

Statement of the American Civil Liberties Union of North Dakota

To: Economic Impact Committee Chairperson Connie Triplett and Economic Impact Committee Members

Fr: Jennifer Cook, Policy Director – American Civil Liberties Union of North Dakota

Re: Legislative Study Relating to the Creation of a Civilian Ground Center for Analysis of Data Received from UAV Operations

Dt: Thursday, November 19, 2015

Introduction

Good afternoon, Chairperson Triplett and members of the Economic Impact Committee. I am Jennifer Cook, policy director for the American Civil Liberties Union of North Dakota. On behalf of our members and activists statewide I want to thank you for the opportunity to testify before this committee about the privacy considerations involving this committee's study on the creation of a Civilian Ground Center to process and analyze data received from Unmanned Aerial Vehicles (hereafter "drones").

We can achieve meaningful privacy protections while still enjoying the benefits of drone technology. Many of the clearest benefits of drone use are either protected by the First Amendment or do not need to involve the collection of personal information while the greatest abuses can be stemmed by adherence to the constitutional protections provided by the Fourth Amendment through strong statutory, judicial and institutional controls.

My testimony will discuss the following: (1.) the current legal landscape; (2) national trends involving drone regulation and privacy laws; and (3) our recommendations to the committee.

Legal Landscape

Constitutional Limitations on Government Use of UAVs

The Supreme Court has not yet had occasion to consider whether the Fourth Amendment places limits on government use of drones. However, it has allowed some warrantless aerial surveillance from *manned* aircraft. Most notably, in the 1986 decision *California v. Ciraolo*, the Court ruled that there was no intrusion into Ciraolo's privacy when police borrowed an airplane, flew it over his backyard and spotted marijuana plants growing there, because "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed."¹

Nonetheless, because of their potential for pervasive use and their capacity for revealing far more than the naked eye, there are good reasons to believe that drones may implicate Fourth Amendment rights in ways that manned flights do not. In both *Dow Chemical Co. v. United*

¹ 476 U.S. 207 (1986).

*States*² and *Kyllo v. United States*,³ the Supreme Court suggested that using sophisticated technology not generally available to the public may be considered a search under the Fourth Amendment.

Further, the Supreme Court has suggested that the continuous use of a surveillance technology may heighten Fourth Amendment concerns. In *United States v. Knotts*, although the Court concluded that the use of a primitive “beeper” tracking device attached to a car in that case did not violate the Fourth Amendment, it held that if “such dragnet type law enforcement practices” as “twenty-four hour surveillance of any citizen of this country” ever arose, it would determine if different constitutional principles would be applicable.⁴ Similarly, in *United States v. Jones*, five justices agreed (in two concurrences) that it was the prolonged nature of tracking a car via GPS that infringed a reasonable expectation of privacy, suggesting that at least prolonged location tracking through other technologies might also constitute a search for Fourth Amendment purposes.⁵

Drone surveillance and any location tracking technology a drone is equipped with enables law enforcement to capture details of someone’s movements for months on end, unconstrained by the normal barriers of cost and officer resources. In a concurrence in the recent Supreme Court case, *U.S. v. Jones*, Justice Sonia Sotomayor described why this was so problematic, emphasizing the intimate nature of the information that might be collected by the GPS surveillance, including “trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.”

While even the limited collection of geolocation information can reveal intimate and detailed facts about a person, the privacy invasion is multiplied many times over when law enforcement agents obtain geolocation information for prolonged periods of time. As the D.C. Circuit Court of Appeals has observed, “[a] person who knows all of another’s travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.”

In addition, there have always been facets of American life that have been uniquely safeguarded from the intrusive interference and observation of government. Constant surveillance threatens

² 476 U.S. 227 (1986). The Supreme Court found that the Environmental Protection Agency did not violate Dow’s Fourth Amendment rights when it employed a commercial aerial photographer to use a precision aerial mapping camera to take photographs of a chemical plant, in part because the camera the EPA used was a “conventional, albeit precise, commercial camera commonly used in mapmaking,” and “the photographs here are not so revealing of intimate details as to raise constitutional concerns.” However, the Court suggested that the use of more sophisticated, intrusive surveillance might justify a different result, writing, “surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant.”

³ 533 U.S. 27 (2001). The Supreme Court rejected the use of thermal imaging devices to peer into a suspect’s home without a warrant, because thermal imaging technology is not readily available to the public.

⁴ 460 U.S. 276, 283-84 (1983).

⁵ 132 S. Ct. at 964 (Alito, J., concurring in judgment), 955 (Sotomayor, J., concurring).

to make even those aspects of life an open book to government. As Justice Sotomayor pointed out in *Jones*, “Awareness that the Government may be watching chills associational and expressive freedoms. And the Government’s unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.”

With drones in so many areas, the technology is moving far more rapidly than our jurisprudence and laws, and it is important that the courts and legislative bodies keep the Constitution relevant in the world of high technology in which we are increasingly going to be living.

Limitations on Private Sector Use of Drones

Government and private sector drone use operate under different legal frameworks. The government currently operates with few restrictions and drone use represents significant potential for immediate harm. In the private sector, harms are also significant but may be buffered by existing legal protections, like tort and peeping tom laws, additional legal protections, and important countervailing First Amendment interests.

Even within these buffers, there are still some areas of concern. One immediate area of concern relevant to the concept of a CGC is the sharing of information between the private sector and police for the purposes of criminal law enforcement. History has demonstrated that information held by the private sector frequently ends up in the hands of government, often in ways that policy makers didn’t anticipate and legal protections don’t address. For example, while the Privacy Act of 1974 is aimed at regulating and safeguarding personal information held by the federal government, federal agencies now circumvent those protections by turning to private data brokers, whose database contains personal information on millions of Americans. Those entities are not regulated by the Privacy Act and routinely provide information that is both inaccurate and inaccessible to its subjects. Given the real and pressing problems we have already described with government drone use, law enforcement must not be able to avoid legal controls by accessing private drone footage. It is this area of concern that additional legal protections should be implemented by the state to avoid civil liberties violations.

The ACLU of North Dakota’s focus is on regulating government use of drones. Private industry and research institutions should be free to continue their research and development, consistent with current state laws. However, putting privacy protections in place regarding private industry to government data sharing is actually good for business. With privacy protections in place, many people will be more comfortable with the idea of domestic drone use, which will create a more favorable business climate. In fact, the Chair of the Aerospace States Association, an organization that represents the aerospace industry, recently recognized that, “If you don’t stand up for privacy, there’s no industry.”

In addition to already existing legal protections regarding the private or commercial use of drones, the FAA Modernization and Reform Act of 2012 requires the FAA to integrate drones into the national airspace by the end of 2015. Although the FAA’s primary focus will be on mechanics of integrating drones into our airspace safely, the FAA has acknowledged that privacy needs to be part of that process. The FAA has determined that the best avenue to develop privacy protection is by integrating their development with the agency’s existing mandate to choose six

test sites, each for five years, for drone research. These test sites are “defined geographic area[s] where research and development are conducted.” And as you know, North Dakota is one such test site. The lessons learned and best practices established at the test sites may be applied more generally to protect privacy in UAS operations throughout the NAS.[National Airspace] The FAA has created the following privacy requirements for each drone test site operator:

1. Maintain and update a publicly available privacy policy which governs all drone operators;
2. Create a mechanism to receive public comment on its policy;
3. Conduct an annual audit of test site operations and assure that all operators are compliant;
4. Comply with all applicable privacy law; and
5. Require all drone operators to have a written plan for retention and use of data collected.

The agency’s goal with these regulations is not only to govern test site operators but also provide an “opportunity for development and demonstration by the test site operators and users of policies and operating approaches that would address both drone operator mission needs and related individual privacy concerns.

State Law Limitations on Drone Use: North Dakota’s Drones Law N.D.C.C. 29-29.4

This past legislative session the legislature passed House Bill 1328. This law provides some regulation of the use of drones and the information obtained from them. Generally, North Dakota’s drones law requires law enforcement to obtain a warrant to use the data collected by drones for use in a prosecution or proceeding within the state. The law does not prohibit the use of drones by law enforcement to conduct mass general surveillance on North Dakota citizens. Specifically, as the law relates to the concept of a CGC, there are a few relevant portions.

First, Section 2, paragraph 1 and 2 prohibit data collected from the operation of drones to be used in a prosecution or proceeding by law enforcement unless it has been obtained pursuant to a court order. With respect to potential CGC operations, any data a CGC collects and retains will be subject to this section in that law enforcement should not be able to access drone surveillance data without a warrant.

The second relevant portion is Section 4, paragraph 2, because it allows law enforcement to access drone data in the event of exigent circumstances. It appears this portion of North Dakota’s drones law may be most applicable to the concept of a CGC, if as the study’s language indicates the purpose of a CGC would be to facilitate data sharing with first responders in the event of a local, state, or federal emergency.

The third relevant portion of North Dakota’s drones law is the data retention restrictions found in Section 6, paragraph 4. Here, any data obtained that is not relevant to an ongoing investigation or trial, and data that does not contain a reasonable and articulable suspicion of criminal wrongdoing must be deleted within 90 days. In the event the CGC receives and analyzes data for

local, state, and federal first responders it will be required to delete data in accordance with this provision.

ND Privacy Laws

Unlike a number of other states, North Dakota does not have a wide array of privacy or electronic data privacy laws that adequately protect its citizens for the digital age we live in. North Dakota lacks an electronic communications privacy act, which is particularly relevant to the concept of a CGC and the potential for it to process electronic signals from cell phones and internet services data.

Additional Considerations: Other States' Privacy Laws & Drones Laws

If the concept of the CGC, as the Mr. Nierode's memo to the committee from the September 17 suggests, is to create a national hub in North Dakota for data analysis, it is imperative that this committee consider the impact laws from other states will have on the economic viability of the CGC. The CGC will likely be required to comply with other states' laws if intends to receive and transfer data to its clients from outside North Dakota.

The current national trend is moving toward regulating government drone use to prevent privacy and civil liberties violations. In the past two years, 24 states have enacted drones legislation. Of those 24 states, at least 16 have passed legislation that limits law enforcement use of drones in some manner.

Additionally, although Congress and the Supreme Court have yet to weigh in on the question of whether warrantless historic or real time geolocation tracking of an individual via their cell phone by law enforcement is constitutional, a growing number of state legislatures are starting to move toward enacting greater privacy protections through electronic communications privacy acts or cell site simulator privacy acts.

Recommendations

Our analysis of the proposed CGC concept leads us to believe that a CGC raises some serious privacy concerns. Specifically, proposed data sharing between the private sector and government agencies, in particular data sharing with law enforcement agencies may lead to Fourth Amendment violations. Additionally, there are data security concerns. A central repository of large amounts of sensitive data is an attractive target for hacking and other forms of unauthorized access. In order to address our concerns we recommend this committee strengthen North Dakota's current drones law and enact an electronic communications privacy act which would allow the CGC to share data with its clients, particularly government agencies and law enforcement, without violating the privacy and civil liberties of North Dakotans or other citizens of the United States. The following list details these two primary recommendations and also provides a few other important considerations:

Strengthen North Dakota's Existing Drones Law

- Include explicit language to prohibit the use of drones for mass surveillance policing
 - This would allow the operation of drones by a law enforcement agency only if the agency obtains a court order or warrant, in accordance with the exceptions to the warrant requirement, and in the event of exigent circumstances
 - Or at the very least require a reasonable and articulable suspicion of criminal wrongdoing to operate the drone in public areas
- Amend the law to include explicit language that prohibits data sharing between:
 - Government agencies to law enforcement for use in a trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the state, or for any intelligence purpose
 - Private entities to government agencies for use in a trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the state, or for any intelligence purpose
 - Include stronger data retention language
 - Prohibit data that is collected on an individual, home, or area other than the target that justified the deployment from being used, copied, or disclosed for any purpose.
 - Require such data be deleted as soon as possible (ideally within 24-48 hours).

Enact a North Dakota Electronic Communications Privacy Act

- Secures the privacy of an individual's electronic communications (to include location tracking via cell phones) by requiring law enforcement obtain a warrant to access such information
 - Provides exceptions for exigent circumstances

Require CGC Specific Regulation

- Require robust data security measures to prevent cyber hacks and unauthorized access
 - Include audit trail requirements for access to data
 - Sanctions in place for mishandling of data
- Require data retention policy
 - Limits to retention period for target data and non-target data
 - Secure methods of data transfer/transmission
- Create an independent oversight board
 - Includes stakeholders from broad interest groups to include privacy and civil liberties groups/advocates

- Require public accountability and transparency
 - Reporting requirement to the legislature
 - Report should include the following information
 - Number of times drone was used, type of incidents and types of justifications for deployment
 - Number of crime investigations aided by use of drone
 - Number of uses of drone for reasons other than criminal investigation
 - Frequency and type of data collected on individuals other than targets
 - Total cost of drone deployments
 - Consider making the legislative report publicly available
 - Public Records Requirement