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 it 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-6(a)4(][-1(.)-2(d-3(-6(X[I(T)-13(ech) 64houbl)-3(-6(t)-o(i)-2(n t)2( )-
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 was also supported by an internal research grant from Syracuse University, a supporter from my school.

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

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

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

Our empirical research started with interviews. So we interviewed ordinary citi people who have never had experience with drones. We did 60 interviews in t Syracuse. This was done last summer. You see that there's a picture of a DJI P one of the donations from DJI. Last year, it was, I guess, a popular model on t market.

So in these interviews, we first show these interviewees this model, this drone. And we is a photo
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 whether 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 peoplelic surf3 n g sf3 ereicd, T* (ow)210(e)4(dto rddtor peoplhis cenaire ofeasf f

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. nd sta /P <<

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 and you please delete it? I mean, at

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 public 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, such as 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.

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

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

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 about 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

referenced how the DAA, Digital Advertising Alliance, has been making a lot of progress in their selfregulati

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.

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 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 a

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 irre

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 one operators that have done videography over construction over strip malls -- 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 conception 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 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 data because it doesn't want to run into a tree, or a neighbor's house. And there may be different types

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 asked consumers about a potential

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 3( )-104 Tw T 0.01 Tw secud [1: St h m e-1(t)-6(s)-4(S)en-4(t)-(pu0('r)3(e)4t)-6(at)-1((ld20(y)17(s)-5(t)4 T-1(e)-10(al)-6((l)-1a

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

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

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

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.

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 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 t

4(6par)3(l)-nd(i)-2(n)-10(g)10( )]T2(nd of-1f((r)42( )]o0(r)u c(t)-2(t)4bou2d)4(t)ow-2(e)4(t)- d2(r

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-- 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 be the next part of where the project needs to go.

But I think I don't--

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

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 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 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, >s, pac 0 Tw -24.704 T8ae disceion of(nnc002 Tw 0nta)4(t)-2(w-1(t)-21kS 4(t)-2( )4(s)-1(, T* [(e)4(ve)TJ -0.003 Tc 0.003 Tw 14.o pa)4(r)3(t)-2(i10 hnouound ut)-2(o m)i19 0 P-0.

conversations in relation to just privacy in general, it seems from my research that 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.