64 STAN. L. REV. ONLINE 29
December 12, 2011

THE DRONE AS PRIVACY CATALYST

M. Ryan Calo*

Associated today with the theatre of war, the widespread domestic use of drones for surveillance seems inevitable. Existing privacy law will not stand in its way. It may be tempting to conclude on this basis that drones will further erode our individual and collective privacy. Yet the opposite may happen. Drones may help restore our mental model of a privacy violation. They could be just the visceral jolt society needs to drag privacy law into the twenty-first century.

Samuel Warren and Louis Brandeis knew what a privacy violation looked like: yellow journalists armed with newly developed "instantaneous photographs" splashing pictures of a respectable wedding on the pages of every newspaper.[1] Their influential 1890 article *The Right To Privacy* crystallized an image of technology-fueled excess, which the authors leveraged to jump-start privacy law in the United States.

But what do privacy violations look like today? They tend to be hard to visualize. Maybe somewhere, in some distant server farm, the government correlates two pieces of disparate information. Maybe one online advertiser you have never heard of merges with another to share email lists. Perhaps a shopper's purchase of an organic product increases the likelihood she is a Democrat just enough to cause her identity to be sold to a campaign. At most one can picture the occasional harmful outcome; its mechanism remains obscure.

It is hard to know exactly what role the inscrutability of privacy has played in the development of contemporary privacy law. But the law has clearly stalled. Tort recovery founders on the question of damages. Privacy statutes tend to respond to specific incidences or abuses: for instance, no provider of videos (broadly defined) may release customer rental history because journalists once managed to procure a list of the videos enjoyed by a Supreme Court nominee. And it must be possible for officers practically to glimpse the prover-

* Director for Privacy and Robotics, Stanford Law School's Center for Internet & Society.

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

Electronic copy available at: http://ssrn.com/abstract=2340753

bial "lady in her sauna" before the Fourth Amendment places serious limits on the deployment of surveillance technology.[2]

The development of American privacy law has been slow and uneven; the advancement of information technology has not. The result is a widening chasm between our collective and individual capacity to observe one another and the protections available to consumers and citizens under the law. We are only now, in 2011, revisiting The Electronic Communications Privacy Act, which controls the circumstances under which the government can intercept or access electronic communications such as emails. The Act was passed in 1986. At the time, lawmakers' kids were trading in their Walkman for a Discman. Al Gore had only just invented the Internet.[3]

Recent shifts in technology and attendant changes to business practices have not led to similar shifts in privacy law, at least not on the order of 1890. Computers, the Internet, RFID, GPS, biometrics, facial recognition—none of these developments has created the same sea change in privacy thinking. One might reasonably wonder whether we will ever have another Warren and Brandeis moment, whether *any* technology will dramatize the need to rethink the very nature of privacy law.

One good candidate is the drone. In routine use by today's military, these unmanned aircraft systems threaten to perfect the art of surveillance. Drones are capable of finding or following a specific person. They can fly patterns in search of suspicious activities or hover over a location in wait. Some are as small as birds or insects, others as big as blimps. In addition to high-resolution cameras and microphones, drones can be equipped with thermal imaging and the capacity to intercept wireless communications.

That drones will see widespread domestic use seems inevitable. They represent an efficient and cost-effective alternative to helicopters and airplanes. Police, firefighters, and geologists will—and do—use drones for surveillance and research. But drones will not be limited to government or scientific uses. The private sector has incentives to use drones as well. The media, in particular, could make widespread use of drones to cover unfolding police activity or traffic stories. Imagine what drones would do for the lucrative paparazzi industry, especially coupled with commercially available facial recognition technology.

You might think drones would already be ubiquitous. There are, however, Federal Aviation Administration restrictions on the use of unmanned aircraft systems, restrictions that date back several years. Some public agencies have petitioned for waiver. Customs and Border Protection uses drones to police our

2. *See* Kyllo v. United States, 533 U.S. 27, 38 (2001) ("The Agema Thermovision 210 might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath . . . .").

3. Then-Senator Albert Gore actually introduced a bill to study the Internet. *See* National Science Foundation Authorization Act for Fiscal Year 1987, Pub. L. No. 99-383, 100 Stat. 813, 816 (1986).

Electronic copy available at: http://ssrn.com/abstract=2340753

borders. Recently the state of Oklahoma asked the FAA for a blanket waiver of eighty miles of airspace. Going forward, waiver may not be necessary. The FAA faces increasing pressure to relax its restrictions and is considering rule-making to reexamine drone use in domestic airspace.[4]

Agency rules impede the use of drones for now; United States privacy law does not. There is very little in our privacy law that would prohibit the use of drones within our borders. Citizens do not generally enjoy a reasonable expectation of privacy in public, nor even in the portions of their property visible from a public vantage. In 1986, the Supreme Court found no search where local police flew over the defendant's backyard with a private plane.[5] A few years later, the Court admitted evidence spotted by an officer in a helicopter looking through two missing roof panels in a greenhouse.[6] Neither the Constitution nor common law appears to prohibit police or the media from routinely operating surveillance drones in urban and other environments.[7]

If anything, observations by drones may occasion *less* scrutiny than manned aerial vehicles. Several prominent cases, and a significant body of scholarship, reflect the view that no privacy violation has occurred unless and until a human observes a person, object, or attribute.[8] Just as a dog might sniff packages and alert an officer only in the presence of contraband, so might a drone scan for various chemicals or heat signatures and alert an officer only upon spotting the telltale signs of drug production.[9]

In short, drones like those in widespread military use today will tomorrow be used by police, scientists, newspapers, hobbyists, and others here at home.

---

4. *See* Operation and Certification of Small Unmanned Aircraft Systems (SUAS), 76 Fed. Reg. 40,107 (July 7, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-07-07/pdf/2011-15494.pdf#page=16.

5. California v. Ciraolo, 476 U.S. 207 (1986). *See also* Dow Chem. Co. v. United States, 476 U.S. 227 (1986) (holding that no warrant was required for the Environmental Protection Agency to employ a commercial aerial photographer to make a photographic map of a chemical plant).

6. Florida v. Riley, 488 U.S. 445 (1989).

7. This could change if the Supreme Court embraces the D.C. Circuit's mosaic theory of the Fourth Amendment in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010). The mosaic theory holds that even public surveillance can rise to the level of a search if it leads to a sufficiently invasive picture of activity in the aggregate. *Id.* at 561-62.

8. *See* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1153-55 (2011).

9. *See* Illinois v. Caballes, 543 U.S. 405 (2005); United States v. Place, 462 U.S. 696, 707 (1983) ("A 'canine sniff' by a well-trained narcotics detection dog, however, does not require opening the luggage. It does not expose noncontraband items that otherwise would remain hidden from public view, as does, for example, an officer's rummaging through the contents of the luggage."); *cf.* United States v. Jacobsen, 466 U.S. 109 (1984) (holding the testing of powder for the presence of narcotics not a search). As is well-known, the Court has held that the use of thermal imaging and other technologies that are "not in general public use" may violate a reasonable expectation of privacy. Kyllo v. United States, 533 U.S. 27, 34 (2001). The premise of my argument, however, is that drones will be in very common use. Moreover, as alluded to above, *Kyllo* involved an officer observing people in the home. *Id.*

And privacy law will not have much to say about it. Privacy *advocates* will. As with previous emerging technologies, advocates will argue that drones threaten our dwindling individual and collective privacy. But unlike the debates of recent decades, I think these arguments will gain serious traction among courts, regulators, and the general public.

I have in mind the effect on citizens of drones flying around United States cities. These machines are disquieting. Virtually any robot can engender a certain amount of discomfort, let alone one associated in the mind of the average American with spy operations or targeted killing. If you will pardon the inevitable reference to *1984*, George Orwell specifically describes small flying devices that roam neighborhoods and peer into windows. Yet one need not travel to Orwell's Oceania—or the offices of our own Defense Advanced Research Projects Agency—to encounter one of these machines. You could travel to one of several counties where American police officers are presently putting this technology through its paces.

The parallels to *The Right to Privacy* are also acute. Once journalists needed to convince high society to pose for a photograph. New technologies made it possible for a journalist automatically to "snap" a picture, which in turn led to salacious news coverage. Americans in 1890 could just *picture* that tweedy journalist in the bushes of a posh wedding, hear the slap of the newspaper the next day, and see the mortified look of the bridal party in the cover art. Today's police have to follow hunches, cultivate informants, subpoena ATM camera footage; journalists must ghost about the restaurant or party of the moment. Tomorrow's police and journalists might sit in an office or vehicle as their metal agents methodically search for interesting behavior to record and relay. Americans can visualize and experience this activity as a physical violation of their privacy.

There are ways that drones might be introduced without this effect. Previous military technology has found its way into domestic use through an acclimation process: it is used in large events requiring heightened security, for instance, and then simply left in place.[10] We could delay public awareness of drones by limiting use to those that are capable of observing the ground without detection. But these efforts would take a knowing, coordinated effort by the government. The more likely scenario, as suggested by Oklahoma's plan, is one in which FAA restrictions relax and private and public drones quickly fill the sky.

Daniel Solove has argued that the proper metaphor for contemporary privacy violations is not the Big Brother of Orwell's *1984*, but the inscrutable courts of Franz Kafka's *The Trial*.[11] I agree, and believe that the lack of a co-

10. SECURITY GAMES: SURVEILLANCE AND CONTROL AT MEGA-EVENTS (Colin J. Bennett & Kevin Haggerty eds., 2011). One example is the use of biometrics for identification.

11. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001).

herent mental model of privacy harm helps account for the lag between the advancement of technology and privacy law. There is no story, no vivid and specific instance of a paradigmatic privacy violation in a digital universe, upon which citizens and lawmakers can premise their concern.

Drones and other robots have the potential to restore that mental model. They represent the cold, technological embodiment of observation. Unlike, say, NSA network surveillance or commercial data brokerage, government or industry surveillance of the populace with drones would be visible and highly salient. People would *feel* observed, regardless of how or whether the information was actually used. The resulting backlash could force us to reexamine not merely the use of drones to observe, but the doctrines that today permit this use.