are there things that you're seeing there at the state level that are consistent with or contrary to what you're hearing is happening in San Francisco?

JEREMY GILLULA: So I should preface this that I'm not a lawyer. So when you say I know a lot about laws in California, I know a lot more about how a drone actually works than the laws. But to be honest, what we've seen in California are some pretty bad drone bills, to be honest. And I'm actually very thankful that the governor ended up not signing quite a few of them, because they did try to make carveouts, and they were very piecemeal. And I don't think they really-- they tried to solve some of the privacy problems, and I thought that, to be honest, they probably would have caused a lot more harm than good.

At the same time, the particular drone bills that we would have liked to see are the ones we're not talking about here, which do have to do with government use of drones, in particular, law enforcement use of drones. But we're not talking about that today, so that's all I'll say about that.

JAMIE HINE: So just a reminder, probably the last chance for any questions anyone may have. We're winding down. We have a few more minutes. Margot, can you talk about the concept of atmospheric notice?

MARGOT KAMINSKI: Oh, so we talked about this on the call prepping for this panel. It's an ill-developed concept. So in one of the FTC's guidance documents-- I want to say it was around facial recognition-- there were suggestions that were put forward about considering various use cases of facial recognition and trying to figure out some way within a particular environment to let people know what was going on surveillance-wise within that particular environment. By the way, when I say surveillance, it's a value neutral term, so I apologize to all of you who are offended by it.

But the idea would be that you create-- you recognize, again, that use cases are-- that privacy expectations tend to be specific to particular environments, like physical environments. And the kind of privacy violations that are happening when we're talking about drones or Internet of Things or home robots, et cetera, tend to be set in a physical environment. There might be some way to build in notice to a particular environment to understand how the surveillance changes behavior in that particular environment.

So that all sounds very vague. The way you would actually operationalize it, for example, would be to say, you walk into a store. You get notice that the entire time you are in the store, you are being recorded, right? Or, you actually think Diana's example earlier of you walk into this physical place. There are signs up that say, while you are in this physical place, you are being recorded. That gives you, as the person who's being observed, as the data subject, some ability to modify your behavior. And as long as we think that the modification of behavior is not itself a harm, that sort of notice may help mitigate some of the concerns that we've been talking about here,

MICHAEL DROBAC: The other thing I think that we have to begin to recognize is, certainly in the commercial context, you've got a lot of large companies that are interested in different use cases that are not only insured, but they're also going to be competing with each other around this concept of which company is going to be the best steward of this technology.

But the other thing that I think can be done through the government is that we have-- existing right now, both pilots and non-pilots are getting certified to use this technology. And I think having done the research on the test and having looked through it, I mean, you're looking through aviation information. It's incredibly robust, and it's not as clear as it could be. And these tests are, for many that are not as skilled at this, very difficult.

But one part of it should be a larger-- I think it should be an online test. I think it should be user friendly. I think it should include privacy notifications about what the expectations are. It can be part of the NTIA's result. But it also can be more robust in terms of how consumers can be good stewards, how companies can be good stewards of the information, because to operate commercially, you've got to get certified.

So there is a mechanism through the federal government where consumers and commercial users should be informed as to what the expectations are. And as those evolve over time, as technology becomes-- and then again, I referenced a company, Airways, and certainly, AirMap earlier, because they're developing incredible new technologies which will make some of these discussions unnecessary. But for the ones that are still necessary, let's address it. Let's have it be in the common place of ideas where people have to be aware of it to pass the exam to get certified.

KATE WHITE: So we have a question from the audience which I think is actually a great wrap-up, which is, "Going back to Commissioner Ohlhausen's citation of the Warren and Brandeis paper on the right to privacy, do you think we'll be OK with drones the same way that we're now OK with cameras?"

DIANA COOPER: I think so. I just think it's a matter of time. People always freak out when we have new technologies. When the automobile came out, people were used to horses and buggies. And they thought all these crazy accidents would happen, and they would be dangerous. People would have to stay home to protect themselves from cars. And now everybody is driving a car.

And you know what? Guess what, there are a lot of accidents, but not enough to say we should restrict that technology. And when things do go wrong, we've got insurance and other mechanisms to protect people.

MARK AITKEN: Yeah. I think one of the other things here-- and I actually wrote this down during her opening comments-- I mean, she was specific to say, talk about societal and non-governmental approaches. And I think that that's key for this industry, because we've seen how long it can take the government to act in a certain space specific to this technology, looking at it strictly from the safety side. And so I think that there is going to be just the societal evolution of this for that public acceptance, as with any sort of emergent technology that comes into their public life.

MICHAEL DROBAC: So I'll just say one thing, which is that we had a gentleman here from France who works for a company that's operating beyond visual line of sight over people at night and has been doing so for years. And his comment was that he looked at the US. And again, I was offended by it, of course. But he said he looked at the United States and found it somewhat interesting that we have such a negative perspective on this technology and that we are trying to find ways to regulate it, just heavily.

He said, it could be that France doesn't use these for military purposes and that the contrast and the conflict between those members who are pro-drones on the defense side, but anti-drones on the commercial and recreational side is crazy, which is, if they're not sophisticated enough to use domestically for commercial or recreational purposes, then why are you using them overseas for targeted missions where people's lives are at stake?

That's a separate conversation, but he just said that the reason the US is in an awkward position, he thought, was that people have a perception of these things being militarized, and that people have a perception of these things being used for things that aren't wonderful the way the French

people look at these. And he said, we've been using these for years, and we're using them in ways that are much more advanced than the United States. And people view this as being positive.

So to answer your question, will we get there? There's no question but that we're-- I mean, we're on our way right now. And we'll have these discussions, but we're absolutely going to get to a place where this is ubiquitous. We'll look back at this, and we'll say, we made some mistakes on this, or we should have done this.

But the reality is, once something is-- once technology becomes popular from consumers, once it makes people's lives easier, there's no stopping it, even if there are some things about it that you'd like to maybe adjust a little bit. But it's going to happen. And it's happening around us right now, which is why we're all here on the panel.

MARGOT KAMINSKI: So I think it's interesting to phrase the question as, assuming that everybody is OK with cameras, particularly when we have ongoing policy debates about what to do about non-consensual distribution of permitted pornography, a.k.a. revenge porn. I think that it's not that we become accustomed to particular technologies, but that we've become accustomed to particular environments, particular uses of technology, in particular, ownerships of spaces, to go back to the study that preceded our panel.

And just as another example, you could ask whether we're OK with technologies such as GPS tracking. You see what the US Supreme Court decided to do after a longstanding debate over the question of whether physical tracking of people in public spaces was in fact a violation of reasonable expectation of privacy. The plurality of the justices in US versus Jones decided that it was, in fact, a violation of reasonable expectations of privacy. So Warren and Brandeis, I think, would see a very different world than the time in which they were writing that article, but maybe not quite so different as that question poses.

JEREMY GILLULA: So I'm not-- I don't think we can know yet whether or not we're going to get to that point. I hope we do. And I think we have to, but I'm not yet convinced that there won't be some bumps along the way. It's sort of a pessimistic optimism, I guess you would say, that I think a lot will depend on, because it is still a nascent industry, how industry collects the data, how it uses the data.

And like I said, based on what I've heard up here, I'm hopeful. And I think we will get there eventually. But just knowing how the world works, I'm sure there will be some bumps along the way.

KRISTINE GLORIA: And I guess I can end it. And this is based on my dissertation research, not necessarily solely on the work we've been doing at Startup Policy Lab. But I do see this becoming pretty normative within the society. But into the point, as some of my research has shown, as long as it's benign in its impact of being intrusive, then more than likely, there will be no problem.

But again, it's part of the PR problem of detaching it from the weaponization that you mentioned earlier that seems to be the greater media coverage that we've been seeing. So based on

conversations in relation to just privacy in general, it seems from my research, the technology, as long as it's non-intrusive, benign, and it's convenient, the easier it will be to become more adoptable into the society.

JAMIE HINE: Great.

KATE WHITE: So thank you all for participating today. I think it's been a great conversation. We really appreciate you guys.

DIANA COOPER: Thank you.

[APPLAUSE]

JAMIE HINE: And with that, we want to thank everybody who participated, everybody who is in the audience, all the people who submitted questions, everybody on the webcast. This is the beginning of a conversation that will continue. We thank you all for being a part of it.

Two last things-- first, 30 days, we'll be accepting comments. Until Monday, November 14th, you'll be able to submit them at the event website on FTC.gov. And last but not least, in two or three days, this event will be archived and will be available for anyone who was unable to watch or anybody who wants to go back and watch it again.

So thank you again. Have a good evening. Take care.