PREPARED STATEMENT OF PROFESSOR MARGOT E. KAMINSKI

For the

COMMITTEE ON ENERGY AND COMMERCE OF THE U.S. HOUSE OF REPRESENTATIVES,

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

On

THE DISRUPTER SERIES: THE FAST-EVOLVING USES AND ECONOMIC IMPACTS OF DRONES

Margot E. Kaminski

Assistant Professor of Law

Moritz College of Law

The Ohio State University

November 19, 2015

Prepared Statement of Professor Margot E. Kaminski

Good morning Chairman Burgess, Ranking Member Schakowsky, and distinguished members of the subcommittee. Thank you very much for the opportunity to testify today on unmanned aircraft systems, or "drones."

I am a professor of law at the Ohio State University Moritz College of Law, and an affiliated fellow at the Information Society Project at Yale Law School. The views I am expressing here today are my own.

In my testimony today, I will focus on the impact of drones on privacy, which is a crucial aspect of consumer protection. For drones to be publicly accepted and fulfill their economic potential, citizens must be able to trust that their surveillance powers will not be abused.

Drones in Residential Areas

Drones will be used for a wide variety of economically and socially beneficial activities, ranging from infrastructure inspection to precision agriculture.[1] In the best scenarios, drones will reduce risks to human actors and enable important information gathering at a relatively low cost. But it is precisely these beneficial aspects of drones—that they enable low-cost, low-risk information gathering through a variety of technologies—that raise the specter of substantial privacy harms. While many uses of drones will have little to no impact on a human population, a wide variety of commercial applications will take place in residential environments, where citizens' expectations of privacy are at their highest.[2]

[1] Analysis of the First 1,000 Commercial UAS Exemptions, AUVSI, http://auvsilink.org/advocacy/Section333.html.
[2] Kyllo v. United States, 533 U.S. 27, 31 (2001)(citing Silverman v. United States, 365 U. S. 505, 511

AUVSI in its analysis of the first 1,000 Commercial UAS Exemptions granted by the Federal Aviation Administration observed that over half of the exemptions were granted for general aerial photography.[3] Real estate uses, which quintessentially impact residential areas, followed with 350 exemptions.[4] Uses that are less likely to impact residential privacy, by contrast, received fewer exemptions. Agricultural use accounted for 164 exemptions, with search and rescue and utility inspection each receiving under 100.[5] And to briefly flag another consumer protection issue for the Committee: insurance-related uses received 25 exemptions.[6]

Drone Privacy Harms

Drones raise privacy concerns on a spectrum with other technologies. Like smart phones, they make surveillance more pervasive by lower its cost and raising the rate of social adoption.[7] Like GPS, they make surveillance more readily persistent, able to follow individuals over long periods of time. Like helicopters, they enable surveillance from disruptive vantage points.

Drones raise privacy problems because of both what they carry, and where they carry it. Where a person used to be able to rely on a privacy fence, remote location, or building height to manage social accessibility, drones disrupt the use of the environmental management tactics we all rely on. These disruptions have real social costs. Not only may citizens fear drones—or even

---

(1961))(observing that the "very core" of privacy is "the right of a man to retreat into his own home").
[3] Analysis of the First 1,000 Commercial UAS Exemptions, AUVSI, http://auvsilink.org/advocacy/Section333.html.
[4] *Id*.
[5] *Id*.
[6] *Id*.
[7] *The number of drones expected to sell during the holidays is scaring the government*, Michal Addady, Fortune, http://fortune.com/2015/09/29/drones-holiday-sales/ (Sep. 29, 2015)(citing an FAA estimate of 1 million drone sales this winter). For a quick overview of consumer drone prices, see *the Best Drone you Can Buy Right Now*, Ben Popper, The Verge, http://www.theverge.com/2014/7/31/5954891/best-drone-you-can-buy(Sep. 23, 2015).

shoot them down[8]—but they will alter their behavior in ways that can be truly socially harmful. Surveillance causes conformity, and conformity has costs to both democracy and the economy.[9]

Not all technological changes should drive legislation. But where a technology significantly lowers the cost of committing a harm, lawmakers often and justifiably step in to raise costs again. We saw this in the early days of online file sharing, and we are seeing it today in state regulation of drones.

State Drone Privacy Laws

Multiple states have recently enacted privacy laws governing information gathering by drones operated by nongovernmental actors. These laws are often, but not always, technology-specific, addressing drones, but not other kinds of surveillance. For the purposes of this committee, it is crucial to note that these state laws govern the moment of actual surveillance, rather than imposing a data privacy regime to govern the information after it is collected. State drone privacy laws build on the tradition of state privacy torts, an area where states are well-accustomed to governing. These drone privacy laws fill perceived gaps between the tort of intrusion, which has often been interpreted to require isolation or complete withdrawal for privacy protection, and Peeping Tom laws, which often require actual physical trespass or peeping through a window. State drone laws, by contrast, can govern surveillance even where there is no trespass, and may be used to govern persistently intrusive surveillance when it is conducted outside the home.

[8] *Judge rules Kentucky man had the right to shoot down his neighbor's drone*, James Vincent, The Verge, http://www.theverge.com/2015/10/28/9625468/drone-slayer-kentucky-cleared-charges (Oct. 28 2015).
[9] Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 483–93 (2014).

The content of state drone privacy laws varies widely. Texas, for example, has taken the approach of widely banning drone surveillance of individuals or real property, but has carved out a long list of permitted exceptions.[10] The exceptions include carve-outs for real estate use and the inspection of oil pipelines, but interestingly not for newsgathering.[11]

Oregon, by contrast, took a trespass-based approach, hewing closely to real property rights.[12] The Oregon drone trespass law creates a private right of action for anybody who "owns or lawfully occupies real property" against a person conducting drone flight over that property. The drone must have been flown over the property on at least one previous occasion, and the property owner or occupant must have notified the drone operator that she did not wish the drone to be flown again.

California took a more technology-neutral approach, amending its paparazzi law to include surveillance by drone, to protect individuals from a "constructive invasion of privacy" where a technology is used to invade a space that otherwise could not have been reached without physical trespass.[13]

Wisconsin's approach to regulating drone surveillance delegates decision-making to its courts. Wisconsin has made it a misdemeanor to use a drone to "photograph, record, or otherwise observe another individual in a place or location where the individual has a reasonable expectation of privacy."[14] Courts will be responsible for interpreting what counts as a place

[10] H.R. 912, 83d Leg., Reg. Sess. § 423.003 (Tex. 2013)(making it illegal "to capture an image of an individual or privately owned real property in this state with the intent to conduct surveillance on the individual.").
[11] H.R. 912, 83d Leg., Reg. Sess. § 423.002 (Tex. 2013)(13),(18)(carving out exceptions for real estate and oil pipeline inspection).
[12] H.R. 2710, § 15, 77th Leg., Reg. Sess. (Or. 2013) (codified as amended by H.R. 2354, 78th Leg., Reg. Sess. (Or. 2015), at OR. REV. STAT. § 837.380 (2014)).
[13] See Assemb. 2306, 2013–2014 Reg. Sess. (Cal. 2014), available at http://leginfo.ca.gov/pub/13-14/bill/asm/ab_2301-2350/ab_2306_bill_20140930_chaptered.pdf; DL Cade, California Updates Invasion of Privacy Law to Ban the Use of Camera Drones, PETAPIXEL (Oct. 14, 2014), http://petapixel.com/2014/10/14/california-passes-law-banning-drones-protect-general-publics-privacy/.
[14] WIS. STAT. ANN. § 942.10 (West, Westlaw through 2015).

where a person has a reasonable expectation of privacy; but by targeting drone surveillance with no mention of property ownership, the Wisconsin legislature has signaled that protection is likely to span beyond the home.

Significant Countervailing First Amendment Interests

Privacy protection is crucially important, but governing drones also implicates important First Amendment interests. Drone journalism is a budding field.[15] Newsgatherers will be able to use drones to gather information about droughts, land management, and government actions, all information that enables democratic self-governance and raises First Amendment concerns.

A number of courts have recognized a First Amendment "right to record."[16] The scope of that right is still uncertain. Courts thus far have limited the right to record to matters of public concern, or actions by government officials, knowing that too broad of a recording right threatens a number of privacy laws.[17] It is against this backdrop that state drone privacy laws have been enacted. These laws will no doubt face First Amendment challenges, many of which will be appropriate. A law that allows real-estate photography but not newsgathering inappropriately targets some speakers, and favors others. The First Amendment does not permit that sort of favoritism.[18]

[15] See, e.g., http://www.dronejournalismlab.org/about.
[16] Glik v. Cunniffe, 655 F.3d 78, 83 (1st Cir. 2011) (finding that "the First Amendment protects the filming of government officials in public spaces"); Smith v. City of Cumming, 212 F.3d 1332, 1333 (11th Cir. 2000) (finding that the "First Amendment protects the right to gather information about what public officials do on public property, and specifically, a right to record matters of public interest"); ACLU v. Alvarez, 679 F.3d 583, 586-87 (7th Cir. 2012) cert. denied, 133 S. Ct. 651, 184 L. Ed. 2d 459 (U.S. 2012).
[17] *Id.*
[18] Sorrell v. IMS Health Inc., 131 S.Ct. 2653 (2011).

For this reason, I caution the federal government against enacting legislation governing information gathering by drones, by private actors.[19] Courts will need time to unravel the tension between state drone privacy laws and countervailing First Amendment interests. In the meantime, federal energy can better be turned towards the data privacy issues that drones and other new technologies raise.

What the Federal Government Can Do: Technology-Neutral Data Privacy Law

Drone surveillance implicates data privacy. The information gathered by drones will be stored, analyzed, and used for a wide variety of purposes. When used out of context, this information has the potential to be socially disruptive or even discriminatory.[20] State drone privacy laws do not attempt to govern this data. This is the place for federal action.

The information privacy harms raised by drones again sit on a spectrum with harms raised by other technologies. Drones surveillance shares features with online surveillance, in that information privacy harms will largely arise because of massive amounts of information being used out of context or in a discriminatory fashion.[21] Drone surveillance differs, however, from online surveillance, in that the surveillance subject often will not be the person who clicks through a user agreement. Like the Internet of Things, drones raise the question of how to govern information privacy when the surveillance subject has no relationship to the product manufacturer or service provider. However accurate or inaccurate our notions of consent are with

[19] Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CALIF. L. REV. CIRCUIT 57, 57–59 (2013).
[20] See *Big Data: Seizing Opportunities, Preserving Values: Interim Progress Report* (Feb. 1, 2015), https://www.whitehouse.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf.
[21] *Id*.

respect to interactions in digital space, they are not applicable when it comes to real-world surveillance by third parties.

Our current data privacy regime, based primarily on requiring companies to comply with their own privacy policies, is ill-equipped to address the issue of the Internet of Other Peoples' Things.[22] As the Federal Trade Commission has used the current regime to reach beyond privacy policies and target unfair data practices, it has faced significant challenges in court.[23] A federal data privacy regime based instead on the Fair Information Practice Principles (FIPPs) would protect the privacy of citizens who are not subject to user agreements, would bolster FTC authority in this area, and would provide a backdrop for encouraging industries to establish best practices even where they have few incentives based on consumer relationships.

I support and have been participating in the Department of Commerce's efforts, through the National Telecommunications Infrastructure Agency, to establish and recommend best practices governing drone use. In the absence of federal data privacy law, however, industry is unlikely to agree to meaningful protections. In the absence of meaningful privacy protections, drones will not get off the ground.

Thank you for your time and attention, and the opportunity to testify today. I would be pleased to answer your questions.

[22] Meg Leta Jones, *Privacy without Screens and the Internet of Other People's Things* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2614066.
[23] *Third Circuit rules in FTC v. Wyndham case*, https://www.ftc.gov/news-events/blogs/business-blog/2015/08/third-circuit-rules-ftc-v-wyndham-case.