

2015 HOUSE JUDICIARY

HB 1328

2015 HOUSE STANDING COMMITTEE MINUTES

House Judiciary Committee
Prairie Room, State Capitol

HB 1328

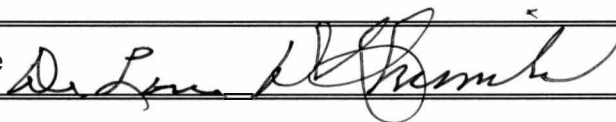
2/4/2015

23253

☐ Subcommittee

☐ Conference Committee

Committee Clerk Signature



Explanation or reason for introduction of bill/resolution:

An Act to provide for limitations on the use of unmanned aircraft for surveillances.

Minutes:

Testimony #1,2,3,4,5,6,7,8,9

Chairman K. Koppelman: Opened the hearing with testimony in support.

Rep. Rick C. Becker: This bill is commonly referred as the drone bill. A large part of this bill has been written by an attorney in Grand Forks who has extensive history with the fourth amendment and with drones. I did incorporate some of the amendments the committee here did put in the bill. The bill intends law enforcement get a warrant prior to conduct surveillance. We need to know where the data is going and who is going to see it. He went through the bill. (2:35-16:21)(See Testimony #1) It is highlighted. The number one concern with FFA felt it would be a negative impact to UND and ND as a whole. We have now been chosen so that is mute. I think drones have created a gray area and so we need to be proactive. Privacy and the issues of privacy make the US special. (0-16:21)

Chairman K. Koppelman: The amendments we added were done were the result of working with law enforcement community during the last session and addressed the concerns that they had voiced. There were still some individuals in law enforcement that didn't like the bill even after amended.

Rep. L. Klemin: What about the nosey neighbor? Is that not a concern?

Rep. Becker: You are correct. I think there are two different issues.

Rep. Lois Delmore: Now we have plain view search. Is that addressed in this bill?

Rep. Becker: The benefit of the drone is it goes beyond plain view. They have many capabilities and imaging. Not only does the drone have the ability to see beyond plain view; it has the technology to see more than visual.

Rep. Lois Delmore: The bill would negate that because you think the drone has more powers than what a police officer might be able to observe?

Rep. Becker: Yes

Rep. Lois Delmore: You have remedies for violations in here. Did you have that in the last bill and can you explain a little more to us what that means?

Rep. Becker: That was in the previous bill. It would be more beneficial to have it answered by a lawyer.

Rep. L. Klemin: Usually we talk about requiring a warrant. Where a person might have a reasonable expectation of privacy are they in here somewhere.

Rep. Becker: No they are not in the bill.

Chairman K. Koppelman: The focus of your bill is the drone. You are trying to be sure privacy is not intruded. Is there a way to help define the definition of plain view?

Rep. Becker: Yes you are right about that. If I am in my back yard a drone or airplane could see into my back yard.

Chairman K. Koppelman: That is what I have struggled with and I don't know a lot about drones and they could survey things, but my struggle is do we deal with that by talking about another product or camera?

Rep. Becker: This is technology specific. I wanted to deal with the here and now. The sheriff's department acquiring their drones and the range of uses for them so I don't know how to rephrase the bill to encompass technologies we don't know.

Rep. D. Larson: Can warrants be obtained to investigate Class A misdemeanors?

Rep. Becker: Yes it is my understanding it can and this committee deleted Subsection 2 or changed it a lot. Should the drones be used for felonies only or for important misdemeanors too? I don't have a major grip about that.

Rep. D. Larson: There may be some times that a judge would issue a warrant regarding safety to other people that may not rise to the point of a felony until it is already done. I am not sure why you would not want to limit a drone usage?

Rep. Becker: Your comments are noted. If warrants are required I rely on the decision making skills and process and judges to use it properly. I cannot disagree with you.

Jennifer Cook, American Civil Liberties Union of ND: (See testimony #2) (31:11-35:41)

Rep. G. Paur: Do you have any idea how this bill compares with other states?

Jennifer Cook: I do not. I can get that information.

Opposition:

Robert Rost, Grand Forks County Sheriff's Department: (See testimony #3) (37:02 - 41:40)

Rep. L. Klemin: What would this bill require you to do that you are not already doing?

Robert Rost: The FFA has established all the rules and guidelines. We would not utilize the aircraft for anything that if we had to do something on the ground to get a search warrant we would do that anyway. The air is free air. Expectation of privacy is if you are in your house or something that would be expectation of privacy. Let the judges do their job.

Rep. L. Klemin:

Robert Rost: We would get a warrant from a judge anyway. We took the least evasive things first.

Rep. G. Paur: You mentioned the helicopter flying at 400' does the same thing as a UAS at 400'. Can a helicopter go at 20' above the ground of a parking lot?

Robert Rost: I am sure he could, but it would be in violation of the FFA law.

Rep. D. Larson: I am sure as a homeowner you own 400' up from your home.

Robert Rost: We are limited to 400'. That is far as the UAS can fly by FFA rules. Air is not part of what you own.

Chairman K. Koppelman: 400' is as high as you can go. UAF can go anywhere below that?

Rep. Brabandt: How many drones are in the air at one time?

Robert Rost: Custom and border patrol use drones. We only have one up at a time. I do have a request from Cass County that he would like to be part of it.

Rep. Mary Johnson: The plain view doctrine it is the ability of the UAS to record and save imaging and so that negates the plain view doctrine because if you are able to go back to imaging that contemporary nature of the plain view doctrine is lost.

Robert Rost: We have not done any of that yet where we have had to take criminal activity pictures. Those are all sent to the FFA.

Rep. Mary Johnson: Then this bill would prohibit that?

Robert Rost: If we are doing criminal activity and I needed a search warrant to do that. I think it will complicate issues.

Rep. Mary Johnson: We regulate judges.

Robert Rost: I don't think we need a bill that says we need a search warrant for felonies. We probably would do that anyway if we were conducting a search.

Chairman K. Koppelman: There is nothing in law framing any regulations for UAS now. What is wrong with having something in law laying out what you need to do?

Robert Rost: You are not giving us any credit for making a decision and I try and do the best I can to make sure I honor people's rights.

Chairman K. Koppelman: This committee worked with lobbyist representing law enforcement during the session to craft amendments to address any concerns indicates that we do trust and respect what you do.

Bruce Buekett, Spokesman for ND Peace Officers Association: (See testimony #4) 56:17-1:02:16)

Mike Corcoran, Ass't Director for the Unmanned Systems for UND: (See testimony #5) (1:02:27-1:10:10)

Rep. Mary Johnson: I trust the committee is developing these policies but they just don't have the force of law.

Rep. K. Wallman: UAS, UAV are the same thing? Page 1 of your testimony you referred Community Standards is a floating definition.

Mike Corcoran: There are various members who are on these committees to establish these standards.

Rep. K. Wallman: All those people got together and decided it was OK.

Mike Corcoran: That maybe better answered by law enforcement. They are not stealth.

Chairman K. Koppelman: We don't like this bill because we think it is an attack on us. Is there anything specific in the bill that you object to?

Mike Corcoran: Section 8, paragraph 6 paints a broad brush in research and it did grab out attention. In research what we have learned is a lot in the last couple years along what the public's perception is and it is very favorable.

Rep. L. Klemin: The UAS research compliant committee is only effective for the sixteen county areas that you are part of.

Mike Corcoran: They have a charter that defines what they do.

Suspended the hearing; it will reopen Monday.

Chairman K. Koppelman: You can contact the committee with constructive information or leave your testimony with us and we will continue with this and thank you for your patience.

Testimony 6,7,8,9 handed in after the meeting:

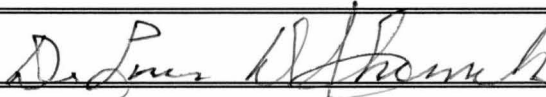
2015 HOUSE STANDING COMMITTEE MINUTES

Judiciary Committee
Prairie Room, State Capitol

HB 1328
2/9/2015
23502

☐ Subcommittee
☐ Conference Committee

Committee Clerk Signature



Minutes:

Testimony #1, 2; 3

Chairman K. Koppelman: reopened the hearing on this bill. I have visited with law enforcement representatives that were in the room that day. They have had input into the proposed amendments and I asked legislative counsel to draft those amendments. If those amendments were offered law enforcement would be taking a neutral stand.

Further support: None

Opposition:

Keith Lund, President Economic Development Association of ND: (See testimony #1) Had been handed out 2-4-15. (2:05-3:12) obviously there has been a lot of emphasis placed on UAS development and particularly out of UND. ND has been designated a test site for FAA. Also we are getting near a lease signing of the Grand Sky UAS development park on the Grand Forks Air Force Base so that has been a lot of hard work in this industry. There are organizations AUSA is the Association of unmanned vehicle systems international that are tracking information related to this industry across the US and across the globe. They are specifically tracking states that have limited legislation that impact the development of UAS. We view UAS as a statewide opportunity. Our board membership and they are unanimous in their opposition of this bill; they are from Fargo, Jamestown, Mandan, Beach and Williston. We have not seen the amendments, but the bill as proposed be are opposed to that.

Chairman K. Koppelman: Those in law enforcement said they have language in the bill that was submitted by UND. I would encourage you to look at those amendments when they are offered.

Rep. L. Klemin: I am puzzled by your comments that we don't need this bill because existing law takes care of the issue. You are on the other hand saying this law would affect the application and use of UAS systems. If we don't need it how can it affect the UAF systems in ND if we did do this?

Keith Lund: There are organizations UAS signed particularly the largest unmanned aircraft systems association are tracking information relative to states and other regions that limit UAF development and so my testimony was to suggest that states or other regions that have specific legislation that limit US development would be put a bad list and that would have the potential to direct investment in ND to other states that do not have that limiting legislation.

Rep. G. Paur: You said they track legislation which inhabits development requiring a search warrant for surveillance is restricting development?

Keith Lund: Legislation that further restricts is what I meant. If this legislation would pass we feel ND would have legislation that would be listed as a state does have a piece of limiting regulation regarding UAF.

Rep. Mary Johnson: So you are arguing for the amendment bill? Is the bill we have before us what you are addressing?

Keith Lund: Yes.

Rep. K. Wallman: This limiting legislation is what this bill would be cauterized in that association is that strictly because it limits research endeavors?

Keith Lund: I don't know if it would limit research.

Rep. K. Wallman: This association do they have a board that has responsibility for the technology as developed? It seems it would be in everyone's responsibility to be sure that states are regulating this in a way so it is not abused.

Keith Lund: I am not certain they do?

Rep. K. Wallman: If the regulations are already in place then they probably shouldn't penalize us for trying to put some regulations in place by putting us on this black list? Does that make sense?

Keith Lund: Yes it does.

Rep. D. Larson: In the bill on page 3 of the bill at the end of section 4 which gives exceptions it says there is #4 that says for testing, training, education and research. Would that take care of your concern?

Keith Lund: That has not been the discussion. When you are doing testing you need to do it at an existing test site; certificate of authorization to the FAA so those types of activities are there. It is the application of UAS technology is a concern in terms being negatively viewed as limiting that development. We feel protections exist in the fourth amendment.

Chairman K. Koppelman: Two years ago we had similar bills and it did pass the house but was defeated in the Senate. The issue for us is to say we have the FFA, fourth amendment, court decisions so we don't need a statute which is what we are hearing in a lot

of ways. Maybe this is the wrong bill, but to simply say don't legislate on this matter because we have the fourth amendment to the Constitution we may as well not meet because a lot of what we do has to do with constitutional principal that has been laid down.

Brian Opp: North Dakota Dept. of Commerce: (Reading Testimony #2) (15:10-17:00)

Rep. L. Klemin: The Northern Plains US Test Site is what?

Brian Opp: The test site is a governmental agency that is under the Department of Commerce. This was the office of record that submitted the proposal to the FAA to be selected as one of six test sites to actually carry out the work of a test site that governmental body was created.

Chairman K. Koppelman: Do you actually regulate it?

Brian Opp: That is more accurately stated. The FAA regulates and overseas the test sites. From a state standpoint the Dept. of Commerce is responsible for the over site of the test site from a state prospective.

Rep. K. Wallman: Mr. Becklund isn't actually in favor of regulating all these other forms of UAS's?

Brian Opp: I can't speak for Mr. Becklund. I think you may be right, but I can't say for certain because I did not have that conversation with him.

Rep. Mary Johnson: Can you provide which specific sections he has concerns about?

Brian Opp: I do not have the specific sections of the bill Mr. Becklund was referring to.

Rep. Mary Johnson: We come down to Rep. Paur and Rep. Wallman's concerns. Can somebody be more specific about this bill?

Brian Opp: The comments on being black listed and tied back to the change of landscape, yes landscape has changed from the last time a similar bill was considered. ND was awarded one of six UAS test sites by the FAA. That test site has become operational as of last year and they have been doing a lot of great work. The real concern going forward is the opportunity to translate the successes so far into tangible outcomes in the future such as the development of this industry within ND.

Rep. Mary Johnson: Somebody from the FFA needs to come in and connect the dots. Right now we are dealing with generalities?

Chairman K. Koppelman: I would encourage you to get a copy of these proposed amendments and see if that eases some of those concerns.

Rep. L. Klemin: This bill may have a dampening effect on various industries. We have this section 9 that says this act may not be construed to limit, constrain, or adversely impact

testing in operations of the state range under FAA Moderation Reform Act. Doesn't that take care of the concern?

Brian Opp: Your comments are on as the bill is written. Where the concern comes in is not from the test site prospective, but private industry that is a client or customer to the test site who's working with ND to carry out testing and development and advancement activities within the state. They would also be a part of this even though they are not part of the test site themselves so would they also be bound by those types of requirements? Would those have those negative impacts and that is where the concern.

Rep. L. Klemin: Are you saying a customer of a test site should be able to do unrestricted without a warrant surveillance of any type?

Brian Opp: Not at all. I don't have a good understand of how a test site client would be impacted by the bill.

Rep. Brabandt: Where is the funding coming from for the Northern Plains Unmanned Aircraft Systems Test Site?

Brian Opp: It is funded by the State of ND. The FAA and the federal government are not funding this program. There is an expectation the test site will be engaging customers and clients and generating revenues going forward.

Rep. K. Hawken: You referenced that you have received amendments.

Chairman K. Koppelman: This is a continuation of the hearing so the amendments will be offered after the hearing is closed.

Rep. Lois Delmore: That is why I wanted to get a copy of those amendments so people involved because it may change very much.

Chairman K. Koppelman: We would welcome them registering their opinion once they have seen the amendments.

Rep. K. Wallman: Mr. Lund testified that the hang up from his prospective was the limits on the use and that also speaks to Rep. Klemin's comments and concerns.

Chairman K. Koppelman: If the concern is language in the bill that deals with technology we would like to know what that is. The intent of the bill is basically dealing with law enforcement and not private industry.

Rep. K. Wallman: Everything is pointing in the direction that folks who want to come and test this technology at our site they want to be able to test it and how it applies to law enforcement, could that be?

Brian Opp: I think there is tremendous interest within the UAS industry for law enforcement applications. I believe there are other industries that maybe don't have the

same applications in mind, but would potentially perhaps is not viewed as business friendly and thus having the dampening effects.

Chairman K. Koppelman: What are the sites that were selected in addition to ND?

Brian Opp: Alaska, Nevada, Texas, Virginia and New York.

Chairman K. Koppelman: Do any of those states have any kind of language in their statutes at all regarding this technology?

Brian Opp: I don't know the answer to that, but we can certainly provide it.

Neutral: None

Hearing closed.

Testimony #3 handed in after the hearing.

2015 HOUSE STANDING COMMITTEE MINUTES

Judiciary Committee
Prairie Room, State Capitol

HB 1328
2/18/2015
24098

☐ Subcommittee
☐ Conference Committee

Committee Clerk Signature



Minutes:

Handout #1, Proposed amendment #2, #3, #4

Chairman K. Koppelman (See handout #1) Went over the handout. (1:45-2:40) (See proposed amendment

Rep. D. Larson: In most of these states it talks about enabling legislation so it comes at it from a much more positive thing rather than it is says law enforcement can obtain the information gathered from this. It spells out the ways they can use it but it feels like a more friendly way of doing this. It spells out the ways they can use it, but it feels like a more friendly way of approaching it. This creates as many laws for neighbors and media or other people who may use UAS's to infringe on people's privacy.

Chairman K. Koppelman: You make a good point. (See proposed amendment #2 .02003 & #3.02002) This came from the law enforcement community. I wanted you to be able to look at all those things including privacy and law enforcement and then carve out exceptions for law enforcement.(4:50-6:50)

Rep. Lois Delmore: I am concerned that two parts of it I can't find. The act does not apply or restrict in any way. We need to fix the language. Very confusing?

Chairman K. Koppelman: The amendment #3 at the end has a section that the law enforcement folks had proposed after talking with the people up at UND. Rep. Delmore also proposed language from them so I wanted her to compare the two and see how they interface.

Rep. Lois Delmore: It needs to add the words this act does not restrict in any way research, education, training testing so it is a cleanup of language. It is also missing in the Section 1 it is missing this act applies only to law enforcement agencies of and within the state of ND and its political subdivisions. Page 5, Under Section 8, part 6 they want to remove that documentation that applies to all uses of unmanned aircraft system including testing, training, education and research. So there is a problem with that documentation and reporting so those are the three. Page five is there.

Chairman K. Koppelman: Page 5 does remove the amendment. Section 9 was originally designed to deal with UND issue and doesn't really apply.

Rep. Lois Delmore: It takes 6-12 out so that is the second amendment I had. We need to add under Section 4 under definitions the act applies to law enforcement agencies of and within the state of ND and its political subdivisions. We need to reword on page 3, line 6 a little bit too.

Chairman K. Koppelman: It already addresses law enforcement agencies specifically and it already takes care of exempting the research and training and all of that. There might be something else in the bill that might apply to others other than law enforcement. I am not sure that is necessary. I am not sure we want to target law enforcement. I think that is the point of some of these. Otherwise I don't have any problem with what you are recommending.

Rep. D. Larson: I don't like shooting from the hip. I would personally like to take under page 1, section 2; I would like to reword it. I would like to say like Texas it enumerates 19 lawful uses of an unmanned aircraft including the use in connection with a valid search warrant etc.

Chairman K. Koppelman: The majority leader wants all these bills out today and I apologize. We did not control the timing and we have had cross over on the calendar for a long time and in our committee for a long time. You are all free to propose amendments and that is why these are before us because we had asked people to do that. You can propose them verbally today too.

Amendment .02003 moved by Rep. L. Klemin: Seconded by Rep. Kretschmar

Discussion:

Chairman K. Koppelman: The bill and these amendments are consistent from the Grand Forks sheriff and I think these amendments take care of #5 of Rep. Delmore's amendment. Those whole bill and these amendments only talk about law enforcement. We are under a time crush now and these are good amendments. We are basically proposing a place holder amendment because we have not had time to get everything together. If you see things you don't like or like some wording changed we can go to the Senate with that and say this is one of the last bills we moved out of judiciary and they can add it and we can have another look at it because we could concur or not concur with a Senate amendment so those are all options in terms of the way the process flows.

Rep. L. Klemin: I have looked through these amendments that we are discussing and it seems to me they are well worded and the basic premise of these amendments are consistent with the bill and it just rewords that basically you have to have a warrant. When the sheriff from Grand Forks was here testifying my notes say if they were going to use it the warrant is required for flights that would infringe on an individual's reasonable expectation of privacy. I see the bill being consistent with the testimony from the sheriff. I also think these amendments take care of #5 of Rep. Delmore's amendment. I think we are under a time crunch right now so I think these are good amendments.

Rep. Maragos: If this bill passes and gets to the Senate and we will have our second chance at it in conference.

Voice vote carried.

Rep. G. Paur Moved a do pass as amended; Seconded Rep. L. Klemin:

Rep. P. Anderson: I am really uncomfortable with what we are doing right here. We can amend this all we want but I am voting no. I don't know the unintended consequences at all.

Rep. K. Wallman: I don't think we have had enough time to look at this bill. This is the first time I have seen these amendments and I like to be through.

Rep. L. Klemin: This bill says if you are going to use the drone for surveillance you need a warrant unless it is subject to a well-recognized court exception and there are a number of those; or unless it is subject to exceptions that we stated in the bill which we have covered the concerns of UND and law enforcement said if we have to get a warrant we would have to get a warrant anyway so I don't see what the problem is. If we look at what other states have done; there are many states that have done exactly the same thing regardless of whether they phase it one way or another.

Chairman K. Koppelman: I don't ever remember getting amendments days in advance so this is not unusual. We do need to get these bills out today.

Rep. D. Larson: So all of these amendments this is what law enforcement said they wanted and they are now comfortable with this is what you are saying?

Chairman K. Koppelman: Yes they are comfortable and Mr. Burkett is in the room and Game & Fish and they noted there might still be members of law enforcement; a sheriff or police chief that may or may not be personally not like the bill, but as a law enforcement community they are comfortable with these amendments.

Roll Call Vote: 9 Yes 4 No 0 Absent Carrier: Chairman K. Koppelman:

(Testimony #4 passed out earlier)

JK
2/18/15

PROPOSED AMENDMENTS TO HOUSE BILL NO. 1328

Page 1, line 1, replace "aircraft" with "aerial vehicle"

Page 1, line 6, after "1." insert "Flight data" means imaging or other observation recording.

2. "Flight information" means flight duration, flight path, and mission objective.

3."

Page 1, line 6, after "agency" insert "or agents"

Page 1, line 6, remove "means a person authorized by law, or funded by the state."

Page 1, line 7, replace "to investigate or prosecute offenses against the state" with "has the meaning provided for law enforcement officer in section 12.1-01-04"

Page 1, line 8, replace "2." with "4."

Page 1, line 8, replace the first "aircraft" with "aerial vehicle"

Page 1, line 8, replace the second "aircraft" with "aerial vehicle"

Page 1, line 9, replace "aircraft" with "aerial vehicle. The term does not include satellites."

Page 1, line 10, replace "3." with "5."

Page 1, line 10, replace the first "aircraft" with "aerial vehicle"

Page 1, line 10, replace the second "aircraft" with "aerial vehicle"

Page 1, line 11, replace "aircraft" with "aerial vehicle"

Page 1, replace lines 15 through 24 with:

"Limitations on use of unmanned aerial vehicle system.

1. Information obtained from an unmanned aerial vehicle is not admissible in a prosecution or proceeding within the state unless the information was obtained:

a. Pursuant to the authority of a search warrant; or

b. In accordance with exceptions to the warrant requirement.

2. Information obtained from the operation of an unmanned aerial vehicle may not be used in an affidavit of probable cause in an effort to obtain a search warrant"

Page 2, line 3, replace "aircraft" with "aerial vehicle"

Page 2, line 5, replace "aircraft" with "aerial vehicle"

Page 2, line 6, replace "aircraft" with "aerial vehicle"

2/3

Page 2, line 7, replace "aircraft" with "aerial vehicle"

Page 2, line 9, replace "aircraft" with "aerial vehicle"

Page 2, line 11, replace "aircraft" with "aerial vehicle"

Page 2, line 12, replace "aircraft" with "aerial vehicle"

Page 2, line 21, replace "aircraft" with "aerial vehicles"

Page 2, line 23, replace "aircraft" with "aerial vehicles"

Page 2, line 26, replace "aircraft" with "aerial vehicles"

Page 3, line 1, replace "aircraft" with "aerial vehicle"

Page 3, line 2, after "state" insert "or local"

Page 3, line 6, replace "Testing, training, education, and research of unmanned aircraft systems." with "Research, education, training, testing, or development efforts undertaken by or in conjunction with a school or institution of higher education within the state and its political subdivisions, nor to public and private collaborators engaged in mutually supported efforts involving research, education, training, testing, or development related to unmanned aerial vehicle systems or unmanned aerial vehicle system technologies and potential applications."

Page 3, line 8, replace "surveillance" with "use"

Page 3, line 9, replace "aircraft" with "aerial vehicle"

Page 3, line 10, remove "Use of force."

Page 3, line 10, replace "state" with "law enforcement"

Page 3, line 11, replace "aircraft" with "aerial vehicle"

Page 3, line 11, remove "or nonlethal"

Page 3, line 11, remove the second comma

Page 3, line 12, remove "including firearms, pepper spray, bean bag guns, mace, and sound-based weapons"

Page 3, line 13, replace "state" with "law enforcement"

Page 3, line 14, replace "aircraft" with "aerial vehicle"

Page 3, remove lines 22 through 31

Page 4, remove lines 1 through 19

Page 4, line 21, replace "aircraft surveillance" with "aerial vehicle use"

Page 4, line 23, replace "aircraft" with "aerial vehicle"

Page 4, line 24, remove ", including the names of place"

Page 4, line 25, remove "or persons authorized to be subject to surveillance"

Page 4, line 26, replace "certified" with "verified"

9/3
Page 4, line 29, after "4." insert "Any imaging or any other forms of data lawfully obtained under this Act which are not accompanied by a reasonable and articulable suspicion that the images or data contain evidence of a crime, or are relevant to an ongoing investigation or trial, may not be retained for more than ninety days.

5."

Page 4, line 29, replace "aircraft" with "aerial vehicle"

Page 5, line 1, replace "aircraft" with "aerial vehicle"

Page 5, line 4, replace "5." with "6."

Page 5, remove lines 6 through 12

Renumber accordingly

Date: 2-18-15
Roll Call Vote #: 1

2015 HOUSE STANDING COMMITTEE
ROLL CALL VOTES
BILL/RESOLUTION NO. 1328

House JUDICIARY

Committee

☐ Subcommittee

☐ Conference Committee

Amendment LC# or Description: 15.0259 . 02003

Recommendation: ☒ Adopt Amendment

☐ Do Pass

☐ Do Not Pass

☐ Without Committee Recommendation

☐ As Amended

☐ Rerefer to Appropriations

Other Actions:

☐ Reconsider

☐

Motion Made By

Rep Klemin

Seconded By

Rep. Kretschmar

Representative	Yes	No	Representative	Yes	No
Chairman K. Koppelman			Rep. Pamela Anderson		
Vice Chairman Karls			Rep. Delmore		
Rep. Brabandt			Rep. K. Wallman		
Rep. Hawken					
Rep. Mary Johnson					
Rep. Klemin					
Rep. Kretschmar					
Rep. D. Larson					
Rep. Maragos					
Rep. Paur					

voice
vote
CARRIED

Total (Yes) _____ No _____

Absent _____

Floor Assignment _____

If the vote is on an amendment, briefly indicate intent:

Date: 2-18-15
Roll Call Vote #: 2

2015 HOUSE STANDING COMMITTEE
ROLL CALL VOTES
BILL/RESOLUTION NO. 1328

House JUDICIARY Committee

☐ Subcommittee ☐ Conference Committee

Amendment LC# or Description: _____

Recommendation: ☒ Adopt Amendment
☒ Do Pass ☐ Do Not Pass ☐ Without Committee Recommendation
☒ As Amended ☐ Rerefer to Appropriations
Other Actions: ☐ Reconsider ☐ _____

Motion Made By Rep. Paur Seconded By Rep. Klemin

Representative	Yes	No	Representative	Yes	No
Chairman K. Koppelman	✓		Rep. Pamela Anderson		✓
Vice Chairman Karls	✓		Rep. Delmore		✓
Rep. Brabandt	✓		Rep. K. Wallman		✓
Rep. Hawken	✓				
Rep. Mary Johnson	✓				
Rep. Klemin	✓				
Rep. Kretschmar	✓				
Rep. D. Larson		✓			
Rep. Maragos	✓				
Rep. Paur	✓				

Total (Yes) 9 No 4

Absent 0

Floor Assignment Rep. Koppelman

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE

HB 1328: Judiciary Committee (Rep. K. Koppelman, Chairman) recommends **AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (9 YEAS, 4 NAYS, 0 ABSENT AND NOT VOTING). HB 1328 was placed on the Sixth order on the calendar.

Page 1, line 1, replace "aircraft" with "aerial vehicle"

Page 1, line 6, after "1." insert "Flight data" means imaging or other observation recording.

2. "Flight information" means flight duration, flight path, and mission objective.

3. "

Page 1, line 6, after "agency" insert "or agents"

Page 1, line 6, remove "means a person authorized by law, or funded by the state."

Page 1, line 7, replace "to investigate or prosecute offenses against the state" with "has the meaning provided for law enforcement officer in section 12.1-01-04"

Page 1, line 8, replace "2." with "4."

Page 1, line 8, replace the first "aircraft" with "aerial vehicle"

Page 1, line 8, replace the second "aircraft" with "aerial vehicle"

Page 1, line 9, replace "aircraft" with "aerial vehicle. The term does not include satellites."

Page 1, line 10, replace "3." with "5."

Page 1, line 10, replace the first "aircraft" with "aerial vehicle"

Page 1, line 10, replace the second "aircraft" with "aerial vehicle"

Page 1, line 11, replace "aircraft" with "aerial vehicle"

Page 1, replace lines 15 through 24 with:

"Limitations on use of unmanned aerial vehicle system.

1. Information obtained from an unmanned aerial vehicle is not admissible in a prosecution or proceeding within the state unless the information was obtained:

a. Pursuant to the authority of a search warrant; or

b. In accordance with exceptions to the warrant requirement.

2. Information obtained from the operation of an unmanned aerial vehicle may not be used in an affidavit of probable cause in an effort to obtain a search warrant"

Page 2, line 3, replace "aircraft" with "aerial vehicle"

Page 2, line 5, replace "aircraft" with "aerial vehicle"

Page 2, line 6, replace "aircraft" with "aerial vehicle"

Page 2, line 7, replace "aircraft" with "aerial vehicle"

Page 2, line 9, replace "aircraft" with "aerial vehicle"

Page 2, line 11, replace "aircraft" with "aerial vehicle"

Page 2, line 12, replace "aircraft" with "aerial vehicle"

Page 2, line 21, replace "aircraft" with "aerial vehicles"

Page 2, line 23, replace "aircraft" with "aerial vehicles"

Page 2, line 26, replace "aircraft" with "aerial vehicles"

Page 3, line 1, replace "aircraft" with "aerial vehicle"

Page 3, line 2, after "state" insert "or local"

Page 3, line 6, replace "Testing, training, education, and research of unmanned aircraft systems." with "Research, education, training, testing, or development efforts undertaken by or in conjunction with a school or institution of higher education within the state and its political subdivisions, nor to public and private collaborators engaged in mutually supported efforts involving research, education, training, testing, or development related to unmanned aerial vehicle systems or unmanned aerial vehicle system technologies and potential applications."

Page 3, line 8, replace "surveillance" with "use"

Page 3, line 9, replace "aircraft" with "aerial vehicle"

Page 3, line 10, remove "Use of force."

Page 3, line 10, replace "state" with "law enforcement"

Page 3, line 11, replace "aircraft" with "aerial vehicle"

Page 3, line 11, remove "or nonlethal"

Page 3, line 11, remove the second comma

Page 3, line 12, remove "including firearms, pepper spray, bean bag guns, mace, and sound-based weapons"

Page 3, line 13, replace "state" with "law enforcement"

Page 3, line 14, replace "aircraft" with "aerial vehicle"

Page 3, remove lines 22 through 31

Page 4, remove lines 1 through 19

Page 4, line 21, replace "aircraft surveillance" with "aerial vehicle use"

Page 4, line 23, replace "aircraft" with "aerial vehicle"

Page 4, line 24, remove ", including the names of place"

Page 4, line 25, remove "or persons authorized to be subject to surveillance"

Page 4, line 26, replace "certified" with "verified"

Page 4, line 29, after "4." insert "Any imaging or any other forms of data lawfully obtained under this Act which are not accompanied by a reasonable and

articulable suspicion that the images or data contain evidence of a crime,
or are relevant to an ongoing investigation or trial, may not be retained
for more than ninety days.

5."

Page 4, line 29, replace "aircraft" with "aerial vehicle"

Page 5, line 1, replace "aircraft" with "aerial vehicle"

Page 5, line 4, replace "5." with "6."

Page 5, remove lines 6 through 12

Renumber accordingly

2015 SENATE JUDICIARY

HB 1328

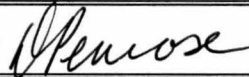
2015 SENATE STANDING COMMITTEE MINUTES

Judiciary Committee Fort Lincoln Room, State Capitol

HB 1328
3/23/2015
25247

- ☐ Subcommittee
☐ Conference Committee

Committee Clerk Signature



Minutes:

1,2,3,4,5,6,7

Ch. Hogue: We will open the hearing on HB 1328.

Rep. Rick C. Becker: Sponsor, support (see attached #1). Two years ago I was before your committee and discussed a very similar bill. You will notice that one thing that is different from last session is that the room is not packed with Grand Forks people and UND people and law enforcement. A lot of their concerns have been addressed in this bill and the way it was amended by the previous committee. The handout (#1) is going to come out in the Grand Forks Herald. I thought it was well written. It had some good points. Section 1 has the definitions, and these were tweaked quite a bit to address concerns by law enforcement and UND; in essence the important aspects of it remain intact. Section 2 is limitations; the gist of the bill is that law enforcement is required to have a warrant to conduct surveillance on a private citizen with a drone. That's the heart and soul of the bill. Of course, we have to get into some particulars and for exceptions. Section 3 does talk about the warrant requirement. There are going to be some specifics to a warrant requirement which are not necessarily apropos to a warrant to search a house. It has a lot to do with data and what to do with the data and where the data is legitimate and where it might not be. Section 4 is the exceptions. Subsection 1) the patrol of national borders was identified as being an exception. The first section deals with the federal patrol of the border is going to have priority over anything that we would want to do in the state anyway; subsection 2) will most likely be the most important exceptions, those are exigent circumstances. That is going to be where there is imminent potential loss of life. You might have a fleeing murderer, a barricaded suspect, armed or potentially armed, the occurrence that happened in ND some years ago, which many people thought was the genesis of this bill, which it actually wasn't, the drone use when someone ran out into a field, armed, they would

not need a warrant to do that because the officers were going in blind after the armed suspect would be put at risk "imminent danger" and therefore they could use the drone readily for the safety of the officers. There are any number of situations which would fall under exigent circumstances; subsection 3) environmental or weather-related catastrophe; subsection 4) is the research testing/education which is important to not impede into the arena of UND Aerospace Sciences and the FAA Test-site. Section 5 does involve the prohibited use for law enforcement: subsection 1) they cannot be armed with any lethal weapons, I'm not in full agreement with, it was any weapon, they did change it to any lethal weapon. In my opinion there should be a nice red line, drones should not be weaponized. When you're not on the ground and you are making the decision and you're separated from the action (depersonalized) whereas if you are going to deploy even a non-lethal weapon on a fellow citizen, you can certainly take a further look at that if you deem appropriate; subsection 2) domestic use and private surveillance, this is intended to prevent law enforcement from circumventing the intent here and going out and getting Joe's Drone Service to do the job without a warrant; Subsection 3) is the surveillance and constitutional rights; it has to do with gathering information at, say a political rally. The thought process there is that drones hovering over a rally would have a very chilling effect on free speech. Is it significantly different than posting officers around the entire perimeter of the gathering, perhaps not? But again you have data storage accumulation on what is being said exactly by whom, etc. That was considered important as well. Section 6 goes into the documentation and what is required for the data that is obtained by the drone flight.

Sen. Luick: In section 5, line 1, talking about lethal weapons being on the drones. What about an instance where you want that for predator control of some sort to monitor or get rid of a rabid animal, varmints.

Rep. Rick C. Becker: I believe that may be taken care of, because it is limited to law enforcement use of the drones. At least my understanding of that is. In last session there were some concerns about limitations for agriculture, for weather, where National Guard may be involved. State agencies aren't in here, at least for the pertinent parts, so it is restricted for law enforcement not to weaponize them. My understanding is that you could use it for varmints as long as law enforcement's not using it with an intended use for humans.

Sen. Luick: Also, on the limitations to privacy and the material and how it is stored if it is recorded materials. What difference does it make if it is done with a drone or done with a camera mounted on the side of a drone, or a

microphone that picks up the speech from a distance away or anything recorded at one of these events? How is it any different?

Rep. Rick C. Becker: There are nuances to it really. It's a matter of the ability of the drones to collect vast and large amount of data at multiple points also using newer technologies that can see or hear through walls. It is a gray area as I mentioned, if you have officers standing around with video cameras on the perimeter is that entirely different. It's difficult to say, but the capabilities of the drone technology and the ability to gather huge amounts of data that they are able to store is quite significant.

Sen. Luick: Also, I was at a US Ag. Conference in Oklahoma where they had multiple states there and they were having the same kind of discussions about the concerns and warrant issues with the drones. Doesn't the FAA control airspace entirely? I'm under the impression that, what they were telling me down there, is that FAA controls everything until you break the plane of an overhead rough for example. So if your drone were to come anywhere underneath of a soffit of a roof, it's your property, you can do what you wish. As far as the FAA is concerned it's open territory above your land, your physical land.

Rep. Rick C. Becker: My understanding is it is 400 ft.

Sen. Casper: Does this, in any way, infringe upon the private use of drones by a private industry.

Rep. Rick C. Becker: It does not.

Sen. Casper: Was there any discussion considering legislation up to this point. I'm looking at section 4, part 4. I'm thinking of the world, where there is an exception for research, education, and training. I'm thinking of law enforcement agency or the public institution that is out doing some research with the drone and the drone is collecting a great deal of data, so I'm a law enforcement agent and something happened near where I know these drones are out collecting data, and I'm investigating a crime that took place and I know UND is doing research there and I know they are flying a drone over and now I want to get a warrant to review all the data that that drone doing research because it may have witnessed a crime. Do you think that will be problematic. I think they would just get a normal warrant and be able to get access to that data and it might not violate, or fall under this exception.

Rep. Rick C. Becker: I did give that a fair amount of consideration because there is that slippery gray area where you can sort of come up with a multitude of reasons to be doing drone flights, which allegedly aren't to conduct surveillance in the hopes that if the drone happened to glance over into Mr. Johnson's yard, who we have been worried about, but don't have enough to get a warrant, but let's conduct a test flight passing by the neighbor's yard. There is a little bit of a gray area.

Sen. Casper: We'll trust the district court judge whether they are going to get the warrant or not.

Rep. Rick C. Becker: I think it is going to be impossible to make it iron-clad and we hope that, exactly what you suggested to be the case, is that they would need to get a warrant and would it be justified.

Sen. Armstrong: One of the problems I had last time was when the case we were talking about during the last session, it was being used on I guess my problem is whether there is a second warrant requirement if there is already a warrant out. If there is a warrant for my arrest and they are trying to arrest me, there is a warrant because I have a probation revocation and they want to utilize a drone in effectuating that arrest, like there is a stand-off situation or office safety situation, I don't think it is in here in the bill. That's what my question is, even in those situations where there may already be an existing warrant for someone, is it the intent of this bill to make sure that they have to get a second warrant to use the drone.

Rep. Rick C. Becker: No. That's not the intent. I think the intent would be that if there is a suspicion that a suspect who has a warrant out for them, is in their cousin's home, we would follow the normal protocols where you have to get a warrant to look into the home. But if you are attempting to isolate and apprehend a suspect for whom a warrant has been issued, I would hope that this didn't require a second warrant.

Sen. Armstrong: I think that could probably be cleaned up in that subsection 2, but the problem is that those might not always be exigent circumstances. There is a distinction and a difference with that terminology. I might try and clean that up.

Rep. Rick C. Becker: Sure.

Ch. Hogue: As I recall this bill from the last session, I think one of the reasons that the Senate defeated it is, in part, because it was regarded as premature. We know of the incidents in Grand Forks County, but have there been other law enforcement agencies in the state that are employing this technology.

Rep. Rick C. Becker: My understanding is that Fargo and Grand Forks have both shown great interest and have purchased them. I don't know that as a fact, but this is what I've read and heard, with the intent that they are conducting training and the intent to use this. UAV's are a wonderful option, a lower cost option and has a rightful place. If I were in their shoes, I would also want to employ, instruct and train to be able to use these. They certainly are in the process of gearing up to use them.

Ch. Hogue: I think the other part of the reason it was opposed was what you mentioned earlier, the Grand Forks, higher education and others were in the process of bidding or attempting to become approved by the FAA as a test site for drones and so do they have any concerns like they did last time.

Rep. Rick C. Becker: I believe their concerns have been addressed. I didn't stay for all the testimony and the discussion afterwards. What was relayed to me by the chairman was an understanding that most, if not all, of the concerns of UND were addressed. They offered amendments which were incorporated into the bill. Much of law enforcement concerns were addressed with amendments proposed by a certain faction. I do know that the Grand Forks Sheriff is still opposed to the bill as it stands now. I believe that most law enforcement is okay with it.

Ch. Hogue: Thank you. Further testimony in support.

Jennifer Cook, Policy Director of the ACLU of ND: Support original bill not the amended one (see attached 2, 3, 4). I would like to speak as a North Dakota citizen because sometimes when we view something through a lens of what we're particularly used to, we fail to see why we should think of it differently. As I pondered the bill, I asked myself, "Why do we care if law enforcement uses drones to conduct general surveillance". Why do I care? If I'm not doing anything wrong, then it shouldn't bother me, right. I recall in the spring of 2009 the flood in Fargo. The flood hit us particularly hard. I was a second year law student in Grand Forks but I lived in Fargo. I spent many of my days away from law school, slinging sand bags to help protect the city I love and live in. One of the aspects of the flood was that multiple times a day I could hear Blackhawk helicopters hovering around the airspace. My military experience

tells me that if a Blackhawk from far away enough that I can't even see it but I can hear it coming, I'm comfortable with the sound of the helicopter in the air. So I had to release all of these biases when I'm thinking about this. The Blackhawk during the flood situation gave me comfort, because while I helped sandbag during the day, when I went to sleep at night, I could hear them hovering around. I knew they were watching the river, so that it wouldn't overflow and wouldn't endanger my family and friends. That gave me comfort, but as I think about this, what if every night when I go to sleep I hear helicopters in the distance, but it's not because they are watching the river, they are watching me. That brings a different perspective to it. I'm not doing anything wrong. I shouldn't have to hear or wonder if there's some type of surveillance going on overhead of my house.

Sen. Armstrong: Let's have a 4th amendment debate here because one of my questions is whenever there is new technology that's what requires specific 4th amendment protection, telephoto lenses, wireless electronic listening devices, these have gone through the history on the 4th amendment. I have a problem with drug dogs and the way they are utilized by law enforcement. That's not a high tech way of doing it; it's very low tech way of doing it. I think the 4th amendment protection in drug dogs is severely lacking. We just had two different US Supreme Court cases on smartphones and I would argue that what you carry on this is some of the most private thing in the world. Why do drones need specific protection? Do we not have confidence that the courts will get it right on the 4th amendment analysis?

Jennifer Cook: The Supreme Court hasn't issued a decision on drones. It is likely they will in the future but how long are we willing to wait for the Supreme Court to decide what they are going to do about drones. Living in a state, such as this, where we are slower than most to embrace new technology and when we do finally embrace new technology we do so cautiously. As Sen. Luick had mentioned previously, drone technology is new, cutting edge and not every law enforcement agency in the state is using it. Instead of being as permissive as to allow law enforcement to use it as they will and trust that they will do what is proper under the 4th amendment, the legislative body should give them guidance. I think that the original version of the bill does so.

Sen. Armstrong: I get concerned when we start parsing out certain sections of the law, like drug dogs, smartphones, drones, etc. I think we have to be cautious that we don't start parsing out 4th amendment issues and let the 4th amendment do what the 4th amendment supposed to do. I don't always have complete and utter trust in law enforcement either. I think that was an

occupational hazard for what I did for 10 years of my life, but I do tend to trust the courts and I tend to trust them to get it right as it moves forward.

Jennifer Cook: I agree with your sentiment. I also think that as I said before, the courts are a remedy for a violation that has already taken place. Why would we be so permissive with new technology that we don't have rules? I suggest that we move slowly and take an expansive view of the 4th amendment and when we see the impacts of what drones can do, if they are used accordingly with the 4th amendment, then perhaps we can look at allowing a more permissive stance. As a starting point I think we shouldn't be so permissive.

Sen. Armstrong: If we are going to talk about a broad and expanse stance, do we need to add the exclusionary rule to this bill. As I read it, there are prohibitions on it but it doesn't tell you what the penalty for violation are.

Jennifer Cook: That's a good point. There was a civil penalty section in this bill before it was amended by the House and it was removed. The way the bill is written already deals with an exclusionary rule; in fact it deals specifically with warrants in section 2, I think you could look at it that way. I'm talking about prior to even obtaining a warrant that drone should not be used as automated police officers.

Sen. Casper: Under the legislation as amended, as it stands before us, law enforcement could use a drone, and then they would have to have a warrant to make the evidence admissible in court, where under your suggestion here, they'd have to go and get a warrant to use the drone in the first place. Is that correct.

Jennifer Cook: As I understand it, yes. We're asking that a drone not be used in that situation. When you use a drone, normally law enforcement to build probable cause to get a warrant to search property would use normal, traditional law enforcement techniques. They would conduct human surveillance; meaning that they perhaps stake out your house and with a drone because you have a camera equipped with amazing technology you can watch an entire city at one time. If you don't have a reasonable, articulate suspicion or probable cause to be watching for specific wrongdoing you can look out and see where there might be criminal wrongdoing and use that and go back through that imaging to then take traditional policing procedures to form probable cause and that's the concern; we're watching people who would be innocent for suspected criminal wrongdoing. The technology is so amazing

the imaging is so fine and definite, that you are looking at something that a human wouldn't normally be able to do.

Sen. Casper: If I look at line 1 on page 2, section 2, information obtained from the operation of UAV may not be used in an affidavit of probable cause in an effort to obtain a search warrant. I'm reading that as saying that the Cass County Sheriff can't fly UAV over an area where they suspect wrongdoing and then collect data there and bring that to the court for the purposes of obtaining a warrant to go in and search through further drone surveillance or go search the property. Is that correct.

Jennifer Cook: When I first read the amended bill, I thought well this doesn't look so bad. It seems like this does what we want it to do, but when you read it further, it is a bit confusing and it's not clear. Basically, it means that in order to bring evidence procured from a drone into court you have to have a warrant, but you don't have to have the warrant to fly over wherever.

Sen. Luick: You were talking about the differences between your personal type of situation with the Blackhawk helicopters, etc. but I didn't quite get the connection there because I think that having those helicopters at night, no matter what, would be a comfort in that situation. We are all being recorded more so all the time, day in and day out. It's being mandated, I believe, nationwide that law enforcement have cameras on. We just passed a bill here the other day that had some information in that it has some kind of bearing upon what is happening here. How do you feel about the information that is being recorded on those cameras vs. the information being recorded on the drone cameras? Can't they be treated equally?

Jennifer Cook: In fact, as I thought about the relation between those two bills I think the difference is that a police body camera whether it be a body camera or even a dash camera in the patrol vehicle captures only what the officer sees and who the officer interacts with in a very confined area. As the ACLU, we still do have very deep concerns about the images that are captured by body cameras in private places. In fact, I believe that there should be strict controls with regard to those images, how they are retained, and how they are disposed of. In response to your comment about the Blackhawk helicopters and how they would be a comfort either way, I can see your point; however, I would counter with this, if you felt that you were always being watched and you can hear helicopters and if you look at the technology of the drone, many of the common drones that law enforcement could use can fly up to 19,000 and they can stay aloft for more than 19 hours. That's an incredible amount of

information that they can capture. I think that, as a society, yes we are moving closer to a world in which we are watched all the time. I'm not sure that we should be so accepting of that. There has to be a balance between what individual privacies that you are willing to give up and your security but it has to be a very careful balance; especially when we have new and emerging technologies, we have to consider those very carefully.

Ch. Hogue: I wanted to clarify your testimony, you said you wanted lines 16-21 on page 1, of the original bill restored, is that correct.

Jennifer Cook: Yes.

Ch. Hogue: I think you gave the committee a version 2000 of the bill. Is this the original or was there something before it.

Jennifer Cook: It's my understanding that the copy I gave you off of the legislature's website and it was the original bill that I was tracking.

Sen. Casper: I looked at the original bill on here dated the 13th of the first reading and it referred to Judiciary as the 2000 version.

Ch. Hogue: So it was already the 2000 version.

Sen. Grabinger: I don't want to take away opportunities for law enforcement to find crime and stop crime. In saying that, I look at this and hypothetically, an individual that they think may have stolen property in the backyard through the means at will, they can't tell. So they want to fly over and see if it's in a backyard, a stolen motorcycle for example. With this, they would have to get a warrant; they'd have to hire another law enforcement agency because they can't hire private without the warrant. Why do you want to take away that opportunity for law enforcement to utilize this technique. In the way I look at it, I think of drones as another way for law enforcement to advance their techniques, such as high powered binoculars, etc. There is an effort to try and prevent crime and stop crime and that's why they do that. Why would we want to take away that opportunity.

Jennifer Cook: We all have an interest in law enforcement being able to do their job exceptionally well and I think we want them to be able to use the tools that are well within their purview to use. However, I would advise caution when it comes to drones because they are not narrowly tailored. They can literally suck information as they are moving to the target area, even if they

have a warrant, they can suck information from city blocks, miles around and that information is captured and stored and there are tools that law enforcement can use already that the courts have decided still protect an individual's right to privacy, but allow law enforcement to do their jobs effectively. Here, we don't have such guidance. I think it's a balancing act. There was testimony on the House side from a law enforcement official during the testimony. Essentially he was asking why he has to get a warrant, most likely we will get a warrant but we do it anyway so why should we be told that you have to do it. Well the reasoning is this. We have checks and balances in our government; the judicial system, the legislative body, and the executive branch, and the legislative body makes the rules that the judicial system enforces. Law enforcement is a tool of enforcement; it does not make up its own rules; that's for this legislative body to decide.

Sen. Luick: Hypothetically, you have a drone flying over and this property over here is the targeted area and you mentioned that I can get information from a larger area. What would your opinion be of something like this? Let's say the efforts were put on this over here but this information gathered over here, where a crime was being committed and we're going to make this personal. It's going to be your family member or even yourself. This particular individual down there has been very shifty and has not been able to get caught, but he's raping an individual. The information is on the camera, but your instance of not being able to use that information, how do you feel about that.

Jennifer Cook: From the ACLU's perspective I think that they would say, that if you don't have a warrant specifically targeting the specific place in which you've requested in the warrant that you are going to look at with this drone camera and there is criminal activity going on outside that realm that you should not be able to look in that area.

Ch. Hogue: Thank you. Further testimony in support.

Sara Sen. Nelson, Journalist, Washington DC: Support (see attached #5).

Ch. Hogue: Thank you. Further testimony in support. Testimony in opposition.

Thomas Kenville, Grand Forks: Opposed (see attached #6).

Ch. Hogue: Regarding law enforcement use of the drones, do you have knowledge how law enforcement in other parts of the country are using unmanned aerial craft.

Thomas Kenville: It's very difficult no matter who you are today to get in the air, because of FAA's rules for safety. It has nothing to do with data; it's very difficult and we are working very hard to get into the air no matter if you are a private citizen or law enforcement. I do know that it is growing but there hasn't been anyone who gets a lot of airtime; even our own sheriff's department in Grand Forks County. Am I worried about them spying on me, I don't care if it makes noise or not. I want my privacy but I think this is going to save lives and create jobs. I think we have laws in place to protect me.

Sen. Armstrong: The FAA already has rules, but the FAA doesn't do 4th amendment analysis.

Thomas Kenville: No. But you have to get into the air to run the drones.

Sen. Casper: Is this going to infringe upon industry in the state, and Rep. Becker said he didn't know. Can I assume from your testimony that you see that differently.

Thomas Kenville: Yes. When I was asked to testify I was sitting in a lawyer's office across the street from the White House. The company that I helped bring here, said the reason they are here is because of our great leadership and how we're open to new industry. The other states that are competing with us, some of them have the new rules and it's another level to go through to get to airspace. The airplanes that are going to be built in Wahpeton could be used by our law enforcement. Are they going to order as many, are they going to construct as many, it's going to hinder growth. Do I believe 10 years from today there might be some new rules to help with the 4th amendment, sure. I just think it is premature right now.

Sen. Casper: There's nothing in here that says a private company can't collect data or fly. Depending on how we might amend this bill and the suggestions of the ACLU, we're really saying is that law enforcement can have a drone and use them. But if they're going to collect data and use that in a court proceeding against someone then they need to have a warrant to do that. I don't know what kind of limiting effect that would have on those companies being able to expand and create sales in the state. Law enforcement will collect data the way they always do and follow procedures of

getting a warrant to use the evidence in court. Since they do that now, I don't see how getting the information from the drone's surveillance will change anything. I don't know if it would keep them from buying them. Have they told you that they aren't going to use drones if this bill passes?

Thomas Kenville: It isn't in this specific case; it just adds a layer of red tape that our industry already has plenty of. Again, this has been a national effort to edit a couple of years ago. It popped up in every state immediately. I just think that the time is yet to put rules in place. We have good checks and balances. We're trying to be frugal with the amount of money we spend to bring these industries here, why have additional red tape. That is where I am coming from.

Ch. Hogue: Thank you. Further testimony in opposition. Neutral testimony.

Bruce Burkett, ND Peace Officer Association: I want to bring you through the history of how the bill got to congress (see attached #7). The initial bill was presented in the House around February 13th. Law enforcement was there and opposed the bill by every speaker that got up. The basic reason was that most of the time we're talking about open fields. We're not talking about getting into places with a drone or another device that is protected or where there is an expectation of privacy. The committee in the House, after hearing our objections to the bill, put it back on us. Our law enforcement committee is made up of all of the different entities of the ND Peace Officer Association and on Friday we have a meeting and all of the entities have a representative at the table. We were asked to redraft the bill, and the language you see there is 85% of our language, with the exception of two matters. I believe Rep. Koppelman from House Judiciary provided an amendment that addresses the things that were left out. The part that got left out happened when it got to Legislative Council when they drafted it. If you look on page 2, after line 1, the punctuation disappeared and they left out two full lines that should have been in the draft that we gave them. The other area is on page 3; section 3, where we had removed a whole section and the amendment that should have been in the bill as it was drafted should have included our other two amendments. We had indicated to the House Judiciary Committee, that if those two pieces were put back, our committee would stand neutral this time. It does set out requirements of use for UAV's. The requirements there are nothing more than good housekeeping. If we are going to be doing it for the records and what we keep, how we keep them. The one area that is different in there, if you look at the search warrant requirement and the items that have to go into that document, it's more inclusive to items that we would normally not have to slide

into that affidavit or search warrant. I have completed a number of those affidavits and I know what needs to be in there to satisfy a judge to give the authorization. I am also a pilot; I have 11,000 hours of flight time. The other item I passed out is what the FAA is doing to promulgate rules in the implementation of drones for all of us. It's obvious the commercial operations and the authorization that Grand Forks has got, is under a certificate of authorization. It's different, it gives parameters that can be used to use that drone and they have to follow the federal rules to get that license. I assume down the road, commercial operators will be in the same boat. If someone wants to use it for wildlife law enforcement, wildlife survey work, and is in the sights of other agencies in what they could use the drones for. A commercial operation is certainly unlimited. Certainly those kinds of opportunities should be investigated. Most of the proposed rulemaking by the FAA is on the website and it has 48 pages of rules; it differentiates and I gave you 10 content pages of things you can prove when you have time. Those are all matters that are coming down the road. They address Ch. Hogue's comment earlier that we might be a little premature in some of the areas that we want to regulate.

Sen. Armstrong: Do we need to exclude Game and Fish because it is a law enforcement agency; they do a lot of non-law enforcement activity.

Bruce Burkett: Correct, 80% of that agency is basically a chamber of commerce type of operation.

Sen. Armstrong: Is the bill, as it is currently written, going to exclude them from doing herd counts or something with the use of the drone.

Bruce Burkett: You would probably have to get a certificate of authorization through the FAA anyway. It would be through rules that they come up with now.

Sen. Armstrong: Maybe because they define law enforcement and not law enforcement activity. I'm just wondering if this bill is moved forward, if we do have to make exclusion for Game and Fish. I am assuming that it could be a warden; they are in dual roles as well. During the off season, you are out doing herd counts, etc.

Bruce Burkett: Most of those types of activity are done by the biologist now. When I came on several years back, 40 years ago, that's the role the warden would be doing. In this day and age, no. The pilot warden might be out doing

another activity but he'd be in a manner airplane. Anything that this drone can do, I have done in my own airplane.

Ch. Hogue: Further neutral testimony relative to HB 1328. We will close the hearing.

2015 SENATE STANDING COMMITTEE MINUTES

Judiciary Committee Fort Lincoln Room, State Capitol

HB 1328
3/31/2015
25634

- ☐ Subcommittee
☐ Conference Committee

Committee Clerk Signature

Memo

Minutes:

1,2

Ch. Hogue: We will take a look at HB 1328. He explained an amendment he had written up (see attached #1 which was not attached to this bill). This bill is the drone bill that puts restrictions on the use of drones for law enforcement and law enforcement agency is a defined term. We should talk about the bill. The one thing that I like about the bill is too often the legislature abdicates its responsibility to say what is an unreasonable search and seizure. A lot of states do, but this is another area where ND just leaves it up to the courts. We always say it's the constitution. Well, what is an unreasonable search and seizure? If we don't define it, the courts do. It is still a legislative responsibility to say what constitutes an unreasonable search and seizure under either constitutional law or statutory law. With my amendment, we are trying to fix a problem that Pol. Subdivisions did not fix, with respect to stolen property. They had a bill in their committee and it passed out 6-0 and law enforcement wanted the power to give back stolen property instead of having to go before the magistrate. It's a purse, children's bike... why do we have to go to the judge to get permission to give it back. The statute, 29.01.20 is the one they wanted to repeal and of course, there are more goods that are alleged to have been stolen or embezzled than just Johnny's bicycle or Aunt Jenny's purse. There are large commercial properties, equipment, rolling stock, sometimes there is a dispute between the lender and the borrower; between the lessor and the lessee; there are just of commercial disputes out there about the ownership of some property. What didn't make sense to me nor did it make sense to Sen. Armstrong who stood up and challenged the 6-0 Do Pass, was that this repeal, this entire statute. I am trying to fix a problem that police officers perceive, which is a) technically we're breaking a law if we give the kid his bike. My amendment proposes is an exception to the general rule in the statute, except for consumer goods as defined in section 44-09-02.1Y when property alleged to have been stolen or embezzled comes into the custody of

the peace officers, the peace officer shall hold it subject to the order of the magistrate. So consumer good are everything that you buy that is meant to be used by a consumer for their personal use, like a purse, cellphone, a bicycle... etc. It has a distinct meaning from commercial property, property used in a trade or profession. That's the purpose of the bill.

Sen. Armstrong: Would a car be a consumer good.

Ch. Hogue: It depends on how it is used. If it is your personal vehicle, that is a consumer good. If it is a truck that you use in your trade or profession, it's not.

Sen. Armstrong: The only reason that I bring that up is because when there are break-ups and payments, I don't know if it would end up in court. I've seen one in a criminal situation, but that's one of the areas where disputed ownership comes into play.

Ch. Hogue: The nice thing about that is that they are titled, and if there is a lienholder on it, it's indicated on the title, so the police officers know how to do that. If it is a Jim or Sally Smith or Jim and Sally Smith, now you're right in the middle but that is when you should be saying "I don't know whose property this is, I paid for it, but I signed the contract."

Sen. Armstrong: You're saying maybe it shouldn't be charged as a crime and figure it out civilly.

Ch. Hogue: That's another option. The bottom line on this is that the police force was proposing to repeal 29-01-20 and 29-01-21, I think under the assumption that they were obsolete provisions and so this is my attempt to try to fix it. Obviously, if we do not pass HB 1328, it doesn't get fixed, but that's the way it goes. I can't put this amendment on spousal support.

Sen. Luick: I am hoping to kill this bill.

Sen. Casper: There's a bill that we passed out dealing with the handheld raffle tickets. I wouldn't mind putting an amendment on too; to bring that back.

Ch. Hogue: If they killed it we have no way of bringing it back.

Sen. Luick: My concern about HB 1328 at this point in the game, I think we are trying to jump into this a little too early. I am very concerned about that.

There are businesses that are starting up in North Dakota that needs some leeway until the FAA gets their act in order to try and figure out where this is going.

Sen. Grabinger: As one of those six, who appreciates you trying to fix this little problem? Do we have any other bills left in political subdivisions that we could put this amendment on?

Ch. Hogue: We have Rep. Brabundt's bill.

Sen. Armstrong: We passed that bill that we're holding and the House Judiciary passed the companion bill, SB 2027, 13-0 yesterday, so there really isn't a need for both of those bills to be floating around. We could reconsider that bill. The bill we passed out yesterday is identical that they just passed out in the House.

Sen. Grabinger: I agree with you. I want to do something to take care of that issue with the peace officers. I don't think it's right. Right now, the officers, if they turn little Johnny's bike to him after Billy stole it; they are actually breaking the law as it's written and they have a problem with that. I agree with you. I think it is admirable that we fix that. As far as HB 1328, I agree. I think we are overstepping.

Ch. Hogue: Maybe we should hold this until we see the fate of SB 2027.

Sen. Armstrong: I am going to support HB 1328, because regardless of what the FAA does and whatever business start-ups are going on, and last session I thought the bill was too broad and also gave some 4th amendment issues. The FAA is not going to deal with the 4th amendment issues. That's not that purview, that's not what they do. They are going to have regulations based on what the FAA regulates. I think bill has been crafted in a way that protects the privacy issues and should not affect the business agencies involved in what is going on. I am not excited about subrogating our 4th amendment rights for the interest of economic enterprise is the best way to put it.

Sen. Grabinger: My reason is that I have issues with the bill and concerns for law enforcement. For example, on page 2, lines 1 and 2, that first paragraph, "Information obtained from the operation of an unmanned aerial vehicle may not be used in an affidavit of probable cause in an effort to obtain a search warrant". I struggle with that. As I look to the hypothetical of something stolen in the backyard and we fly a UAV over it to see if it is in the back yard,

because it is a fenced in backyard to see it there, then we should be able to get a search warrant and take care of it. I think this could hamper law enforcement and I don't want to do that.

Sen. Armstrong: My response to that would be that they shouldn't be flying a drone over someone's property without probable cause, just to see if they have the stolen bike just because they can. I would say that Rep. Koppelman's amendment deals with some of those issues right there; if we are going to offer that amendment. Because that deals with exactly what Sen. Grabinger was talking about, unless it was obtained under the circumstances described in subdivision a or b, of subsection 1 or was obtained through the monitoring of public lands or international borders; I don't remember what (a) or (b) is. Oh, that is just pursuant to the search warrant or one of the exceptions.

Ch. Hogue: The ACLU supports this bill.

Sen. Armstrong: If you don't like the bill as written, these amendments will tighten it up a little bit. If that is your position, do you want it ugly so it doesn't pass or do you want to make the bill better before you vote against it? On page 2, line 2 language is good in the amendment. It says "information obtained from the operation of an unmanned aerial vehicle may not be used in an affidavit of probable cause in an effort to obtain a search warrant" unless the information was obtained under the circumstances described in subdivision (a) or (b) of subsection 1, which lists (a) warrant or an exception to the warrant requirement or was obtained through the monitoring of public lands or international borders. I think I agree with page 3, line 27. After "Surveillance of the exercise of constitutional rights." I don't think you need the rest of that section. I think it is duplicative. It may just add "unless the surveillance is otherwise allowed under this chapter. I think the amendments tighten up the bill. I move the amendments .03001 by Rep. K. Koppelman.

Sen. Grabinger: Second the motion.

Ch. Hogue: Voice vote, motion carried. I'd like to wait with my amendment until I know what happens with the committee's recommendation. I'm torn on this bill. I hate to get in the way of business on the one hand, but on the other hand I hate for the legislature to always be silent on areas where we should be exercising some leadership.

Sen. Armstrong: This isn't just applicable to drones, but that is what is in front of us. The problem with deciding the 4th amendment in the courtroom is that there is always a guilty defendant sitting next to you, with 100 lbs. of marijuana or 5 lbs. of meth. In these broad policy determinations of what the 4th amendment protects, it's easier and I agree with what you are saying, is that it is something the legislature should be wading into more often because we can have a discussion in broad stroke hypothetical as opposed to have a guilty defendant sitting next to you in the courtroom all the time. How you define the 4th amendment is easier to do in this body than the courts. I think the question of privacy is going to come up more and more often whether it is drones or surveillance or cameras on the streets. In our technological age, privacy is going by the wayside. I don't have a problem with this bill being here for that reason.

Sen. Luick: I am getting feedback from concerned citizens like Mr. Kenville, who works very closely with the UAV and trying to get more into the state of ND through UND and Grand Forks. There are a lot of efforts being put into place to try and get more of this technology and business opportunities brought to the state; not only his concern but the people that he works with is that we start regulating this at this point before FAA comes up with their rulings on the federal level, we are maybe going to harm the industry and it's unwarranted at this time. I am hoping that others will vote my way. I hope there is enough concern to just slow it down for two years.

Sen. Casper: I am torn by this bill. I don't quite buy the business argument. I asked some questions in regard to that during the hearing and I think the UAV industry in the state is great and I think it is expanding. I think they are doing great things. All we're saying here is that if someone's flying a drone and they are collecting data, and we only use that in a criminal case, we're acquiring that there is probable cause, and we're not allowing them to willy-nilly fly drones all over the state, looking in search of someone committing crime without them having a warrant; which would require them to have probable cause. I don't see the tie-in to how it is detrimental to business. The only argument that you could say, the bottom line would be that law enforcement is going to purchase less drones, because they can't now, under this law, fly drones wherever they want to see what anyone is doing. I don't feel that is good policy, and probably unconstitutional. I have no problem going and talking to the folks that are in favor of the UAV industry in our state. This could happen without us passing this law anyway. They could be selling drones to policy departments who would then go out and use them and then find out all the data that they collected was inadmissible because a judge or

the ND Supreme Court can end up ruling that way anyway. Correct. All we're saying is that we are using these in the law enforcement context; we have to have a warrant or probable cause; there are some exceptions there, and there are always exceptions with regard to probable cause and warrants. I think the typical exceptions.

Ch. Hogue: This bill is so interesting because the cops, the police love whiz bang stuff, they love technology. I can see a lot of law enforcement wanting to go out and buy these things and use them without any restrictions. As the U S Supreme Court said, the police forces are a competitive group and they like to catch the bad guys. Here is a tool that would help them and they will use it in any way that they are authorized to do so by either the courts or the legislative body. My major policy issue is that I feel like the legislature should, at some point, say what a proper use of this is. We don't in other areas. Sen. Armstrong is right, the problem with deciding what is a reasonable search and seizure, when it comes before the courts, the courts are like okay that guy is guilty, and do I want to let him off to uphold some constitutional principle. No, they always find a workaround. The statutory procedure is better because you set out the rules of the game up front. I am torn by it. We had a broader bill last session and I opposed it, and I said that we were just being paranoid. This is premature, but of course, the industry has come a long ways since last session. By the way, everybody I've talked to, the best drones are made by the Chinese and you can buy a Chinese drone for under \$500.00 and you can actually mount a camera on it and works pretty good. You can look over and see if Johnny stole the bike. It's not inaccessible technology any more.

Sen. Armstrong: The other thing is the last session bill was essentially a drone warrant bill; like for any circumstance where you used a drone, you had to get a warrant, to effectuate an arrest, officer safety, etc. This is going to what Sen. Casper said; this is for the investigative portion of law enforcement. You can still use it for officer safety, the weather related catastrophes, the exigent circumstances that language is in this bill. This is definitely not the same bill we had last session. This is tightened up quite a bit. It says that for investigative purposes before you use a drone, you have to have probable cause. At the end of the day, that's what this bill says for four pages.

Sen. Grabinger: How far does this go? The game warden, sitting on a hill, half a mile away with a high-powered telescope, looking at some people in a boat breaking the law. Is there any difference between that and flying a drone over them and seeing them break the law? It seems to me that we're talking about the same thing here. To say that it is okay with the high powered

telescope looking at the boat and viewing that, that is okay; but with the UAV no we can't use it unless we have a warrant.

Sen. Casper: I think the answer is that it comes down to sort of the jurisprudence of them being in a public place. The other question is if you are using it, could that be seen beyond the human eye. I look at this you need a warrant and probable cause before you kick somebody's door in and go into the house because you think they might have something in there that is illegal, you should have probable cause before you fly the drone over their backyard, because the way to get to the backyard is to kick the door in and go into their house.

Sen. Luick: In response to Sen. Grabinger's comment about the high powered telescope or camera. You can look at it from a helicopter viewpoint also. It is legal for them to sit up in a helicopter, 400 ft. high and get the same information that they can get with a drone, but it's illegal to get it with a drone because it is unmanned. That doesn't make a lot of sense to me.

Sen. Armstrong: I was actually going to use that as the analogous; it's more analogous to use an airplane or a helicopter. The huge difference from those two things is that it is incredibly expensive to fly and one is cheap to fly. That is the difference and the reason it is different is that law enforcement has limited budgets and game wardens use airplanes all the time; but a drone is significantly easier and cheaper to fly and it also can go places where an airplane can't go. We all talk about the 400 ft. but a drone can fly (we'll have to see what the FAA's regulations do, size requirements, etc.) in areas where planes and helicopters cannot. I will say that was the speech I gave on the Floor two years ago. Why are we parsing out specific pieces of technology? The 4th amendment should apply somewhat equally to all pieces of technology. The difference with drones is that they are highly technically advanced and incredibly efficient to use compared to other forms of technology.

Ch. Hogue: The difference between helicopters, which are very expensive to fly, or a drone is if police were just sending up helicopter just out looking for criminal activity, I think you would see an effort to regulate that as well. I think a lot of it is practical dollars and cents. That high powered scope, you're sitting in a public place, on a lake. Secondly, the police officer can visually observe and he's supposed to be looking for that activity. Some drones have the capability to scan everything that happens. Can they see remotely as the

drone is going over the backyard? I know they can in military applications but I don't know about the ones out in the public.

Sen. Luick: I think that anything that you can put on a helicopter you can put on a drone, even thermal imaging. If you can do it on the land, you can do it with a drone. If you want to compare the cost of a helicopter to a drone or whether they are efficient or not is fine. You can go back and look at that in any industry. In agriculture we still have the regulations of how we put on chemicals, whether it is by hand sprayer or a \$400,000 spray outfit. It doesn't matter; the law is the law about what can get applied. It shouldn't matter whether that information is being gathered by a \$1,000 piece of equipment or a \$200,000 piece of equipment. If you send your highway patrolman out with a 1965 Ford pickup or a 2016 Cruiser, they could be doing the same job but now because they are in a more expensive vehicle that shouldn't limit the amount of information that they can gather. To me, whether it is a helicopter or a drone, that information gathering technique shouldn't make any difference.

Sen. Casper: I just want to be clear. We're saying that what is viewed from a helicopter or an airplane, with those certain requirements on the height that really applies to page 2, line 1-2. Law enforcement can use information gathered via helicopter or airplane, which meet certain requirements to create probable cause in the warrant process. So with this, we would need probable cause before the drone can be used. Don't planes and helicopters have to have probable cause too, the way the drones would in some cases.

Ch. Hogue: It goes back to my point. It is whatever the courts have been saying. So if we say nothing, then the courts will decide these issues. If you are up in a plane, it's in plain view because you're in a plane. We could say that is impermissible too. You would think that someone would say that wasn't a good use of resources for the police to be going up in the air with a helicopter looking for criminal activity when all you have to do is drive a patrol car around, no need to get up in the air.

Sen. Nelson: I wanted clarification. I wasn't here for the hearing. How does this relate to the Happy Hooligans in Fargo; they were reassigned duties that are now flying drones into Afghanistan and other places, is there anything in here that will restrict anything that the military is doing.

Ch. Hogue: No, we should take a look at the definition of law enforcement but I don't think the National Guard would fit into that.

Sen. Casper: Aren't law enforcement officers required to get probable cause or warrants for surveillance done on farmlands and part of military operations, but maybe someday.

Sen. Armstrong: National Guard doesn't do domestic law enforcement. Even if they are a state run agency, they would still have the ability to do this for military reasons.

Ch. Hogue: They do some, they do what is called drug interdiction where they will actually fly the plane but there are separate agents that do all the visual observation, which was a real interesting issue but I don't think this impinges on the Happy Hooligans.

Sen. Grabinger: It seems to me that we may be targeting these UAV's for law enforcement and their use of it. I do have a concern that these UAV's could be used for committing crimes and should we be looking at this regulating them or putting penalties in place if they were used to commit a crime, instead of trying to basically thwart the efforts of law enforcement and their use. The issue of the UAV landing on the White House lawn; that's very scary on how these could be used to commit crimes, start fires, burn houses; these could be very easily used in criminal actions. It would be tough to catch them. Therefore, I am wondering if we should be looking at a law that brings out penalties for the use of these in the commission of a crime.

Ch. Hogue: We passed a bill in Energy and Natural Resources because somebody brought us a bill that if you are philosophically opposed to hunting, you could use a drone to scare the game away, whether it's big game or birds. So you see a party out hunting, and you use the drones to scare the game away and we just passed that bill out of committee about a month ago. When it is brought to the legislature's attention that this is a way that the technology is being used, we said no, you can't do that.

Sen. Armstrong: If there is a crime committed, there is a crime committed. There is already a penalty in place as opposed to what you use to do it. I don't agree with the characterization that this bill is thwarting law enforcement. I think the bill last session was to some degree. It was doing something different. Whether they are completely happy with it or not, I know they were involved in the re-write of this process and they were consulted at every step of the way. You say thwart law enforcement and I say protect 4th amendment privacy rights to some degree or another. They still have the capability to

utilizing these in many aspects of law enforcement, just not on blank fishing expeditions without probable cause.

Ch. Hogue: The one thing we haven't brought up and somebody brought it up during the hearing was the folks from Grand Forks really didn't want this because they were in the bid process to get their site approved and they thought that even though the bill doesn't affect them, they didn't want any headlines about North Dakota adopts bill to limit drone use. They just wanted to make sure that ND had a clean application and we were approved.

Sen. Luick: I think that the stigma is still there hanging in the air right now today. There are other things that are being considered for ND because of the weather, because of the weather, because of the open space, because of the business climate and I don't think that it was a wonderful idea last session, but I don't think we are out of the woods yet.

Sen. Casper: To reiterate the point of Sen. Armstrong's last statement, when it comes to limiting law enforcement, we may be limiting law enforcement but the only limit we're putting on them is that they can't fly drones where ever they want, whenever they want, looking at whatever they want. Basically we're limiting them only to the extent that they can't say let's go buy four \$500 drones that run on 12 hour shifts and we will always have two flying over the city of Fargo at any given time monitoring people. Then we have to hire two people to be constantly watching those videos to see if anything, anybody is doing anything wrong ever. That is the only limitation and the next point is in regard to the businesses. I think we're on the cutting edge of drone technology in this state, but all we're doing is saying that law enforcement has to have probable cause when using a drone. They are required to do that with all other kinds of searches that they do. What is the big deal if they are doing it with a drone? I don't think the folks who are looking at buying drones with regard to weather, agriculture, etc. are going to say, I'm not going to buy this drone because it may view something that a police officer would then come and want to look at it, and they are going to have to have probable cause to use that in a courtroom. I think we're talking about 1% of 1% of the use of these products. I don't see it having a detrimental impact other than some people trying to make this look like they were purposely out there doing something anti-drones. I don't think we are. We're just saying probable cause.

Sen. Luick: Is there a problem today; are there cases where drones have been identified as being an issue with 4th amendment or any type of privacy issues or cases where it has evolved into a problem. I have not heard of any.

Ch. Hogue: I think in the last session we knew that the Grand Forks police or sheriff was using a drone. It wasn't to go out and just sort of look for criminal activity. Generally, I think there was a specific reason, I don't know if it was a missing person.

Sen. Armstrong: There was a siege situation where they used the drone to fly over to find out if the people were armed and it was for law enforcement protection and one of the reasons that I had a problem with the bill last session was that they would have had to get a specific warrant for that. It was a drone warrant bill, and I thought that was ridiculous. If it is a situation where you can protect officers and the defendants effectively, I think this drone use would be completely legal in this bill. You could use a drone in this situation like it was used last time. I think that's the distinction between the investigative portion of law enforcement and the effectuating the arrest and the imminent portion that is excluded in this bill. I want to stress that because I think when law enforcement is using them to protect their officers or to effectuate an arrest, or in that type of situation, they should be completely able to do so. When law enforcement is doing things that have any danger associated in that, they should be able to use whatever technology is available to protect themselves and the public. It's the investigative portion that we're trying to put some limits on in this bill.

Sen. Luick: I move a Do Not Pass as amended.

Sen. Grabinger: Second the motion.

2 YES 4 NO MOTION FAILED

Sen. Armstrong: I move a Do Pass as amended.

Sen. Casper: Second the motion.

4 YES 2 NO 0 ABSENT DO PASS AS AMENDED

CARRIER: Sen. Casper

3/31/15
JK

PROPOSED AMENDMENTS TO ENGROSSED HOUSE BILL NO. 1328

Page 1, line 1, after "of" insert "an"

Page 2, line 2, after "warrant" insert ", unless the information was obtained under the circumstances described in subdivision a or b of subsection 1 or was obtained through the monitoring of public lands or international borders"

Page 3, line 27, after "the" insert "lawful"

Page 3, line 27, after "rights" insert ", unless the surveillance is otherwise allowed under this chapter"

Page 3, line 27, remove "A state agency may not authorize"

Page 3, remove lines 28 through 30

Renumber accordingly

Date: 3/31/2015
Roll Vote # 1

2015 SENATE STANDING COMMITTEE
" VOTE
BILL/RESOLUTION NO. 1328

Senate Judiciary Committee

☐ Subcommittee

Amendment LC# or Description: Koppelman Amendment (att.# 2)

Recommendation: ☒ Adopt Amendment

☐ Do Pass ☐ Do Not Pass ☐ Without Committee Recommendation

☐ As Amended ☐ Rerefer to Appropriations

☐ Place on Consent Calendar

Other Actions: ☐ Reconsider ☐ _____

Seconded By

Motion Made By Sen. Armstrong

Sen. Grabinger

Senators	Yes	No	Senators	Yes	No
Ch. Hogue			Sen. Grabinger		
Sen. Armstrong			Sen. C. Nelson		
Sen. Casper					
Sen. Luick					

Total (Yes) _____ No _____

Absent _____

Floor
Assignment _____

If the vote is on an amendment, briefly indicate intent:

Voice Vote: Carried

Date: 3/31/15
Roll Vote # 2

2015 SENATE STANDING COMMITTEE
VOTE
BILL/RESOLUTION NO. 1328

Senate Judiciary Committee

☐ Subcommittee

Amendment LC# or Description: 15.0259.03001 04000

Recommendation: ☐ Adopt Amendment
☐ Do Pass ☒ Do Not Pass ☐ Without Committee Recommendation
☒ As Amended ☐ Rerefer to Appropriations
☐ Place on Consent Calendar

Other Actions: ☐ Reconsider ☐ _____

Seconded By

Motion Made By Sen. Luick Sen. Grabinger

Senators	Yes	No	Senators	Yes	No
Ch. Hogue		✓	Sen. Grabinger	✓	
Sen. Armstrong		✓	Sen. C. Nelson		✓
Sen. Casper		✓			
Sen. Luick	✓				

Total (Yes) 2 No 4

Absent 0

Floor Assignment _____

If the vote is on an amendment, briefly indicate intent:

Motion Failed

Date: 3/31/15
Roll/ote # 3

2015 SENATE STANDING COMMITTEE
VOTE
BILL/RESOLUTION NO. 1328

Senate Judiciary Committee

☐ Subcommittee

Amendment LC# or Description: 15.0259.03001 04000

Recommendation: ☐ Adopt Amendment

☒ Do Pass ☐ Do Not Pass ☐ Without Committee Recommendation

☒ As Amended ☐ Rerefer to Appropriations

☐ Place on Consent Calendar

Other Actions: ☐ Reconsider ☐ _____

Seconded By

Motion Made By

Sen. Armstrong

Sen. Casper

Senators	Yes	No	Senators	Yes	No
Ch. Hogue	✓		Sen. Grabinger		✓
Sen. Armstrong	✓		Sen. C. Nelson	✓	
Sen. Casper	✓				
Sen. Luick		✓			

Total (Yes) 4 No 2

Absent Ø

Floor Assignment Sen. Casper

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE

HB 1328, as engrossed: Judiciary Committee (Sen. Hogue, Chairman) recommends **AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (4 YEAS, 2 NAYS, 0 ABSENT AND NOT VOTING). Engrossed HB 1328 was placed on the Sixth order on the calendar.

Page 1, line 1, after "of" insert "an"

Page 2, line 2, after "warrant" insert ", unless the information was obtained under the circumstances described in subdivision a or b of subsection 1 or was obtained through the monitoring of public lands or international borders"

Page 3, line 27, after "the" insert "lawful"

Page 3, line 27, after "rights" insert ", unless the surveillance is otherwise allowed under this chapter"

Page 3, line 27, remove "A state agency may not authorize"

Page 3, remove lines 28 through 30

Renumber accordingly

2015 TESTIMONY

HB 1328

#1
HB1328
2-4-15

“I’ve Got Nothing to Hide” and Other Misunderstandings of Privacy

DANIEL J. SOLOVE*

TABLE OF CONTENTS

I.	INTRODUCTION	745
II.	THE “NOTHING TO HIDE” ARGUMENT	748
III.	CONCEPTUALIZING PRIVACY	754
	A. <i>A Pluralistic Conception of Privacy</i>	754
	B. <i>The Social Value of Privacy</i>	760
IV.	THE PROBLEM WITH THE “NOTHING TO HIDE” ARGUMENT	764
	A. <i>Understanding the Many Dimensions of Privacy</i>	764
	B. <i>Understanding Structural Problems</i>	768
V.	CONCLUSION	772

I. INTRODUCTION

Since the September 11 attacks, the government has been engaging in extensive surveillance and data mining. Regarding surveillance, in December 2005, the *New York Times* revealed that after September 11, the Bush Administration secretly authorized the National Security Administration (NSA) to engage in warrantless wiretapping of American citizens’ telephone calls.¹ As for data mining, which involves analyzing

* © Daniel J. Solove 2007. Associate Professor, George Washington University Law School; J.D., Yale Law School. Thanks to Chris Hoofnagle, Adam Moore, and Michael Sullivan for helpful comments, and to my research assistant Sheerin Shahinpoor. I develop some of the ideas in this essay in significantly more depth in my forthcoming book, *Understanding Privacy*, to be published by Harvard University Press in May 2008.

1. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts: Secret Order to Widen Domestic Monitoring*, N.Y. TIMES, Dec. 16, 2005, at A1.

personal data for patterns of suspicious behavior, the government has begun numerous programs. In 2002, the media revealed that the Department of Defense was constructing a data mining project, called "Total Information Awareness" (TIA), under the leadership of Admiral John Poindexter.² The vision for TIA was to gather a variety of information about people, including financial, educational, health, and other data. The information would then be analyzed for suspicious behavior patterns. According to Poindexter: "The only way to detect . . . terrorists is to look for patterns of activity that are based on observations from past terrorist attacks as well as estimates about how terrorists will adapt to our measures to avoid detection."³ When the program came to light, a public outcry erupted, and the U.S. Senate subsequently voted to deny the program funding, ultimately leading to its demise.⁴ Nevertheless, many components of TIA continue on in various government agencies, though in a less systematic and more clandestine fashion.⁵

In May 2006, *USA Today* broke the story that the NSA had obtained customer records from several major phone companies and was analyzing them to identify potential terrorists.⁶ The telephone call database is reported to be the "largest database ever assembled in the world."⁷ In June 2006, the *New York Times* stated that the U.S. government had been accessing bank records from the Society for Worldwide Interbank Financial Transactions (SWIFT), which handles financial transactions for thousands of banks around the world.⁸ Many people responded with outrage at these announcements, but many others did not perceive much of a problem. The reason for their lack of concern, they explained, was because: "I've got nothing to hide."⁹

The argument that no privacy problem exists if a person has nothing to hide is frequently made in connection with many privacy issues. When the government engages in surveillance, many people believe that there is no threat to privacy unless the government uncovers unlawful activity, in which case a person has no legitimate justification to claim that it

2. John Markoff, *Pentagon Plans a Computer System That Would Peek at Personal Data of Americans*, N.Y. TIMES, Nov. 9, 2002, at A12.

3. John M. Poindexter, *Finding the Face of Terror in Data*, N.Y. TIMES, Sept. 10, 2003, at A25.

4. DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 169 (2004).

5. Shane Harris, *TIA Lives On*, NAT'L J., Feb. 25, 2006, at 66.

6. Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at A1; Susan Page, *Lawmakers: NSA Database Incomplete*, USA TODAY, June 30, 2006, at A1.

7. Cauley, *supra* note 6, at A1.

8. Eric Lichtblau & James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES, June 23, 2006, at A1.

9. *See infra* text accompanying notes 12–33.

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

remain private. Thus, if an individual engages only in legal activity, she has nothing to worry about. When it comes to the government collecting and analyzing personal information, many people contend that a privacy harm exists only if skeletons in the closet are revealed. For example, suppose the government examines one's telephone records and finds out that a person made calls to her parents, a friend in Canada, a video store, and a pizza delivery place. "So what?," that person might say. "I'm not embarrassed or humiliated by this information. If anybody asks me, I'll gladly tell them where I shop. I have nothing to hide."

The "nothing to hide" argument and its variants are quite prevalent in popular discourse about privacy. Data security expert Bruce Schneier calls it the "most common retort against privacy advocates."¹⁰ Legal scholar Geoffrey Stone refers to it as "all-too-common refrain."¹¹ The nothing to hide argument is one of the primary arguments made when balancing privacy against security. In its most compelling form, it is an argument that the privacy interest is generally minimal to trivial, thus making the balance against security concerns a foreordained victory for security. Sometimes the nothing to hide argument is posed as a question: "If you have nothing to hide, then what do you have to fear?" Others ask: "If you aren't doing anything wrong, then what do you have to hide?"

In this essay, I will explore the nothing to hide argument and its variants in more depth. Grappling with the nothing to hide argument is important, because the argument reflects the sentiments of a wide percentage of the population. In popular discourse, the nothing to hide argument's superficial incantations can readily be refuted. But when the argument is made in its strongest form, it is far more formidable.

In order to respond to the nothing to hide argument, it is imperative that we have a theory about what privacy is and why it is valuable. At its core, the nothing to hide argument emerges from a conception of privacy and its value. What exactly is "privacy"? How valuable is privacy and how do we assess its value? How do we weigh privacy against countervailing values? These questions have long plagued those seeking to develop a theory of privacy and justifications for its legal protection.

10. Bruce Schneier, Commentary, *The Eternal Value of Privacy*, WIRED, May 18, 2006, <http://www.wired.com/news/columns/1,70886-0.html>.

11. Geoffrey R. Stone, Commentary, *Freedom and Public Responsibility*, CHL. TRIB., May 21, 2006, at 11.

This essay begins in Part II by discussing the nothing to hide argument. First, I introduce the argument as it often exists in popular discourse and examine frequent ways of responding to the argument. Second, I present the argument in what I believe to be its strongest form. In Part III, I briefly discuss my work thus far on conceptualizing privacy. I explain why existing theories of privacy have been unsatisfactory, have led to confusion, and have impeded the development of effective legal and policy responses to privacy problems. In Part IV, I argue that the nothing to hide argument—even in its strongest form—stems from certain faulty assumptions about privacy and its value. The problem, in short, is not with finding an answer to the question: “If you’ve got nothing to hide, then what do you have to fear?” The problem is in the very question itself.

II. THE “NOTHING TO HIDE” ARGUMENT

When discussing whether government surveillance and data mining pose a threat to privacy, many people respond that they have nothing to hide. This argument permeates the popular discourse about privacy and security issues. In Britain, for example, the government has installed millions of public surveillance cameras in cities and towns, which are watched by officials via closed circuit television.¹² In a campaign slogan for the program, the government declares: “If you’ve got nothing to hide, you’ve got nothing to fear.”¹³ In the United States, one anonymous individual from the Department of Justice comments: “If [government officials] need to read my e-mails . . . so be it. I have nothing to hide. Do you?”¹⁴ One blogger, in reference to profiling people for national security purposes, declares: “Go ahead and profile me, I have nothing to hide.”¹⁵ Another blogger proclaims: “So I don’t mind people wanting to find out things about me, I’ve got nothing to hide! Which is why I support President Bush’s efforts to find terrorists by monitoring our phone calls!”¹⁶ Variations of nothing to hide arguments frequently appear in blogs, letters to the editor, television news interviews, and other forums. Some examples include:

12. JEFFREY ROSEN, *THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE* (2004).

13. *Id.* at 36.

14. Comment of NonCryBaby to <http://www.securityfocus.com/comments/articles/2296/18105/threaded> (Feb. 12, 2003).

15. Comment of Yoven to <http://www.danielpipes.org/comments/47675> (June 14, 2006, 14:03 EST).

16. Reach For The Stars!, <http://greatcarrieoakey.blogspot.com/2006/05/look-all-you-want-ive-got-nothing-to.html> (May 14, 2006, 09:04 PST).

+

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

- I don't have anything to hide from the government. I don't think I had that much hidden from the government in the first place. I don't think they care if I talk about my ornery neighbor.¹⁷
- Do I care if the FBI monitors my phone calls? I have nothing to hide. Neither does 99.99 percent of the population. If the wiretapping stops one of these Sept. 11 incidents, thousands of lives are saved.¹⁸
- Like I said, I have nothing to hide. The majority of the American people have nothing to hide. And those that have something to hide should be found out, and get what they have coming to them.¹⁹

The argument is not only of recent vintage. For example, one of the characters in Henry James's 1888 novel, *The Reverberator*, muses: "[I]f these people had done bad things they ought to be ashamed of themselves and he couldn't pity them, and if they hadn't done them there was no need of making such a rumpus about other people knowing."²⁰

I encountered the nothing to hide argument so frequently in news interviews, discussions, and the like, that I decided to blog about the issue. I asked the readers of my blog, *Concurring Opinions*, whether there are good responses to the nothing to hide argument.²¹ I received a torrent of comments to my post:

- My response is "So do you have curtains?" or "Can I see your credit card bills for the last year?"²²
- So my response to the "If you have nothing to hide . . ." argument is simply, "I don't need to justify my position. You need to justify yours. Come back with a warrant."²³

17. Comment of annegb to Concurring Opinions, http://www.concurringopinions.com/archives/2006/05/is_there_a_good.html#comments (May 23, 2006, 11:37 EST).

18. Joe Schneider, Letter to the Editor, *NSA Wiretaps Necessary*, ST. PAUL PIONEER PRESS, Aug. 24, 2006, at 11B.

19. *Polls Suggest Americans Approve NSA Monitoring* (NPR radio broadcast, May 19, 2006), available at 2006 WLNR 22949347.

20. HENRY JAMES, *THE REVERBERATOR* (1888), reprinted in *NOVELS 1886-1880*, at 555, 687 (1989).

21. Concurring Opinions, *supra* note 17 (May 23, 2006, 00:06 EST).

22. Comment of Adam to Concurring Opinions, *supra* note 17 (May 23, 2006, 16:27 EST).

23. Comment of Dissent to Concurring Opinions, *supra* note 17 (May 24, 2006, 07:48 EST).

- I don't have anything to hide. But I don't have anything I feel like showing you, either.²⁴
- If you have nothing to hide, then you don't have a life.²⁵
- Show me yours and I'll show you mine.²⁶
- It's not about having anything to hide, it's about things not being anyone else's business.²⁷
- Bottom line, Joe Stalin would [have] loved it. Why should anyone have to say more?²⁸

Most replies to the nothing to hide argument quickly respond with a witty retort. Indeed, on the surface it seems easy to dismiss the nothing to hide argument. Everybody probably has something to hide from somebody. As the author Aleksandr Solzhenitsyn declared, "Everyone is guilty of something or has something to conceal. All one has to do is look hard enough to find what it is."²⁹ Likewise, in Friedrich Dürrenmatt's novella *Traps*, which involves a seemingly innocent man put on trial by a group of retired lawyers for a mock trial game, the man inquires what his crime shall be. "'An altogether minor matter,' the prosecutor replied . . . 'A crime can always be found.'"³⁰ One can usually think of something compelling that even the most open person would want to hide. As one comment to my blog post noted: "If you have nothing to hide, then that quite literally means you are willing to let me photograph you naked? And I get full rights to that photograph—so I can show it to your neighbors?"³¹ Canadian privacy expert David Flaherty expresses a similar idea when he argues:

24. Comment of Ian to Concurring Opinions, *supra* note 17 (May 24, 2006, 19:51 EST).

25. Comment of Matthew Graybosch to Concurring Opinions, *supra* note 17 (Oct. 16, 2006, 12:09 EST).

26. Comment of Neureaux to Concurring Opinions, *supra* note 17 (Oct. 16, 2006, 14:39 EST).

27. Comment of Catter to Concurring Opinions, *supra* note 17 (Oct. 16, 2006, 11:36 PM EST).

28. Comment of Kevin to Concurring Opinions, *supra* note 17 (July 24, 2006, 12:36 EST).

29. ALEKSANDR SOLZHENITSYN, *CANCER WARD 192* (Nicholas Bethell & David Burg trans., Noonday Press 1991) (1968).

30. FRIEDRICH DÜRRENMATT, *TRAPS* 23 (Richard & Clara Winston trans., 1960).

31. Comment of Andrew to Concurring Opinions, *supra* note 17 (Oct. 16, 2006, 15:06 EST).

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

There is no sentient human being in the Western world who has little or no regard for his or her personal privacy; those who would attempt such claims cannot withstand even a few minutes' questioning about intimate aspects of their lives without capitulating to the intrusiveness of certain subject matters.³²

Such responses only attack the nothing to hide argument in its most extreme form, which is not particularly strong. As merely a one-line utterance about a particular person's preference, the nothing to hide argument is not very compelling. But stated in a more sophisticated manner, the argument is more challenging. First, it must be broadened beyond the particular person making it. When phrased as an individual preference, the nothing to hide argument is hard to refute because it is difficult to quarrel with one particular person's preferences. As one commenter aptly notes:

By saying "I have nothing to hide," you are saying that it's OK for the government to infringe on the rights of potentially millions of your fellow Americans, possibly ruining their lives in the process. To me, the "I have nothing to hide" argument basically equates to "I don't care what happens, so long as it doesn't happen to me."³³

In its more compelling variants, the nothing to hide argument can be made in a more general manner. Instead of contending that "I've got nothing to hide," the argument can be recast as positing that all law-abiding citizens should have nothing to hide. Only if people desire to conceal unlawful activity should they be concerned, but according to the nothing to hide argument, people engaged in illegal conduct have no legitimate claim to maintaining the privacy of such activities.

In a related argument, Judge Richard Posner contends: "[W]hen people today decry lack of privacy, what they want, I think, is mainly something quite different from seclusion: they want more power to conceal information about themselves that others might use to their disadvantage."³⁴ Privacy involves a person's "right to conceal discreditable facts about himself."³⁵ In other words, privacy is likely to be invoked when there is something to hide and that something consists of negative

32. David H. Flaherty, *Visions of Privacy: Past, Present, and Future*, in *VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE* 19, 31 (Colin J. Bennett & Rebecca Grant eds., 1999).

33. Comment of BJ Horn to Concurring Opinions, *supra* note 17 (June 2, 2006, 18:58 EST).

34. RICHARD A. POSNER, *THE ECONOMICS OF JUSTICE* 271 (1983).

35. RICHARD A. POSNER, *ECONOMIC ANALYSIS OF LAW* 46 (5th ed. 1998).

information about a person. Posner asserts that the law should not protect people in concealing discreditable information. "The economist," he argues, "sees a parallel to the efforts of sellers to conceal defects in their products."³⁶

Of course, one might object, there is nondiscreditable information about people that they nevertheless want to conceal because they find it embarrassing or just do not want others to know about. In a less extreme form, the nothing to hide argument does not refer to all personal information, but only to that subset of personal information that is likely to be involved in government surveillance. When people respond to NSA surveillance and data mining that they have nothing to hide, the more sophisticated way of understanding their argument should be as applying to the particular pieces of information that are gathered in the NSA programs. Information about what phone numbers people dial and even what they say in many conversations is often not likely to be embarrassing or discreditable to a law-abiding citizen. Retorts to the nothing to hide argument about exposing people's naked bodies to the world or revealing their deepest secrets to their friends are only relevant if there is a likelihood that such programs will actually result in these kinds of disclosures. This type of information is not likely to be captured in the government surveillance. Even if it were, many people might rationally assume that the information will be exposed only to a few law enforcement officials, and perhaps not even seen by human eyes. Computers might store the data and analyze it for patterns, but no person might have any contact with the data. As Posner argues:

The collection, mainly through electronic means, of vast amounts of personal data is said to invade privacy. But machine collection and processing of data cannot, as such, invade privacy. Because of their volume, the data are first sifted by computers, which search for names, addresses, phone numbers, etc., that may have intelligence value. This initial sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer.³⁷

There is one final component of the most compelling versions of the nothing to hide argument—a comparison of the relative value of the privacy interest being threatened with the government interest in promoting security. As one commenter to my blog post astutely notes: "You can't talk about how people feel about the potential loss of privacy in any meaningful way without recognizing that most of the people who don't mind the NSA programs see it as a potential exchange of a small

36. *Id.*

37. Richard A. Posner, *Our Domestic Intelligence Crisis*, WASH. POST, Dec. 21, 2005, at A 31.

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

amount of privacy for a potential national security gain.”³⁸ In other words, the nothing to hide argument can be made by comparing the relative value between privacy and security. The value of privacy, the argument provides, is low, because the information is often not particularly sensitive. The ones with the most to worry about are the ones engaged in illegal conduct, and the value of protecting their privacy is low to nonexistent. On the government interest side of the balance, security has a very high value. Having a computer analyze the phone numbers one dials is not likely to expose deep dark secrets or embarrassing information to the world. The machine will simply move on, oblivious to any patterns that are not deemed suspicious. In other words, if you are not doing anything wrong, you have nothing to hide and nothing to fear.

Therefore, in a more compelling form than is often expressed in popular discourse, the nothing to hide argument proceeds as follows: The NSA surveillance, data mining, or other government information-gathering programs will result in the disclosure of particular pieces of information to a few government officials, or perhaps only to government computers. This very limited disclosure of the particular information involved is not likely to be threatening to the privacy of law-abiding citizens. Only those who are engaged in illegal activities have a reason to hide this information. Although there may be some cases in which the information might be sensitive or embarrassing to law-abiding citizens, the limited disclosure lessens the threat to privacy. Moreover, the security interest in detecting, investigating, and preventing terrorist attacks is very high and outweighs whatever minimal or moderate privacy interests law-abiding citizens may have in these particular pieces of information.

Cast in this manner, the nothing to hide argument is a formidable one. It balances the degree to which an individual's privacy is compromised by the limited disclosure of certain information against potent national security interests. Under such a balancing scheme, it is quite difficult for privacy to prevail.

38. Comment of MJ to Concurring Opinions, *supra* note 17 (May 23, 2006, 17:30 EST).

III. CONCEPTUALIZING PRIVACY

For quite some time, scholars have proclaimed that privacy is so muddled a concept that it is of little use. According to Arthur Miller, privacy is “exasperatingly vague and evanescent.”³⁹ As Hyman Gross declares, “[T]he concept of privacy is infected with pernicious ambiguities.”⁴⁰ Colin Bennett similarly notes, “Attempts to define the concept of ‘privacy’ have generally not met with any success.”⁴¹ Robert Post declares that “[p]rivacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.”⁴² “Perhaps the most striking thing about the right to privacy,” Judith Jarvis Thomson observes, “is that nobody seems to have any very clear idea what it is.”⁴³

Often, the philosophical discourse about conceptualizing privacy is ignored in legal and policy debates. Many jurists, politicians, and scholars simply analyze the issues without articulating a conception of what privacy means. However, conceptualizing privacy is essential for the analysis of these issues. Those working on legal and policy issues all have some implicit conception of privacy. In many cases, privacy issues never get balanced against conflicting interests because courts, legislators, and others fail even to recognize that privacy is implicated. It is therefore of paramount importance that we continue to work on developing a conception of privacy. But how? Why have existing attempts been so unsatisfying?

A. A Pluralistic Conception of Privacy

Many attempts to conceptualize privacy do so by attempting to locate the essence of privacy—its core characteristics or the common denominator that links together the various things we classify under the rubric of “privacy.” I refer to this as the traditional method of conceptualizing. This method seeks to understand privacy *per genus et differentiam*—by looking for necessary and sufficient elements that demarcate what privacy is.

39. ARTHUR R. MILLER, *THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS* 25 (1971).

40. Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34, 35 (1967).

41. COLIN J. BENNETT, *REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES* 25 (1992).

42. Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001).

43. Judith Jarvis Thomson, *The Right to Privacy*, in *PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY* 272, 272 (Ferdinand David Schoeman ed., 1984).

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

In my article, *Conceptualizing Privacy*, I discussed a wide range of attempts to locate the common denominator of privacy.⁴⁴ I examined several different candidates for the common denominator in the existing philosophical and legal literature. Some attempts to conceptualize privacy were too narrow, excluding things we commonly understand to be private. For example, several theorists have contended that privacy should be defined in terms of intimacy. According to philosopher Julie Inness: "[T]he content of privacy cannot be captured if we focus exclusively on either information, access, or intimate decisions because privacy involves all three areas. . . . I suggest that these apparently disparate areas are linked by the common denominator of intimacy—privacy's content covers *intimate* information, access, and decisions."⁴⁵ The problem with understanding privacy as intimacy, however, is that not all private information or decisions we make are intimate. For instance, our Social Security number, political affiliations, religious beliefs, and much more may not be intimate, but we may regard them as private. Of course, intimacy could be defined quite broadly, though then it merely becomes a synonym for privacy rather than an elaboration of what privacy means. The purpose of defining privacy as intimacy is to develop a bounded and coherent conception of privacy, but it comes at the cost of being far too narrow.

On the other hand, some attempts to conceptualize privacy are far too broad, such as Samuel Warren and Louis Brandeis's understanding of privacy as the "right to be let alone."⁴⁶ What exactly does being let alone entail? There are many ways in which people are intruded upon that they would not consider privacy violations. If you shove me, you are not leaving me alone. You may be harming me, but it is not a problem of privacy.

Ultimately, any attempt to locate a common core to the manifold things we file under the rubric of "privacy" faces a difficult dilemma. If one chooses a common denominator that is broad enough to encompass nearly everything, then the conception risks the danger of being overinclusive or too vague. If one chooses a narrower common denominator, then the risk is that the conception is too restrictive. In *Conceptualizing Privacy*,

44. Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1095–99 (2002).

45. JULIE C. INNESS, *PRIVACY, INTIMACY, AND ISOLATION* 56 (1992).

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

I surveyed the various proposed conceptions and found all to suffer from these problems.⁴⁷

I argued that instead of conceptualizing privacy with the traditional method, we should instead understand privacy as a set of family resemblances. In *Philosophical Investigations*, Ludwig Wittgenstein argued that some concepts do not have “one thing in common” but “are related to one another in many different ways.”⁴⁸ Instead of being related by a common denominator, some things share “a complicated network of similarities overlapping and criss-crossing: sometimes overall similarities, sometimes similarities of detail.”⁴⁹ In other words, privacy is not reducible to a singular essence; it is a plurality of different things that do not share one element in common but that nevertheless bear a resemblance to each other.

In my work on conceptualizing privacy thus far, I have attempted to lay the groundwork for a pluralistic understanding of privacy. In some works, I have attempted to analyze specific privacy issues, trying to better articulate the nature of the problems. For example, in my book, *The Digital Person*, I argued that the collection and use of personal information in databases presents a different set of problems than government surveillance.⁵⁰ Many commentators had been using the metaphor of George Orwell’s *1984* to describe the problems created by the collection and use of personal data.⁵¹ I contended that the Orwell metaphor, which focuses on the harms of surveillance (such as inhibition and social control) might be apt to describe law enforcement’s monitoring of citizens. But much of the data gathered in computer databases is not particularly sensitive, such as one’s race, birth date, gender, address, or marital status. Many people do not care about concealing the hotels they stay at, the cars they own or rent, or the kind of beverages they drink. People often do not take many steps to keep such information secret. Frequently, though not always, people’s activities would not be inhibited if others knew this information.

I suggested a different metaphor to capture the problems: Franz Kafka’s *The Trial*, which depicts a bureaucracy with inscrutable purposes that uses people’s information to make important decisions about them, yet denies the people the ability to participate in how their information is

47. Solove, *supra* note 44, at 1099–1124.

48. LUDWIG WITTGENSTEIN, *PHILOSOPHICAL INVESTIGATIONS* § 65 (G.E.M. Anscombe trans., 3d ed. 2001).

49. *Id.* § 66.

50. SOLOVE, *supra* note 4, at 6–9.

51. GEORGE ORWELL, *1984* (Signet Classic 1984) (1949); SOLOVE, *supra* note 4, at 7.

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

used.⁵² The problems captured by the Kafka metaphor are of a different sort than the problems caused by surveillance. They often do not result in inhibition or chilling. Instead, they are problems of information processing—the storage, use, or analysis of data—rather than information collection. They affect the power relationships between people and the institutions of the modern state. They not only frustrate the individual by creating a sense of helplessness and powerlessness, but they also affect social structure by altering the kind of relationships people have with the institutions that make important decisions about their lives.

I explored the ways that legal and policy solutions were focusing too much on the nexus of problems under the Orwell metaphor—those of surveillance—and were not adequately addressing the Kafka problems—those of information processing.⁵³ The difficulty was that commentators were trying to conceive of the problems caused by databases in terms of surveillance when, in fact, these problems were different. The way that these problems are conceived has a tremendous impact on the legal and policy solutions used to solve them. As John Dewey observed, “[A] problem well put is half-solved.”⁵⁴ “The way in which the problem is conceived,” Dewey explained, “decides what specific suggestions are entertained and which are dismissed; what data are selected and which rejected; it is the criterion for relevancy and irrelevancy of hypotheses and conceptual structures.”⁵⁵

In a subsequent article, *A Taxonomy of Privacy*, I developed a taxonomy of privacy—a way of mapping out the manifold types of problems and harms that constitute privacy violations.⁵⁶ The taxonomy is my attempt to formulate a model of the problems from studying the welter of laws, cases, issues, and cultural and historical materials. The taxonomy I developed is as follows:

52. FRANZ KAFKA, *THE TRIAL* 50–58 (Willa & Edwin Muir trans., Random House 1956) (1937); SOLOVE, *supra* note 4, at 8–9.

53. SOLOVE, *supra* note 4, at 27–75.

54. JOHN DEWEY, *LOGIC: THE THEORY OF INQUIRY* 112 (Jo Ann Boydston ed. 1991) (1938).

55. *Id.*

56. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

Information Collection
 Surveillance
 Interrogation
Information Processing
 Aggregation
 Identification
 Insecurity
 Secondary Use
 Exclusion
Information Dissemination
 Breach of Confidentiality
 Disclosure
 Exposure
 Increased Accessibility
 Blackmail
 Appropriation
 Distortion
Invasion
 Intrusion
 Decisional Interference

The taxonomy has four general categories of privacy problems with sixteen different subcategories. The first general category is information collection, which involves the ways that data is gathered about people. The subcategories, surveillance and interrogation, represent the two primary problematic ways of gathering information. A privacy problem occurs when an activity by a person, business, or government entity creates harm by disrupting valuable activities of others. These harms need not be physical or emotional; they can occur by chilling socially beneficial behavior (for example, free speech and association) or by leading to power imbalances that adversely affect social structure (for example, excessive executive power).

The second general category is information processing. This involves the storing, analysis, and manipulation of data. There are a number of problems that information processing can cause, and I included five subcategories in my taxonomy. For example, one problem that I label *insecurity* results in increasing people's vulnerability to potential abuse of their information.⁵⁷ The problem that I call *exclusion* involves people's inability to access and have any say in the way their data is used.⁵⁸

57. *Id.* at 516–20.

58. *Id.* at 522–25.

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

Information dissemination is the third general category. Disseminating information involves the ways in which it is transferred—or threatened to be transferred—to others. I identify seven different information dissemination problems. Finally, the last category involves invasions. Invasions are direct interferences with the individual, such as intruding into her life or regulating the kinds of decisions she can make about her life.

My purpose in advancing the taxonomy is to shift away from the rather vague label of *privacy* in order to prevent distinct harms and problems from being conflated or not recognized. Some might contend, however, that several of the problems I discuss are not really “privacy” problems. But with no satisfactory set of necessary or sufficient conditions to define *privacy*, there is no one specific criterion for inclusion or exclusion under the rubric of “privacy.” Privacy violations consist of a web of related problems that are not connected by a common element, but nevertheless bear some resemblances to each other. We can determine whether to classify something as falling in the domain of privacy if it bears resemblance to other things we similarly classify. In other words, we use a form of analogical reasoning in which “[t]he key task,” Cass Sunstein observes, “is to decide when there are relevant similarities and differences.”⁵⁹ Accordingly, there are no clear boundaries for what we should or should not refer to as “privacy.” Some might object to the lack of clear boundaries, but this objection assumes that having definitive boundaries matters. The quest for a traditional definition of *privacy* has led to a rather fruitless and unresolved debate. In the meantime, there are real problems that must be addressed, but they are either conflated or ignored because they do not fit into various prefabricated conceptions of privacy. The law often neglects to see the problems and instead ignores all things that do not fall into a particular conception of privacy. In this way, conceptions of privacy can prevent the examination of problems. The problems still exist regardless of whether we classify them as being “privacy” problems.

A great deal of attention is expended trying to elucidate the concept of privacy without looking at the problems we are facing. My goal is to begin with the problems and understand them in detail. Trying to fit them into a one-size-fits-all conception of privacy neglects to see the problems in their full dimensions or to understand them completely.

59. CASS R. SUNSTEIN, LEGAL REASONING AND POLITICAL CONFLICT 67 (1996).

15

Conceptions should help us understand and illuminate experience; they should not detract from experience and make us see and understand less.

The term *privacy* is best used as a shorthand umbrella term for a related web of things. Beyond this kind of use, the term *privacy* has little purpose. In fact, it can obfuscate more than clarify.

Some might object to the inclusion or exclusion of certain problems in the taxonomy. I do not advance the taxonomy as perfect. It is a bottom-up ongoing project. As new problems arise, the taxonomy will be revised. Whether a particular problem is classified as one of privacy is not as important as whether it is recognized as a problem. Regardless of whether we label the problem as part of the privacy cluster, it still is a problem, and protecting against it still has a value. For example, I classify as a privacy violation a problem I call *distortion*, which involves disseminating false or misleading information about a person. Some might argue that distortion really is not a privacy harm, because privacy only involves true information. But does it matter? Regardless of whether distortion is classified as a privacy problem, it is nevertheless a problem. Classifying it as a privacy problem is merely saying that it bears some resemblance to other privacy problems, and viewing them together might be helpful in addressing them.

B. The Social Value of Privacy

Many theories of privacy view it as an individual right. For example, Thomas Emerson declares that privacy “is based upon premises of individualism, that the society exists to promote the worth and the dignity of the individual. . . . The right of privacy . . . is essentially the right not to participate in the collective life—the right to shut out the community.”⁶⁰ In the words of one court: “Privacy is inherently personal. The right to privacy recognizes the sovereignty of the individual.”⁶¹

Traditionally, rights have often been understood as protecting the individual against the incursion of the community, based on respect for the individual’s personhood or autonomy. Many theories of privacy’s value understand privacy in this manner. For example, Charles Fried argues that privacy is one of the

basic rights in persons, rights to which all are entitled equally, by virtue of their status as persons. . . . In this sense, the view is Kantian; it requires recognition of persons as ends, and forbids the overriding of their most fundamental interests for the purpose of maximizing the happiness or welfare of all.⁶²

60. THOMAS I. EMERSON, *THE SYSTEM OF FREEDOM OF EXPRESSION* 545, 549 (1970).

61. *Smith v. City of Artesia*, 772 P.2d 373, 376 (N.M. Ct. App. 1989).

62. Charles Fried, *Privacy*, 77 *YALE L.J.* 475, 478 (1968); see also INNESS, *supra* note 45, at 95 (“[P]rivacy is valuable because it acknowledges our respect for persons as

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

Many of the interests that conflict with privacy, however, also involve people's autonomy and dignity. Free speech, for example, is also an individual right which is essential to autonomy. Yet, in several cases, it clashes with privacy. One's privacy can be in direct conflict with another's desire to speak about that person's life. Security, too, is not merely a societal interest; it is essential for individual autonomy as well. Autonomy and dignity are often on both sides of the balance, so it becomes difficult to know which side is the one that protects the "sovereignty of the individual."⁶³

Communitarian scholars launch a formidable critique of traditional accounts of individual rights. Amitai Etzioni, for example, contends that privacy is "a *societal license* that exempts a category of acts (including thoughts and emotions) from communal, public, and governmental scrutiny."⁶⁴ For Etzioni, many theories of privacy treat it as sacrosanct, even when it conflicts with the common good.⁶⁵ According to Etzioni, "privacy is not an absolute value and does not trump all other rights or concerns for the common good."⁶⁶ He goes on to demonstrate how privacy interferes with greater social interests and often, though not always, contends that privacy should lose out in the balance.⁶⁷

Etzioni is right to critique those who argue that privacy is an individual right that should trump social interests. The problem, however, is that utilitarian balancing between individual rights and the common good rarely favors individual rights—unless the interest advanced on the side of the common good is trivial. Society will generally win when its interests are balanced against those of the individual.

The deeper problem with Etzioni's view is that in his critique of liberal theories of individual rights as absolutes, he views individual rights as being in tension with society. The same dichotomy between

autonomous beings with the capacity to love, care and like—in other words, persons with the potential to freely develop close relationships."); BEATE ROSSLER, *THE VALUE OF PRIVACY* 117 (R.D.V. Glasgow trans., Polity Press 2005) (2001) ("Respect for a person's privacy is respect for her as an autonomous subject."); Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, in *NOMOS XIII: PRIVACY* 1, 26 (J. Roland Pennock & John W. Chapman eds., 1971) ("[R]espect for someone as a person, as a chooser, imp[lie[s]] respect for him as one engaged on a kind of self-creative enterprise, which could be disrupted, distorted, or frustrated even by so limited an intrusion as watching.").

63. *Smith*, 772 P.2d at 376.

64. AMITAI ETZIONI, *THE LIMITS OF PRIVACY* 196 (1999).

65. *Id.* at 187–88.

66. *Id.* at 38.

67. *Id.* at 187–88.

individual and society that pervades liberal theories of individual rights also pervades Etzioni's communitarianism. Etzioni views the task of communitarians as "balanc[ing] individual rights with social responsibilities, and individuality with community."⁶⁸ The problem with Etzioni's communitarian view is that individuality need not be on the opposite side of the scale from community. Such a view assumes that individual and societal interests are distinct and conflicting. A similar view also underpins many liberal conceptions of individual rights.

In contrast, John Dewey proposed an alternative theory about the relationship between individual and community. For Dewey, there is no strict dichotomy between individual and society. The individual is shaped by society, and the good of both the individual and society are often interrelated rather than antagonistic: "We cannot think of ourselves save as to some extent *social* beings. Hence we cannot separate the idea of ourselves and our own good from our idea of others and of their good."⁶⁹ Dewey contended that the value of protecting individual rights emerges from their contribution to society. In other words, individual rights are not trumps, but are protections by society from its intrusiveness. Society makes space for the individual because of the social benefits this space provides. Therefore, Dewey argues, rights should be valued based on "the contribution they make to the welfare of the community."⁷⁰ Otherwise, in any kind of utilitarian calculus, individual rights would not be valuable enough to outweigh most social interests, and it would be impossible to justify individual rights. As such, Dewey argued, we must insist upon a "social basis and social justification" for civil liberties.⁷¹

I contend, like Dewey, that the value of protecting the individual is a social one. Society involves a great deal of friction, and we are constantly clashing with each other. Part of what makes a society a good place in which to live is the extent to which it allows people freedom from the intrusiveness of others. A society without privacy protection would be suffocating, and it might not be a place in which most would want to live. When protecting individual rights, we as a society decide to hold back in order to receive the benefits of creating the kinds of free zones for individuals to flourish.

As Robert Post has argued, privacy is not merely a set of restraints on society's rules and norms. Instead, privacy constitutes a society's

68. *Id.* at 198.

69. JOHN DEWEY, *ETHICS* (1908), *reprinted in* 5 *THE MIDDLE WORKS: 1899–1924*, at 268 (Jo Ann Boydston ed., S. Ill. Univ. Press 1978).

70. JOHN DEWEY, *LIBERALISM AND CIVIL LIBERTIES* (1936), *reprinted in* 11 *THE LATER WORKS, 1935–1937*, at 373 (Jo Ann Boydston ed., S. Ill. Univ. Press 1987).

71. *Id.* at 375.

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

attempt to promote rules of behavior, decorum, and civility.⁷² Society protects privacy as a means of enforcing a kind of order in the community. As Spiros Simitis declares, "[P]rivacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone."⁷³ Several scholars have argued that privacy is "constitutive" of society and must be valued in terms of the social roles it plays.⁷⁴ Privacy, then, is not the trumpeting of the individual against society's interests, but the protection of the individual based on society's own norms and values. Privacy is not simply a way to extricate individuals from social control, as it is itself a form of social control that emerges from a society's norms. It is not an external restraint on society, but is in fact an internal dimension of society. Therefore, privacy has a social value. Even when it protects the individual, it does so for the sake of society. It thus should not be weighed as an individual right against the greater social good. Privacy issues involve balancing societal interests on both sides of the scale.

Because privacy involves protecting against a plurality of different harms or problems, the value of privacy is different depending upon which particular problem or harm is being protected. Not all privacy problems are equal; some are more harmful than others. Therefore, we cannot ascribe an abstract value to privacy. Its value will differ substantially depending upon the kind of problem or harm we are safeguarding against. Thus, to understand privacy, we must conceptualize it and its value more pluralistically. Privacy is a set of protections against a related set of problems. These problems are not all related in the same way, but they resemble each other. There is a social value in protecting

72. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 968 (1989).

73. Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 709 (1987). In analyzing the problems of federal legislative policymaking on privacy, Priscilla Regan demonstrates the need for understanding privacy in terms of its social benefits. See PRISCILLA M. REGAN, *LEGISLATING PRIVACY*, at xiv (1995) ("[A]nalysis of congressional policy making reveals that little attention was given to the possibility of a broader social importance of privacy.").

74. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1427-28 (2000) ("Informational privacy, in short, is a constitutive element of a civil society in the broadest sense of that term."); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613 (1999) ("[I]nformation privacy is best conceived of as a constitutive element of civil society."); see also Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 455 (1980) ("Privacy is also essential to democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy.").

against each problem, and that value differs depending upon the nature of each problem.

IV. THE PROBLEM WITH THE “NOTHING TO HIDE” ARGUMENT

A. Understanding the Many Dimensions of Privacy

It is time to return to the nothing to hide argument. The reasoning of this argument is that when it comes to government surveillance or use of personal data, there is no privacy violation if a person has nothing sensitive, embarrassing, or illegal to conceal. Criminals involved in illicit activities have something to fear, but for the vast majority of people, their activities are not illegal or embarrassing.

Understanding privacy as I have set forth reveals the flaw of the nothing to hide argument at its roots. Many commentators who respond to the argument attempt a direct refutation by trying to point to things that people would want to hide. But the problem with the nothing to hide argument is the underlying assumption that privacy is about hiding bad things. Agreeing with this assumption concedes far too much ground and leads to an unproductive discussion of information people would likely want or not want to hide. As Bruce Schneier aptly notes, the nothing to hide argument stems from a faulty “premise that privacy is about hiding a wrong.”⁷⁵

The deeper problem with the nothing to hide argument is that it myopically views privacy as a form of concealment or secrecy. But understanding privacy as a plurality of related problems demonstrates that concealment of bad things is just one among many problems caused by government programs such as the NSA surveillance and data mining. In the categories in my taxonomy, several problems are implicated.

The NSA programs involve problems of information collection, specifically the category of surveillance in the taxonomy. Wiretapping involves audio surveillance of people’s conversations. Data mining often begins with the collection of personal information, usually from various third parties that possess people’s data. Under current Supreme Court Fourth Amendment jurisprudence, when the government gathers data from third parties, there is no Fourth Amendment protection because people lack a “reasonable expectation of privacy” in information exposed to others.⁷⁶ In *United States v. Miller*, the Supreme Court concluded that there is no reasonable expectation of privacy in bank records because “[a]ll of the documents obtained, including financial statements and

75. Schneier, *supra* note 10.

76. *United States v. Katz*, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."⁷⁷ In *Smith v. Maryland*, the Supreme Court held that people lack a reasonable expectation of privacy in the phone numbers they dial because they "know that they must convey numerical information to the phone company," and therefore they cannot "harbor any general expectation that the numbers they dial will remain secret."⁷⁸ As I have argued extensively elsewhere, the lack of Fourth Amendment protection of third party records results in the government's ability to access an extensive amount of personal information with minimal limitation or oversight.⁷⁹

Many scholars have referred to information collection as a form of surveillance. *Dataveillance*, a term coined by Roger Clarke, refers to the "systemic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons."⁸⁰ Christopher Slobogin has referred to the gathering of personal information in business records as "transaction surveillance."⁸¹ Surveillance can create chilling effects on free speech, free association, and other First Amendment rights essential for democracy.⁸² Even surveillance of legal activities can inhibit people from engaging in them. The value of protecting against chilling effects is not measured simply by focusing on the particular individuals who are deterred from exercising their rights. Chilling effects harm society because, among other things, they reduce the range of viewpoints expressed and the degree of freedom with which to engage in political activity.

The nothing to hide argument focuses primarily on the information collection problems associated with the NSA programs. It contends that limited surveillance of lawful activity will not chill behavior sufficiently to outweigh the security benefits. One can certainly quarrel with this

77. 425 U.S. 435, 442 (1976).

78. 442 U.S. 735, 743 (1979).

79. SOLOVE, *supra* note 4, at 165–209; see also Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1117–37 (2002).

80. Roger Clarke, *Information Technology and Dataveillance*, 31 COMM. OF THE ACM 498, 499 (1988); see also Roger Clarke, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, AUSTRALIAN NATIONAL UNIVERSITY, Aug. 7, 2006, <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>.

81. Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 140 (2005).

82. Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 154–59 (2007).

argument, but one of the difficulties with chilling effects is that it is often very hard to demonstrate concrete evidence of deterred behavior.⁸³ Whether the NSA's surveillance and collection of telephone records has deterred people from communicating particular ideas would be a difficult question to answer.

Far too often, discussions of the NSA surveillance and data mining define the problem solely in terms of surveillance. To return to my discussion of metaphor, the problems are not just Orwellian, but Kafkaesque. The NSA programs are problematic even if no information people want to hide is uncovered. In *The Trial*, the problem is not inhibited behavior, but rather a suffocating powerlessness and vulnerability created by the court system's use of personal data and its exclusion of the protagonist from having any knowledge or participation in the process. The harms consist of those created by bureaucracies—indifference, errors, abuses, frustration, and lack of transparency and accountability. One such harm, for example, which I call *aggregation*, emerges from the combination of small bits of seemingly innocuous data.⁸⁴ When combined, the information becomes much more telling about a person. For the person who truly has nothing to hide, aggregation is not much of a problem. But in the stronger, less absolutist form of the nothing to hide argument, people argue that certain pieces of information are not something they would hide. Aggregation, however, means that by combining pieces of information we might not care to conceal, the government can glean information about us that we might really want to conceal. Part of the allure of data mining for the government is its ability to reveal a lot about our personalities and activities by sophisticated means of analyzing data. Therefore, without greater transparency in data mining, it is hard to claim that programs like the NSA data mining program will not reveal information people might want to hide, as we do not know precisely what is revealed. Moreover, data mining aims to be predictive of behavior, striving to prognosticate about our future actions. People who match certain profiles are deemed likely to engage in a similar pattern of behavior. It is quite difficult to refute actions that one has not yet done. Having nothing to hide will not always dispel predictions of future activity.

Another problem in the taxonomy, which is implicated by the NSA program, is the problem I refer to as *exclusion*.⁸⁵ Exclusion is the problem caused when people are prevented from having knowledge about how their information is being used, as well as barred from being

83. *Id.*

84. Solove, *supra* note 56, at 506–11.

85. *Id.* at 522–25.

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

able to access and correct errors in that data. The NSA program involves a massive database of information that individuals cannot access. Indeed, the very existence of the program was kept secret for years.⁸⁶ This kind of information processing, which forbids people's knowledge or involvement, resembles in some ways a kind of due process problem. It is a structural problem involving the way people are treated by government institutions. Moreover, it creates a power imbalance between individuals and the government. To what extent should the Executive Branch and an agency such as the NSA, which is relatively insulated from the political process and public accountability, have a significant power over citizens? This issue is not about whether the information gathered is something people want to hide, but rather about the power and the structure of government.

A related problem involves "secondary use." Secondary use is the use of data obtained for one purpose for a different unrelated purpose without the person's consent. The Administration has said little about how long the data will be stored, how it will be used, and what it could be used for in the future. The potential future uses of any piece of personal information are vast, and without limits or accountability on how that information is used, it is hard for people to assess the dangers of the data being in the government's control.

Therefore, the problem with the nothing to hide argument is that it focuses on just one or two particular kinds of privacy problems—the disclosure of personal information or surveillance—and not others. It assumes a particular view about what privacy entails, and it sets the terms for debate in a manner that is often unproductive.

It is important to distinguish here between two ways of justifying a program such as the NSA surveillance and data mining program. The first way is to not recognize a problem. This is how the nothing to hide argument works—it denies even the existence of a problem. The second manner of justifying such a program is to acknowledge the problems but contend that the benefits of the NSA program outweigh the privacy harms. The first justification influences the second, because the low value given to privacy is based upon a narrow view of the problem.

The key misunderstanding is that the nothing to hide argument views privacy in a particular way—as a form of secrecy, as the right to hide

86. Risen & Lichtblau, *supra* note 1.

things. But there are many other types of harm involved beyond exposing one's secrets to the government.

Privacy problems are often difficult to recognize and redress because they create a panoply of types of harm. Courts, legislators, and others look for particular types of harm to the exclusion of others, and their narrow focus blinds them to seeing other kinds of harms.

B. Understanding Structural Problems

One of the difficulties with the nothing to hide argument is that it looks for a visceral kind of injury as opposed to a structural one. Ironically, this underlying conception of injury is shared by both those advocating for greater privacy protections and those arguing in favor of the conflicting interests to privacy. For example, law professor Ann Bartow argues that I have failed to describe privacy harms in a compelling manner in my article, *A Taxonomy of Privacy*, where I provide a framework for understanding the manifold different privacy problems.⁸⁷ Bartow's primary complaint is that my taxonomy "frames privacy harms in dry, analytical terms that fail to sufficiently identify and animate the compelling ways that privacy violations can negatively impact the lives of living, breathing human beings beyond simply provoking feelings of unease."⁸⁸ Bartow claims that the taxonomy does not have "enough dead bodies" and that privacy's "lack of blood and death, or at least of broken bones and buckets of money, distances privacy harms from other categories of tort law."⁸⁹

Most privacy problems lack dead bodies. Of course, there are exceptional cases such as the murders of Rebecca Shaeffer and Amy Boyer. Rebecca Shaeffer was an actress killed when a stalker obtained her address from a Department of Motor Vehicles record.⁹⁰ This incident prompted Congress to pass the Driver's Privacy Protection Act of 1994.⁹¹ Amy Boyer was murdered by a stalker who obtained her personal information, including her work address and Social Security number, from a database company.⁹² These examples aside, there is not a lot of death and gore in privacy law. If this is the standard to recognize a problem, then few privacy problems will be recognized. Horrific cases

87. Ann Bartow, *A Feeling of Unease About Privacy Law*, 155 U. PA. L. REV. PENNumbra 52, 52 (2006), <http://www.pennumbra.com/issues/articles/154-3/Bartow.pdf>.

88. *Id.*

89. *Id.* at 52, 62.

90. SOLOVE, *supra* note 4, at 147.

91. *Id.*

92. *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001, 1005-06 (N.H. 2003).

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

are not typical, and the purpose of my taxonomy is to explain why most privacy problems are still harmful despite this fact.

Bartow's objection is actually very similar to the nothing to hide argument. Those advancing the nothing to hide argument have in mind a particular kind of visceral privacy harm, one where privacy is violated only when something deeply embarrassing or discrediting is revealed. Bartow's quest for horror stories represents a similar desire to find visceral privacy harms. The problem is that not all privacy harms are like this. At the end of the day, privacy is not a horror movie, and demanding more palpable harms will be difficult in many cases. Yet there is still a harm worth addressing, even if it is not sensationalistic.

In many instances, privacy is threatened not by singular egregious acts, but by a slow series of relatively minor acts which gradually begin to add up. In this way, privacy problems resemble certain environmental harms which occur over time through a series of small acts by different actors. Bartow wants to point to a major spill, but gradual pollution by a multitude of different actors often creates worse problems.

The law frequently struggles with recognizing harms that do not result in embarrassment, humiliation, or physical or psychological injury.⁹³ For example, after the September 11 attacks, several airlines gave their passenger records to federal agencies in direct violation of their privacy policies. The federal agencies used the data to study airline security.⁹⁴ A group of passengers sued Northwest Airlines for disclosing their personal information. One of their claims was that Northwest Airlines breached its contract with the passengers. In *Dyer v. Northwest Airlines Corp.*, the court rejected the contract claim because "broad statements of company policy do not generally give rise to contract claims," the passengers never claimed they relied upon the policy or even read it, and they "failed to allege any contractual damages arising out of the alleged breach."⁹⁵ Another court reached a similar conclusion.⁹⁶

Regardless of the merits of the decisions on contract law, the cases represent a difficulty with the legal system in addressing privacy problems.

93. SOLOVE, *supra* note 4, at 93-97, 100-01, 195-208; Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1228 (2003).

94. SOLOVE, *supra* note 4, at 93.

95. 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004).

96. *In re Nw. Airlines Privacy Litig.*, No. 04-126, 2004 WL 1278459 (D. Minn. June 6, 2004).

25

The disclosure of the passenger records represented a “breach of confidentiality.”⁹⁷ The problems caused by breaches of confidentiality do not merely consist of individual emotional distress; they involve a violation of trust within a relationship. There is a strong social value in ensuring that promises are kept and that trust is maintained in relationships between businesses and their customers. The problem of secondary use is also implicated in this case.⁹⁸ Secondary use involves data collected for one purpose being used for an unrelated purpose without people’s consent. The airlines gave passenger information to the government for an entirely different purpose beyond that for which it was originally gathered. Secondary use problems often do not cause financial, or even psychological, injuries. Instead, the harm is one of power imbalance. In *Dyer*, data was disseminated in a way that ignored airline passengers’ interests in the data despite promises made in the privacy policy. Even if the passengers were unaware of the policy, there is a social value in ensuring that companies adhere to established limits on the way they use personal information. Otherwise, any stated limits become meaningless, and companies have discretion to boundlessly use data. Such a state of affairs can leave nearly all consumers in a powerless position. The harm, then, is less one to particular individuals than it is a structural harm.

A similar problem surfaces in another case, *Smith v. Chase Manhattan Bank*.⁹⁹ A group of plaintiffs sued Chase Manhattan Bank for selling customer information to third parties in violation of its privacy policy, which stated that the information would remain confidential. The court held that even presuming these allegations were true, the plaintiffs could not prove any actual injury:

[T]he “harm” at the heart of this purported class action, is that class members were merely offered products and services which they were free to decline. This does not qualify as actual harm.

The complaint does not allege any single instance where a named plaintiff or any class member suffered any actual harm due to the receipt of an unwanted telephone solicitation or a piece of junk mail.¹⁰⁰

The court’s view of harm, however, did not account for the breach of confidentiality.

When balancing privacy against security, the privacy harms are often characterized in terms of injuries to the individual, and the interest in security is often characterized in a more broad societal way. The security

97. Solove, *supra* note 56, at 526–30.

98. *Id.* at 520–22.

99. 741 N.Y.S.2d 100 (N.Y. App. Div. 2002).

100. *Id.* at 102.

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

interest in the NSA programs has often been defined improperly. In a Congressional hearing, Attorney General Alberto Gonzales stated:

Our enemy is listening, and I cannot help but wonder if they are not shaking their heads in amazement at the thought that anyone would imperil such a sensitive program by leaking its existence in the first place, and smiling at the prospect that we might now disclose even more or perhaps even unilaterally disarm ourselves of a key tool in the war on terror.¹⁰¹

The balance between privacy and security is often cast in terms of whether a particular government information collection activity should or should not be barred.

The issue, however, often is not whether the NSA or other government agencies should be allowed to engage in particular forms of information gathering; rather, it is what kinds of oversight and accountability we want in place when the government engages in searches and seizures. The government can employ nearly any kind of investigatory activity with a warrant supported by probable cause. This is a mechanism of oversight—it forces government officials to justify their suspicions to a neutral judge or magistrate before engaging in the tactic. For example, electronic surveillance law allows for wiretapping, but limits the practice with judicial supervision, procedures to minimize the breadth of the wiretapping, and requirements that the law enforcement officials report back to the court to prevent abuses.¹⁰² It is these procedures that the Bush Administration has ignored by engaging in the warrantless NSA surveillance. The question is not whether we want the government to monitor such conversations, but whether the Executive Branch should adhere to the appropriate oversight procedures that Congress has enacted into law, or should covertly ignore any oversight.

Therefore, the security interest should not get weighed in its totality against the privacy interest. Rather, what should get weighed is the extent of marginal limitation on the effectiveness of a government information gathering or data mining program by imposing judicial oversight and minimization procedures. Only in cases where such procedures will completely impair the government program should the security interest

101. *Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 15 (2006) (statement of Alberto Gonzales, Att'y Gen. of the United States).

102. Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 *FORDHAM L. REV.* 747, 775–76 (2005).

be weighed in total, rather than in the marginal difference between an unencumbered program versus a limited one.

Far too often, the balancing of privacy interests against security interests takes place in a manner that severely shortchanges the privacy interest while inflating the security interests. Such is the logic of the nothing to hide argument. When the argument is unpacked, and its underlying assumptions examined and challenged, we can see how it shifts the debate to its terms, in which it draws power from its unfair advantage. It is time to pull the curtain on the nothing to hide argument.

V. CONCLUSION

Whether explicit or not, conceptions of privacy underpin nearly every argument made about privacy, even the common quip “I’ve got nothing to hide.” As I have sought to demonstrate in this essay, understanding privacy as a pluralistic conception reveals that we are often talking past each other when discussing privacy issues. By focusing more specifically on the related problems under the rubric of “privacy,” we can better address each problem rather than ignore or conflate them. The nothing to hide argument speaks to some problems, but not to others. It represents a singular and narrow way of conceiving of privacy, and it wins by excluding consideration of the other problems often raised in government surveillance and data mining programs. When engaged with directly, the nothing to hide argument can ensnare, for it forces the debate to focus on its narrow understanding of privacy. But when confronted with the plurality of privacy problems implicated by government data collection and use beyond surveillance and disclosure, the nothing to hide argument, in the end, has nothing to say.

#2
HB1328
2-4-15

Testimony of the American Civil Liberties Union of North Dakota

In Support of HB 1328 – An Act to provide for limitations on the use of
unmanned aircraft for surveillance

House Judiciary Committee

February 4, 2015

On behalf of ACLU of North Dakota and its members and activists statewide, we commend the effort to regulate the use of unmanned aerial vehicles (UAVs), more commonly referred to as drones, through legislation that includes protections for individual privacy and oversight of their use. Unregulated, warrantless use of drones could have a chilling effect on the use of public spaces for First Amendment protected activities and could result in discriminatory targeting, institutional abuse, and automated law enforcement.

The ACLU has serious concerns about the use of unmanned aerial vehicle surveillance technology to collect information about individuals. The pace at which surveillance technology has evolved in recent years has far outstripped the pace at which laws have adapted to protect individuals' privacy. Strict controls are needed to help guide law enforcement in using surveillance technology. Without those limits, we risk inching further into a society under constant and permanent surveillance.

While Congress has required the Federal Aviation Administration (FAA) to open domestic airspace more widely to drones by 2015, the FAA has indicated that its mandate is airspace safety, not privacy. Therefore, it is incumbent upon the legislature to protect North Dakotans' privacy and ensure that we can enjoy the benefits of this technology without bringing us closer to a "surveillance society," in which everyone's move is monitored, tracked, recorded, and scrutinized by authorities.

HB 1328 strikes the right balance by permitting law enforcement use of drones in emergencies or with court oversight in investigative circumstances while prohibiting the indiscriminate use of drones. After all, it is a core value in our society that we do not watch innocent people just in case they do something wrong.

The bill also prohibits law enforcement from identifying anyone or anything other than the target that justified the warrant and drone deployment. And, it ensures that wherever drones are used, information that is incidentally collected cannot be used in court. This is very important – unlike many traditional searches that can be narrowly tailored to collect information only on a particular target, drones can be equipped with a host of technologies that can suck in information on not just the target, but everyone else who happens to be nearby, or underneath the drone as it travels to the target area.

Meanwhile, HB 1328 prohibits weaponization of drones, because an officer on the ground has a very different perception of when it is necessary to use force and what force is appropriate than an officer observing the scene on a screen from a distance might.

The bill exempts public universities from the warrant requirement so that drones can be used for research and academic purposes, allowing North Dakota to continue to partake in the cutting edge drone research and development field while still protecting individuals' privacy.

Drone technology brings with it many opportunities. But the types of surveillance drones are capable of carries risks to our way of life. Drones are being developed that are small enough to fly into houses undetected, and drones aren't subject to the same limitations as helicopters with their human pilots and need for launch pads and flight and ground crews. It may soon become technologically feasible to watch everyone all the time, which may have a profound effect on our society. Psychologists have repeatedly found that people who are being observed tend to behave differently, and make different decisions, than when they are not being watched. This effect is so great that a recent study found that "merely hanging up posters of staring human eyes is enough to significantly change people's behavior."¹

Before drones become ubiquitous in our airspace, we need clear privacy rules so that we can enjoy this new technology without sacrificing our privacy. HB 1328 would provide those rules and ensure that drones are prohibited for indiscriminate mass surveillance, with their use by police only permitted where there are grounds to believe they will collect evidence relating to a specific instance of criminal wrongdoing, or in emergencies. North Dakota should join Florida, Idaho, Illinois, Montana, North Carolina, Oregon, Tennessee, Texas and Virginia in passing legislation to regulate government deployment of this powerful technology.

On behalf of ACLU of North Dakota and its members and activists statewide, we urge you to give HB 1328 a Do Pass recommendation.

¹ Sander van der Linden, "How the Illusion of Being Observed Can Make You a Better Person," Scientific American, May 3, 2011, online at <http://www.scientificamerican.com/article.cfm?id=how-the-illusion-of-being-observed-can-make-you-better-person>.

243
HB 1328
2-4-15

GRAND FORKS COUNTY SHERIFF'S DEPARTMENT

PO BOX 12608

GRAND FORKS, NORTH DAKOTA 58208-2608

122 SOUTH FIFTH STREET, SUITE 210

PHONE: 701-780-8280

FAX: 701-780-8307

SHERIFF ROBERT W ROST



Good Morning Mr. Chairman and members of the Committee, my name is Bob Rost. I currently serve as the Sheriff of Grand Forks County. The Grand Forks County Sheriff's Department is the host agency for the Northeast Regional Unmanned Aircraft Systems Unit. Our UAS Unit was one of the first to be established in the nation and is the only non-federal UAS Unit in the State of North Dakota. Thank you for listening to my concerns regarding House Bill 1328.

House Bill 1328 appears to be a solution in search of a problem. The Grand Forks County Sheriff's Department has been operating UAS for over 3 years. During that period, we have not received a single complaint or allegation of misuse of our aircraft. In fact, we have received numerous compliments and accolades on the Unit from the press and the public. Our agency has exceeded all Federal Aviation Administration requirements by assigning only FAA certified commercial pilots to operate our UAS; conducting monthly UAS Unit training; and reporting our UAS flights to the FAA each month. Our UAS Unit is managed by a 34 year law enforcement veteran with significant law enforcement manned air support

experience. We have subjected our UAS mission sets to review by the University of North Dakota's Unmanned Aircraft Systems Research Compliance Committee and have fully implement their recommendations into our operations. Not one of the 16 UAS missions we have conducted has involved a covert surveillance. On the contrary, we have photographed homicide and fatal traffic accident scenes; searched for fleeing suspects; and done post-disaster assessment flights.

Our Unit is operated in compliance with an extensive UAS Unit Operations Manual that emphasizes the importance of protecting the privacy of the public we serve and which requires a search warrant for flights that would infringe upon an individual's reasonable expectation of privacy.

The U.S Supreme Court has effectively addressed the issue of law enforcement observations occurring from aircraft in the cases of *Ciraolo (SIR-E-A-LO) vs. California* and *Florida vs. Riley*. These cases provide ample direction to law enforcement on when a search warrant is required. Application of the language found in House Bill 1328 would negate the long-standing doctrine of plain view. A law enforcement officer does not need a warrant to observe a shopping center

parking lot from a helicopter at 400' above ground level. Why should the standard be higher for that same observation made from a UAS? Eventually, as the use of UAS expands, images from UAS will begin to be utilized as evidence in criminal cases. The judiciary, tasked by our Federal Constitution with determining the constitutionality of evidence, will then have the opportunity to weigh in on evidence gathered by UAS. House Bill 1328 would, to a great degree, preempt this process. Please allow our elected judges to do their jobs.

In closing, the crime rate in North Dakota is rapidly rising. Law enforcement agencies, especially those in the western portion of our state, are struggling to try to suppress an ever increasing volume of violent and drug related crimes. In order to do this, North Dakota law enforcement needs more cost effective technologies, not less. Please support law enforcement by making it easier, not harder, to utilize innovative technologies such as unmanned aircraft systems. Let's not try to fix something that is not broken. Thank you.

HB 1328

#4
HB1328
2-4-15
1 of 5

My name is Bruce Burkett, a spokesperson for the North Dakota Peace Officers Association. We are in opposition to House Bill 1328.

The bill would put blinders on law enforcement from making observations from a location where we have a right to be. Observations made from locations considered open fields do not require a search warrant by law enforcement.

Operations of unmanned and manned aircrafts are regulated by the FAA. Regulations of UAV's is laid out in Part 107 of the Federal regulations. At this time "drone" operations by citizens needs to look and sound as a hobbyist. The aircraft must weigh less than fifty five pounds and are exempt from complying with part 91 of the Federal Regulations. UAV's operated other than the "hobbyist" category as of now, must be operated by a certified pilot, the aircraft needs to be registered and needs to be certified as "airworthy" by the FAA and must have a certificate of authorization.

North Dakota law enforcement uses fixed winged aircraft for many law enforcement purposes. The Crime Bureau, ND Highway Patrol and the Game and Fish Department are State assets that are available for law enforcement services. Other agencies sometimes lease aircraft from fixed base operators for issues in their area. Anything that can be observed using a LEGAL UAV aircraft, I can do using a fixed winged airplane. Over the last 34 years, my law enforcement missions comprised flying to detect game and fish law violations, assisting other

agencies following suspects, conducting surveillance for burglary activities, searching for stolen property, photo surveillance for search warrant development, search and rescue, missing person searches along with federal agencies on drug interception and smuggling cases.

FAA rules require aircraft flown over sparsely populated areas to fly at least 500 feet above any person, vessel, vehicle or structure. When flying over a congested area (city, town or settlement) the aircraft must be at least 1000 feet above the highest obstacle except for takeoff and landing operations.

Certainly quality photography equipment available to citizens and law enforcement used during manned flights can only see things in plain view. Over the last 7 years, on my personal time, I have taken aerial photos of rural residences and farms for a company in Wisconsin. The camera I use is capable of taking high resolution photos from a place I have a right to be.

This bill is unnecessary and for those reasons we oppose its adoption.



Federal Aviation Administration

Unmanned Aircraft Systems

(<http://www.faa.gov/news/updates/?newsId=81485>)

Unmanned Aircraft and NFL Football Don't Mix

(<http://www.faa.gov/news/updates/?newsId=81485>)

The Super Bowl is a no drone zone, so leave your drone at home.

< () > (

Safety is the FAA's top mission, and the agency maintains the world's safest aviation system. The FAA first authorized use of unmanned aircraft in the National Airspace System (NAS) in 1990.

Today, unmanned aircraft are flying in the NAS under very controlled conditions, performing border and port surveillance by the Department of Homeland Security, helping with scientific research and environmental monitoring by NASA and NOAA, supporting public safety by law enforcement agencies, helping state universities conduct research, and supporting various other missions for public (government) entities. Operations range from ground level to above 50,000 feet, depending on the specific type of aircraft. However, UAS operations are currently not authorized in Class B airspace (http://www.faa.gov/regulations_policies/handbooks_manuals/aviation/pilot_handbook/media/PHAK%20-%20Chapter%2014.pdf) (PDF), which exists over major urban areas and contains the highest density of manned aircraft in the National Airspace System.

What are the different types of UAS operations?

There are three types of unmanned aircraft system operations: Civil, Public and Model Aircraft.

• Civil UAS

Obtaining a Special Airworthiness Certificate

(http://www.faa.gov/aircraft/air_cert/airworthiness_certification/sp_awcert/experiment/sac/) in the experimental category for a particular UAS is currently the only way civil operators of unmanned aircraft are accessing the NAS. Experimental certificate regulations preclude carrying people or property for compensation or hire, but do allow operations for research and development, flight and sales demonstrations and crew training. The FAA is working with civilian operators to collect technical and operational data that will help refine the UAS airworthiness certification process. The agency is currently developing a future path for safe integration of civil UAS into the NAS as part of NextGen implementation. Read more about Civil Operations (civil operations/).

The FAA has been working for several months to implement the provisions of Section 333 ([legislative_programs/section_333/](http://www.faa.gov/legislative_programs/section_333/)) of the FAA Modernization and Reform Act of 2012, "Special Rules for Certain Unmanned Aircraft Systems," which will allow for commercial operations in low-risk, controlled environments. Read more about Section 333 (legislative_programs/section_333/).

- **Public UAS**

COAs

(http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaaim/organizations/uas/coa/) are available to public entities that want to fly a UAS in civil airspace. Common uses today include law enforcement, firefighting, border patrol, disaster relief, search and rescue, military training, and other government operational missions. Applicants make their request through an online process

(http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaaim/organizations/uas/coa/) and the FAA evaluates the proposed operation to see if it can be conducted safely. Read more about Public Operations ([public_operations/](#)).

- **Model Aircraft**

Recreational use of airspace by model aircraft is covered by FAA Advisory Circular 91-57

(http://www.faa.gov/documentLibrary/media/Advisory_Circular/91-57.pdf) (PDF), which generally limits operations for hobby and recreation to below 400 feet, away from airports and air traffic, and within sight of the operator. In June 2014, the FAA published a Federal Register notice ([media/model_aircraft_spec_rule.pdf](#)) (PDF) on its interpretation of the statutory special rules for model aircraft in the FAA Modernization and Reform Act of 2012. The law is clear that the FAA may take enforcement action against model aircraft operators who operate their aircraft in a manner that endangers the safety of the national airspace system. In the notice, the FAA explains that this enforcement authority is designed to protect users of the airspace as well as people and property on the ground. Read the full press release (http://www.faa.gov/news/press_releases/news_story.cfm?newsId=16474). Read more about Model Aircraft Operations ([publications/model_aircraft_operators/](#)).

What can I do with my model aircraft?

Having fun means flying safely! Hobby or recreational flying doesn't require FAA approval but you must follow safety guidelines. Any other use requires FAA authorization. Here is a list of Do's and Don'ts for flying model aircraft ([publications/model_aircraft_operators/](#)).

Contact Us (contacts/)

The agency wants the public to know how and when to contact the FAA regarding safety concerns with UAS operations. You can visit the Agency's Aviation Safety Hotline website (http://www.faa.gov/contact/safety_hotline/) or call 1-866-835-5322, Option 4.

Page last modified: January 28, 2015 3:55:11 PM EST

This page was originally published at: <https://www.faa.gov/uas/>



Federal Aviation Administration

Public Operations (Governmental)

For public operation, the FAA issues a Certificate of Authorization or Waiver (COA)

(http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/coa/) that permits public agencies and organizations to operate a particular UA, for a particular purpose, in a particular area. The FAA works with these organizations to develop conditions and limitations for UA operations to ensure they do not jeopardize the safety of other aviation operations. The objective is to issue a COA with parameters that ensure a level of safety equivalent to manned aircraft. Usually, this entails making sure that the UA does not operate in a populated area and that the aircraft is observed, either by someone in a manned aircraft or someone on the ground. Common uses today include law enforcement, firefighting, border patrol, disaster relief, search and rescue, military training, and other government operational missions.

Applicants make their request through an online process (https://ioeaaa.faa.gov/oeaaa/oeaaa_login.jsp). After a complete application is submitted, FAA conducts a comprehensive operational and technical review. If necessary, provisions or limitations may be imposed as part of the approval to ensure the UA can operate safely with other airspace users. In most cases, FAA will provide a formal response within 60 days from the time a completed application is submitted.

The COA allows an operator to use a defined block of airspace and includes special provisions unique to the proposed operation. For instance, a COA may require flying only under Visual Flight Rules (VFR) and/or only during daylight hours. COAs usually are issued for a specific period—up to two years in many cases.

Most COAs require coordination with an appropriate air traffic control facility and may require a transponder on the UAS to operate in certain types of airspace.

Because UAS technology cannot currently comply with "see and avoid" rules that apply to all aircraft, a visual observer or an accompanying "chase plane" must maintain visual contact with the UAS and serve as its "eyes" when operating outside airspace restricted from other users.

Please email the FAA/UAS office at 9-AJR-36-UAS@faa.gov with any questions or for more information regarding Certificates of Waiver or Authorization.

Related sites

- Clarification of June 13, 2014 Interpretation on Research Using UAS
(http://www.faa.gov/about/office_org/headquarters_offices/agc/pol_adjudication/agc200/interpretations/data/interps/2014/williams-afs-80%20-%20%282014%29%20legal%20interpretation.pdf) (PDF), July 3, 2014
- UAS Operations by Public Universities for Aeronautical Research
(http://www.faa.gov/about/office_org/headquarters_offices/agc/pol_adjudication/agc200/interpretations/data/interps/2014/williams-afs-80%20-%20%282014%29%20legal%20interpretation.pdf) (PDF), June 13, 2014
- Certificate of Authorization or Waiver (COA)
(http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/coa/), ATA UAS description of the COA process.
- COA Online System (<https://ioeaaa.faa.gov/oeaaa/Welcome.jsp>), used by applicants to request a COA. Applicants must obtain an account to access the system.

#5
HB 1328
2-4-15

Testimony to the
House Judiciary Committee
University of North Dakota

February 4, 2015

Chairman Koppelman and members of the Committee:

My name is Michael Corcoran, and I am with the University of North Dakota UAS Center of Excellence. I am here to speak about House Bill 1328 on behalf of the University.

Although we agree with the sponsors of this bill that privacy concerns related to use of Unmanned Aircraft Systems (UASs) are valid, we do not believe that this legislation is necessary for several reasons:

- First, many of these concerns—including those expressed during the 63rd Legislative Assembly—have already been addressed through the establishment of an independent oversight committee, the UAS Research Compliance Committee. In response, the Committee has modified every protocol to address privacy usage and has commissioned a survey of citizen attitudes on UASs and privacy. It has also denied many UAS use requests in cases where concerns about privacy existed.
- Second, our experience in UAS activities working with a number of public and private entities, and our analysis of the public opinion survey I mentioned, lead us to conclude that the public supports responsible use of UAS.
- Third, we believe that this bill will have a negative effect on the development of UAS activities in our State. These activities are a proposed future driver of economic activity and have received significant state support in the past. I will briefly describe in more detail the basis for our concerns.

From the beginning of its UAS program, UND has recognized that privacy and other ethical issues needed to be addressed in order to allow the use of UASs by the public. In 2012 we formed the nation's first UAS Research Compliance Committee. The committee was originally developed to review all proposed uses of UASs by the Grand Forks County Sheriff's Department, with whom we are collaborating on developing procedures for law enforcement use of UASs, in a project funded through the ND Department of Commerce. It has been expanded to review all proposed uses of UASs by University members and the FAA Test Site. This committee has garnered national and international interest as a way to address issues related to UAS use based on community standards. The committee's work is based on three underlying principles:

- First, that all decisions are made taking into account community standards,
- Second, that the decision-making process is completely open and transparent, and
- Finally, that all decisions consider risk versus benefit to the public.

The committee includes representatives from local law enforcement, local government, the community, faculty, aviation experts, and UND's general counsel and office of research development and compliance. In addition, there is usually a reporter from the local newspaper, the Grand Forks Herald, present at all the meetings reporting on the committee to the community. This committee reviews how law enforcement plans to use UASs in different situations, such as looking for a lost child, and also how data and images are secured and stored. We believe that this type of cooperation between law enforcement and research entities is adequately addressing privacy and other ethical issues regarding UASs.

As I mentioned in my opening remarks, in order to help the committee to address issues related to UAS use, in April 2013, UND commissioned a scientific survey of people's attitudes toward using UASs in the counties covered by the FAA Certificate of Authorization used by the Grand Forks Sheriff's office.

The results of this survey have been included with my testimony, and I will only mention that people in the 16 counties of Northeastern North Dakota view UAS uses by law enforcement, first responders, and others very favorably for most uses. Where there is a clear public good, like searching for a lost person or an active shooter, the public is overwhelmingly in favor of using a UAS (80-90%). It is only for things like speeding or other traffic violations that a significant percentage of people are against the use of UASs, although this percentage is still less than 50%. For specific details, see the survey results.

We believe that our approach to using UASs is working. The University of North Dakota, Grand Forks County Sheriff's Department, Northern Plains UAS Test Site, and the North Dakota Air National Guard have conducted hundreds of UAS flights without receiving any complaints. This is largely due to the fact that all of these state and local government agencies have operated their UAS in an ethical manner that respects the privacy and other concerns of the citizens of North Dakota.

Another main concern about this bill is that it will have a negative impact on the development of a UAS industry in North Dakota. We are very concerned about how this bill might impact UND's program of education, training, research and testing of Unmanned Aircraft Systems. UND is a national leader in these areas and was the first university to offer a four-year degree in UAS operation. We have also developed training that is of interest to companies in the UAS industry and to the US Air Force.

We are concerned that passage of this privacy bill could adversely influence how potential UAS manufacturers and investors perceive the state of North Dakota with respect to research and testing of UASs. Through vast collaborations with industry partners and other academic institutions across the country, UND has grown into a national leader for UAS Research, Education and Training. Examples of this include our recent designation as an FAA UAS Test Site, while we continue to pursue emerging opportunities for designation within the FAA UAS Center of Excellence (a sponsored research effort with the FAA). Since 2005, UND has fostered millions of dollars of advanced research through programs like these, developing tangible products with industry leaders such as Rockwell Collins. Collectively, we are creating the next generation of technologies for the next generation of aircraft – all while creating jobs within the industry, and for North Dakota. Legislation that inherently curtails the use of UAS in North Dakota carries with it a risk for slowing the growth of both research programs, and commercial opportunities.

I would add that, specifically concerning the UAS test site, that the bill's preliminary language initially appears to exempt the test site from the legislation. However, the Bill also goes on to include an unequivocal requirement that ALL users of UASs, including testing, training, education and research, must comply with rather onerous documentation requirements. Such documentation is subject to public records laws disclosure, which will be of significant concern to potential test site clients who wish to maintain the confidentiality of their proprietary UAS data.

The state of North Dakota has also made an initial investment in an UAS business park called Grand Sky. Grand Sky is a UAS-focused park planned for 217 acres on Grand Forks Air Force Base. The park would have more than 1 million square feet of space for offices, classrooms, hangars, warehouses, shops and other needs of its tenants. The land will be leased for 50 years by Grand Sky Development from the county, which in turn will lease it from the Air Force. The lease agreement signing ceremony is scheduled for February 18, 2015.

The investment the state has made in these projects indicates that there are many who recognize the importance and the potentially huge economic impact of the UAS industry in North Dakota. The continued viability of the test site and Grand Sky is dependent upon attracting UAS manufacturers to North Dakota.

Finally, the risk of invasion of privacy by UASs is proving to be confined to privately operated UAS, not UAS operated by government agencies who operate in strict compliance to FAA and agency policies and procedures. However, this bill does not address private use of UASs.

Again, we want to emphasize that we understand and appreciate the Committee's concerns about potential invasion of privacy by government UAS is important. At the same time, we believe that the overall interests of the state will be best served if this bill is not passed. We believe that UND and its partners are handling UAS related issues through UND's research compliance committee in a way that best represents the interests of the citizens of North Dakota.

UAS Community Perceptions

The Community Attitudes toward Unmanned Aerial Systems (UAS) Research team was supported by a UND Division of Research Collaborative Research Seed Money grant. The project goal was to assess attitudes toward the use of UAS for a variety of purposes, among North Dakotans living in the 16 counties of the Northeast Region. The study was conducted through a telephone survey (using both cellular and landline telephone numbers) developed by the Research Team (UND faculty: Cindy Juntunen, Abdallah Badahdah, Thomasine Heitkamp, Randy Nedegaard; UND students: Stephen Grey, Laura Parson, and Antonia Forbes). The survey was implemented by the Social Sciences Research Institute at UND, under the direction of Cordell Fontaine.

This Executive Summary provides a brief description of the initial findings of the survey conducted by the Research Team. For questions, please contact the lead investigator, Cindy Juntunen, at 701-777-3740 or cindy.juntunen@und.edu.

Participants

Surveys were conducted with 728 participants. Of that sample, 647 (89%) reported some familiarity with the terms UAVs, UASs, or drones. The sub-sample of 81 (11%) who had no familiarity with the terms were younger (60% were under 34 years) and had less education than the group that was familiar with one of the terms.

The rest of this report includes only data from the 647 participants who had some familiarity with UASs (most were familiar with the term "drone") and completed the entire survey.

Key descriptors for survey completers (N = 647)

- 343 (53%) men; 304 (47%) women
- 575 (88%) White; 45 (7%) Native American; 12 (2%) Latina/o; 27 (4%) Other
- 28 (4%) less than HS diploma; 164 (25%) HS or GED; 259 (40%) some college; 139 (21%) college degree; 47 (9%) graduate degree
- 383 (59%) currently employed for a salary; 264 (41%) were not employed – 119 (18%) retired
- 248 (38%) owned farm or lake land; 391 (60%) did not own land
- 100 (15%) Liberal; 217 (34%) Moderate; 239 (37%) Conservative; 91 (14%) no response
- Age Groups: 18-24 (64 or 10%); 25-34 (86 or 13%); 35-44 (86 or 13%); 45-54 (139 or 21%); 55-64 (138 or 21%); 65+ (134 or 21%)

Summary of Survey Responses

Table 1. Are you concerned about the following items? If so, how concerned are you?

Issue	Not at all	Not	Neutral	Concerned	Extremely
Personal Privacy	243 (38%)	217 (34%)	73 (11%)	81 (13%)	29 (5%)
Airspace Safety	86 (13%)	207 (32%)	124 (19%)	189 (39%)	30 (5%)
Safety on Ground	80 (12%)	218 (34%)	114 (18%)	201 (31%)	27 (4%)
Use by Government	146 (23%)	225 (35%)	138 (21%)	118 (18%)	14 (2%)
Use by business	108 (17%)	242 (38%)	144 (22%)	129 (20%)	16 (3%)
Use by individuals	167 (26%)	246 (38%)	113 (18%)	96 (15%)	18 (3%)
Hijacking or hacking	212 (33%)	274 (42%)	65 (10%)	71 (11%)	12 (2%)

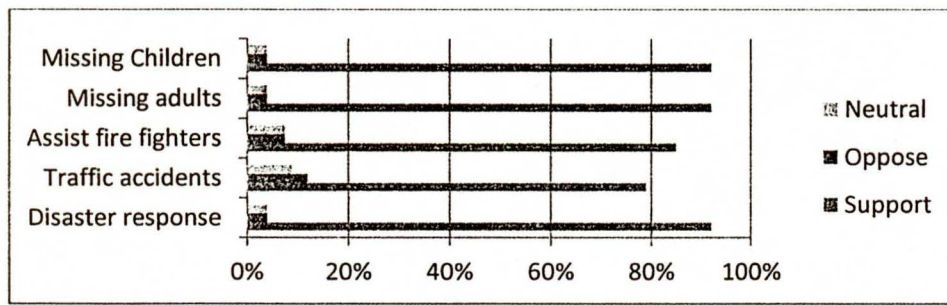
A number of differences emerged across groups in terms of the potential areas of concern listed in Table 1.

1. **People with higher levels of education were significantly more concerned** about personal privacy ($p = .037$), airspace safety ($p = .00$), and safety of people or property on the ground ($p = .03$).
2. **Men were significantly more concerned than women** about airspace safety ($p = .00$), safety of people or property on the ground ($p = .00$), hacking or hijacking ($p = .00$) and use of UASs by the government ($p = .00$).
3. People identifying as **politically Moderate were significantly less concerned** about use of UASs by individuals ($p = .03$) or by business/industry ($p = .00$).
4. In general, **property owners had lower levels of concern** across the issues listed in Table 1 than did non-property owners.
- 5.

To what extent do you support the use of UASs in the following activities?

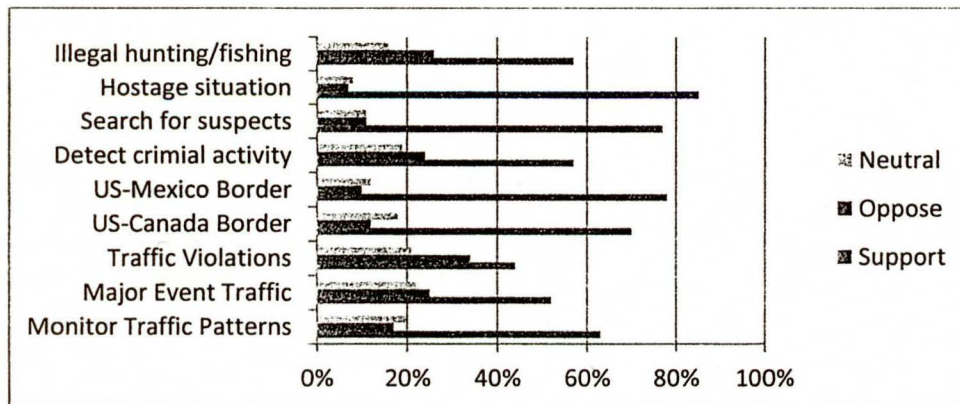
(Group differences are noted with an * below each summary table.)

Search and Rescue Operations



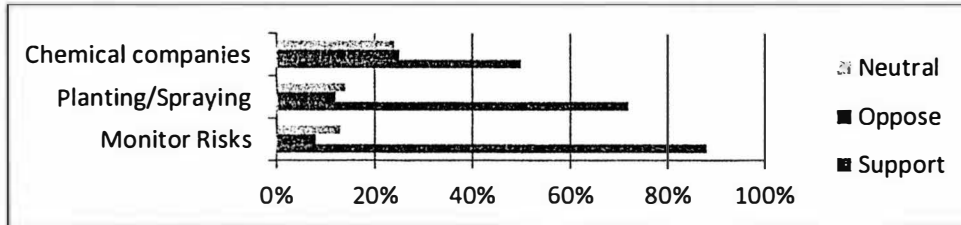
*Those with Moderate political ideology were significantly more supportive ($p = .04$).

Law Enforcement Operations



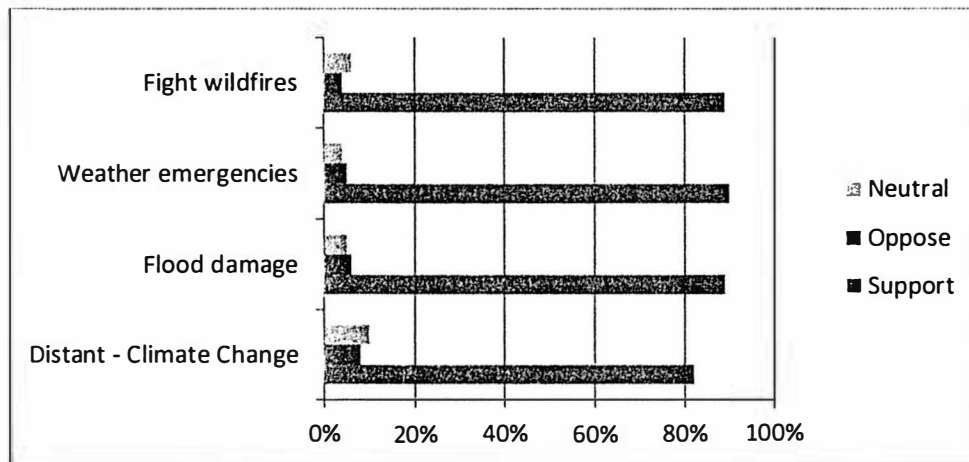
5

Agricultural Operations



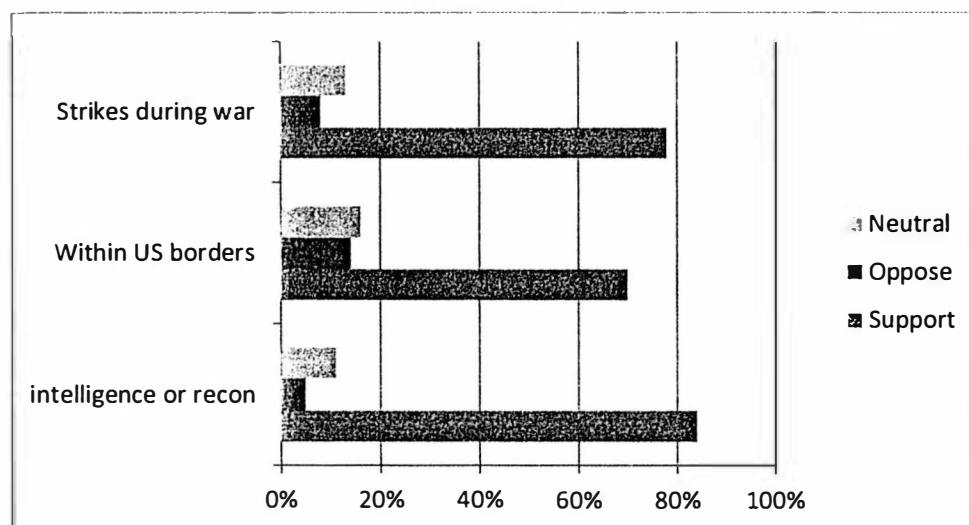
*Those with Moderate political ideology were significantly more supportive ($p = .02$).

Weather & Climate Monitoring

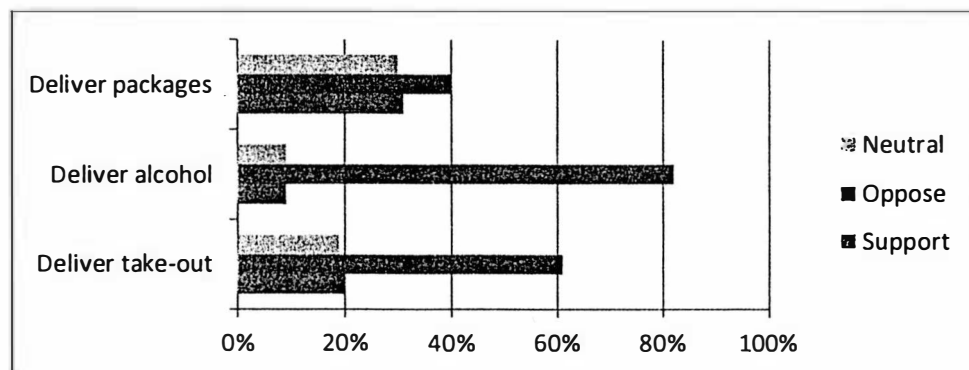


*Those with Moderate political ideology were significantly more supportive ($p = .01$).

Military Operations



Commercial Deliveries



*Men were significantly more supportive than women ($p = .03$).

HL
HB1328
2-4-16

NDLA, H JUD - Shimek, Delores

From: Walton, Susan <susan.walton@email.und.edu>
Sent: Thursday, February 05, 2015 8:01 PM
To: NDLA, H JUD - Shimek, Delores
Subject: Suggested amendments to HB 1328 from UND

Enclosed please find, in response to legislative request, recommended amendments to HB 1328, submitted by the University of North Dakota. Thank you for your assistance—several Committee members have requested that this information be provided to them as quickly as possible.

Please let us know if you need any additional information.

Regards,

Susan Walton

Suggested amendments below:

Under Section 1, Definitions, we suggest retitling this section as “Definitions and Applications,” and adding two subparagraphs following subparagraph 3:

4. This Act applies only to law enforcement agencies of and within the state of North Dakota and its political subdivisions.

5. This Act does not apply to, or restrict in any way, research, education, training, testing, or development efforts undertaken by or in conjunction with a school or educational institution of or within the state of North Dakota and its political subdivisions, nor to public and private collaborators engaged in mutually supported efforts involving research, education, training, testing, or development related to unmanned aircraft systems or unmanned aircraft system technologies and potential applications thereof.

Under Section 8, we suggest the removal of subparagraph 6, which currently reads:

6. The documentation required by this section applies to all uses of unmanned aircraft systems, including testing, training, education and research.

(end suggested amendments)

Thank you again.

Susan

Susan Balcom Walton, M.A., APR
Vice President for University and Public Affairs

University of North Dakota
Twamley Hall, Room 409
264 Centennial Drive, Stop 8179
Grand Forks, North Dakota 58202-8179
Direct line: (701) 777-2501
Fax: (701) 777-2325



2-4-15

Mr. Chairman and members of the Committee, my name is Alan Frazier.

I am employed as a Grand Forks County Deputy Sheriff supervising our Unmanned Aircraft Systems Unit and as an Associate Professor teaching aviation at the University of North Dakota. I have spent over 34 years as a law enforcement officer in local, state and federal agencies. I address you today as a private citizen as the official positions of the Grand Forks County Sheriff's Department and the University of North Dakota have been communicated by Sheriff Rost and Mr.

Corcoran.

My greatest concern with this bill is that it attempts to fix a problem that does not exist. In the 3 years that the Grand Forks Sheriff's Department has operated UAS, we have not received a single complaint. We have however received numerous compliments and been the subject of numerous positive newspaper and magazine articles as well as television documentary and news programs. Our UAS Unit policy has been requested by, and sent to, over 40 agencies

nationwide. Those agencies intend to use it as a model for their UAS Units.

Our written UAS Unit policy emphasizes the importance of safeguarding the privacy of the public we protect and, absent a search warrant, prohibits the use of UAS in a situation that invokes a reasonable expectation of privacy. Our mission sets are reviewed and approved by an independent body, the UND UAS Research Compliance Committee. Since we are the only non-federal agency in North Dakota utilizing UAS, it would appear that the Grand are already addressing the substance of the bill voluntarily.

The Bill does not provide any greater protections than are already provided by current law. The relief outlined in the bill is a civil remedy. The aggrieved party can sue the agency operating the UAS. The ability to sue for a perceived invasion of privacy already exists rendering the Bill's stated violation remedy redundant.

The Bill would impose unnecessary warrant requirements on North Dakota law enforcement agencies at a period when violent and drug related crimes in Western North Dakota are increasing at an unprecedented rate. It would negate the long-standing legal principle of "plain view search". Ample federal case law exists to guide law enforcement's use of aircraft. North Dakota needs the ability to more effectively use technology now more than at any other period in the past. UAS are one of the promising technologies that can assist our law enforcement agencies in trying to keep North Dakota safe for all of us.

If in the future, invasion of privacy by government operated UAS becomes a reality, I will be a strong supporter of a bill that would place reasonable controls on government use of UAS. Until that time, please do not handcuff law enforcement by imposing unreasonable restrictions on the use of this valuable technology.

8
HB 1328

**TESTIMONY OF
ROBERT J BECKLUND
EXECUTIVE DIRECTOR, NORTHERN PLAINS UAS TEST SITE
RELATING TO
HOUSE BILL 1328
FEBRUARY 4, 2015**

Mr. Chairman and Members of the Committee:

I am Robert Becklund, Executive Director of the Northern Plains Unmanned Aircraft Systems Test Site and am offering testimony in opposition to House Bill 1328.

Although this bill appears to be targeted at the Unmanned Aircraft Systems (UAS) utilized by law enforcement agencies, I am concerned that unintended consequences threaten negative impacts to the state's broader efforts and contributions to the national efforts relating to the safe integration of UAS into the National Airspace System (NAS).

Specifically, I feel that the language in this bill may have a dampening effect on the various industries looking to the FAA's UAS Test Sites, including the Northern Plains UAS Test Site (NP UAS TS) to provide them airspace and services to support their UAS research needs. For example, this bill would require the retention of data for 5 years. The costs associated with retaining large amounts of data could be prohibitive to some companies. Additionally, retention of data for long periods of time makes it more prone to hacking or inadvertent release in the public domain. For example, one of the biggest users of this new technology is expected to be the agricultural industry. North Dakota farmers would not want to risk their propriety data to such exposure.

Additionally, this bill is specifically related to the use of UAS for surveillance and is not platform agnostic. If issues of surveillance are the concern, then perhaps all the other platforms that carry or host sensors capable of surveillance should be included: for example, sensors on platforms such as manned aircraft, traffic cameras, police cameras, etc., would likely result in the same concerns as those flown on UAS.

It is my opinion that the existing laws relating to privacy and ethics already cover this evolving technology sufficiently. Most importantly, the NP UAS TS utilizes UND's UAS Research Compliance Committee to address any issues with the ethics or privacy associated with UAS and, to date, have had no complaints associated with any of our UAS operations in ND.

I ask for your consideration to reject HB 1328 as written and I would make myself available to you to answer any questions at your convenience.

#9
HB 1328

**Testimony of Keith Lund, President
Economic Development Association of North Dakota
In Opposition to HB 1328
February 4, 2015**

Chairman Koppelman and members of the House Judiciary Committee, I'm Keith Lund, vice president of the Grand Forks Region Economic Development and president of the Economic Development Association of North Dakota (EDND). On behalf of EDND, I would like to express our opposition to HB 1328.

EDND represents more than 80 state economic development organizations on the front line of economic development efforts throughout North Dakota. The primary purpose of the organization is to support the creation of new wealth and the diversification of North Dakota's economy.

It is my understanding, based on the testimony of law enforcement and others last session, that the protections sought by this bill already exist in state and federal law. The UAS industry is collecting information and reporting on each state's openness to UAS development. A new law that would have the option of limiting the application and use of unmanned systems would place North Dakota in a negative position from this standpoint, which could affect industry's desire to consider the state for their development efforts.

We would urge the committee to give HB 1328 a do not pass recommendation.



#1
HB 1328
2-9-15

**Testimony of Keith Lund, President
Economic Development Association of North Dakota
In Opposition to HB 1328
February 4, 2015**

Chairman Koppelman and members of the House Judiciary Committee, I'm Keith Lund, vice president of the Grand Forks Region Economic Development and president of the Economic Development Association of North Dakota (EDND). On behalf of EDND, I would like to express our opposition to HB 1328.

EDND represents more than 80 state economic development organizations on the front line of economic development efforts throughout North Dakota. The primary purpose of the organization is to support the creation of new wealth and the diversification of North Dakota's economy.

It is my understanding, based on the testimony of law enforcement and others last session, that the protections sought by this bill already exist in state and federal law. The UAS industry is collecting information and reporting on each state's openness to UAS development. A new law that would have the option of limiting the application and use of unmanned systems would place North Dakota in a negative position from this standpoint, which could affect industry's desire to consider the state for their development efforts.

We would urge the committee to give HB 1328 a do not pass recommendation.

#2
HB 1328
2-9-15

**TESTIMONY OF
ROBERT J BECKLUND
EXECUTIVE DIRECTOR, NORTHERN PLAINS UAS TEST SITE
RELATING TO
HOUSE BILL 1328
FEBRUARY 4, 2015**

Mr. Chairman and Members of the Committee:

I am Robert Becklund, Executive Director of the Northern Plains Unmanned Aircraft Systems Test Site and am offering testimony in opposition to House Bill 1328.

Although this bill appears to be targeted at the Unmanned Aircraft Systems (UAS) utilized by law enforcement agencies, I am concerned that unintended consequences threaten negative impacts to the state's broader efforts and contributions to the national efforts relating to the safe integration of UAS into the National Airspace System (NAS).

Specifically, I feel that the language in this bill may have a dampening effect on the various industries looking to the FAA's UAS Test Sites, including the Northern Plains UAS Test Site (NP UAS TS) to provide them airspace and services to support their UAS research needs. For example, this bill would require the retention of data for 5 years. The costs associated with retaining large amounts of data could be prohibitive to some companies. Additionally, retention of data for long periods of time makes it more prone to hacking or inadvertent release in the public domain. For example, one of the biggest users of this new technology is expected to be the agricultural industry. North Dakota farmers would not want to risk their propriety data to such exposure.

Additionally, this bill is specifically related to the use of UAS for surveillance and is not platform agnostic. If issues of surveillance are the concern, then perhaps all the other platforms that carry or host sensors capable of surveillance should be included: for example, sensors on platforms such as manned aircraft, traffic cameras, police cameras, etc., would likely result in the same concerns as those flown on UAS.

It is my opinion that the existing laws relating to privacy and ethics already cover this evolving technology sufficiently. Most importantly, the NP UAS TS utilizes UND's UAS Research Compliance Committee to address any issues with the ethics or privacy associated with UAS and, to date, have had no complaints associated with any of our UAS operations in ND.

I ask for your consideration to reject HB 1328 as written and I would make myself available to you to answer any questions at your convenience.

Paur, Gary A.

#3
HD 1328
2-9-15

From: Ron DePue <depue@aero.und.edu>
Sent: Monday, February 09, 2015 6:44 AM
Subject: Paur, Gary A.
Helicopter questions

Mr. Paur,

Hi my name is Ron DePue. I am the Helicopter Chief Pilot for the University of North Dakota Aerospace. I am responding to questions you posed to UND Aerospace.

1. How low can a helicopter be operated? Well that is a bit of a difficult question to answer with a solid yes or no type response. Here is an extract of the FAA regulation governing the Minimum Safe Altitudes for Aircraft .

FAR 91.119

Except when necessary for takeoff or landing, no person may operate an **aircraft** below the following altitudes:

- (a) Anywhere. **An altitude allowing, if a power unit fails, an emergency landing without undue hazard to persons or property on the surface.**
- (b) Over congested areas. Over any congested area of a city, town, or settlement, or over any open air assembly of persons, an altitude of 1,000 feet above the highest obstacle within a horizontal radius of 2,000 feet of the aircraft.
- (c) Over other than congested areas. An altitude of 500 feet above the surface, except over open water or sparsely populated areas. In those cases, the aircraft may not be operated closer than 500 feet to any person, vessel, vehicle, or structure.
- (d) **Helicopters**, powered parachutes, and weight-shift-control aircraft. **If the operation is conducted without hazard to persons or property on the surface—**
 - (1) **A helicopter may be operated at less than the minimums prescribed in paragraph (b) or (c) of this section, provided each person operating the helicopter complies with any routes or altitudes specifically prescribed for helicopters by the FAA;**

The answer is that there is no general hard minimum altitude published for helicopters other than how high they would have to be in order to land safely in the event of an engine failure. The minimum altitude required for the possible engine failure is very situational and is based upon many variables. Some of the considerations are the altitude/airspeed combination of the flight, the specific model of helicopter, weather conditions, pilot proficiency and the nature of the people and property being over flown to just name a few.

2. What kind of price is associated with a police or law enforcement helicopter? This also is highly dependent. It will depend upon the specific make and model being considered. If an agency is considering a used turbine powered helicopter the price can range anywhere from a few hundred thousand dollars to just under two million dollars. I would also note that this cost is **only the airframe**. The additional cost of the **law enforcement equipment** installed in the airframe could also run into the six digit range.

If you would like to discuss any of your questions further please do not hesitate to call me as I would be glad to assist in any way possible.

Ron DePue
Chief Flight Instructor Helicopter

#1
HB 1328
2-18-15

UAS Test Sites w/ State UAS Legislation

Source: National Conference of State Legislatures

(<http://www.ncsl.org/research/civil-and-criminal-justice/current-uas-state-law-landscape.aspx>)

Alaska, Hawaii, Oregon

Alaska enacted HB 255 creating procedures and standards for law enforcement's use of unmanned aircraft, as well as, regulations for the retention of information collected with UAS. It requires law enforcement agencies to adopt procedures that ensure: the appropriate Federal Aviation Administration flight authorization is obtained; UAS operators are trained and certified; a record of all flights are kept and there is an opportunity for community involvement in the development of the agencies' procedures. Under the law, police may use UAS pursuant to a search warrant, pursuant to a judicially recognized exception to the warrant requirement and in situations not involving a criminal investigation. Images captured with UAS may be retained by police under the law for training purposes or if it is required as part of an investigation or prosecution. The law also authorizes the University of Alaska to develop a training program for operating UAS. The state senate also adopted a resolution HCR 15 to extend the operating time and expand the duties of the state UAS task force.

Oregon's HB 2710 defines a drone as an unmanned flying machine, not including model aircraft. The law allows a law enforcement agency to operate a drone if it has a warrant and for enumerated exceptions including for training purposes. It also requires that a drone operated by a public body be registered with the Oregon Department of Aviation (DOA), which shall keep a registry of drones operated by public bodies. The law grants the DOA rulemaking authority to implement these provisions. It also creates new crimes and civil penalties for mounting weapons on drones and interfering with or gaining unauthorized access to public drones. Under certain conditions a landowner can bring an action against someone flying a drone lower than 400 feet over their property.

The law also requires that the DOA must report to legislative committees on the status of federal regulations and whether UAV's operated by private parties should be registered in a manner similar to the requirement for other aircraft.

The Hawaii Legislature passed SB 1221, which appropriates \$100,000 in funds for two staff positions, contracted through the University of Hawaii, to plan for the creation of three degree and training programs on advanced aviation. One of the programs is a professional unmanned aircraft systems pilot program administered through Hawaii Community College.

Texas

Texas recently enacted HB 912, which enumerates 19 lawful uses for unmanned aircraft, including their use in airspace designated as an FAA test site, their use in connection with a valid search warrant and their use in oil pipeline safety and rig protection. The law creates two new crimes, the illegal use of an unmanned aircraft to capture images and the offense of possessing or distributing the image; both offenses are class C misdemeanors. "Image" is defined in the law as any sound wave, thermal, ultraviolet, visible light or other electromagnetic waves, odor, or other conditions existing on property or an individual located on the property. Additionally, the measure requires the Department of Public Safety to adopt rules for use of UAS by law enforcement and mandates that law enforcement agencies in communities of over 150,000 people make annual reports on their use. Texas HCR 217 altered reporting requirements from the original HB 912.

Virginia, New Jersey

On April 3, 2013, Virginia enacted the first state drone laws in the country with the passage of HB 2012 and SB 1331. The new laws prohibit drone use by any state agencies "having jurisdiction over criminal law enforcement or regulatory violations" or units of local law enforcement until July 1, 2015. Numerous exceptions to the ban are enumerated including enabling officials to deploy drones for Amber Alerts, Blue Alerts and use by the National Guard, by higher education institutions and search and rescue operations. The enacted bills also require the Virginia Department of Criminal Justice Services and other state agencies to research and develop model protocols for drone use by law enforcement in the state. They are required to report their findings to the General Assembly and governor by Nov. 1, 2013.

New York, Massachusetts

None.

Nevada

Nevada AB 507 appropriated \$4,000,000 to the interim Finance Committee for allocation to the Governor's Office of Economic Development for the Unmanned Aerial Vehicle (UAV) program. The funds can only be appropriated if Nevada is selected as a Federal Aviation Administration test site.

North Dakota

North Dakota law, SB 2018 grants \$1 million from the state general fund to pursue designation as a Federal Aviation Administration unmanned aircraft systems test site. If selected, the law would grant an additional \$4 million to operate the site.

Other States w/ UAS Legislation

Source: National Conference of State Legislatures

(<http://www.ncsl.org/research/civil-and-criminal-justice/current-uas-state-law-landscape.aspx>)

2014 Laws Enacted

Illinois enacted SB 2937 creating regulations for how law enforcement can obtain and use information gathered from a private party's use of UAS. The law requires police to follow warrant protocols to compel third parties to share information, and if the information is voluntarily given to police, authorities are required to follow the state's law governing UAS data retention and disclosure. The law also loosens regulations around law enforcement's use of UAS during a disaster or public health emergency.

Indiana is the first state to enact a UAS law in 2014. HB 1009 creates warrant requirements and exceptions for the police use of unmanned aircraft and real time geo-location tracking devices. It also prohibits law enforcement from compelling individuals to reveal passwords for electronic devices without a warrant. If law enforcement obtains information from an electronic service provider pursuant to a warrant, the provider is immune from criminal or civil liability. The law provides that if police seek a warrant to compel information from media entities and personnel, then those individuals must be notified and given the opportunity to be heard by the court concerning issuance of the warrant. The new law also creates the crime of "Unlawful Photography and Surveillance on Private Property," making it a Class A misdemeanor. This crime is committed by a person who knowingly and intentionally electronically surveys the private property of another without permission. The law also requests that the state's legislative council study digital privacy during the 2014 interim.

Iowa enacted HF 2289, making it illegal for a state agency to use a UAS to enforce traffic laws. The new law requires a warrant, or other lawful means, to use information obtained with UAS in a civil or criminal court proceeding. It also requires the department of public safety to develop guidelines for the use of UAS and to determine whether changes to the criminal code are necessary. The department must report on their findings to the general assembly by Dec. 31, 2014.

Louisiana enacted HB 1029, creating the crime of unlawful use of an unmanned aircraft system. The new law defines the unlawful use of an unmanned aircraft system as the intentional use of a UAS to conduct surveillance of a targeted facility without the owner's prior written consent. The crime is punishable by a fine of up to 500 dollars and imprisonment for six months. A second offense can be punished by a fine up to 1000 dollars and one year imprisonment.

North Carolina enacted SB 744 creating regulations for the public, private and commercial use of UAS. The new law prohibits any entity from conducting UAS surveillance of a person or private property and also prohibits taking a photo of a person without their consent for the purpose of distributing it. The law

creates a civil cause of action for those whose privacy is violated. In addition, the law authorizes different types of infrared and thermal imaging technology for certain commercial and private purposes including the evaluation of crops, mapping, scientific research and forest management. Under the law, the state Division of Aviation is required to create a knowledge and skills test for operating unmanned aircraft. All agents of the state who operate UAS must pass the Division's knowledge and skills test. The law enables law enforcement to use UAS pursuant to a warrant, to counter an act of terrorism, to oversee public gatherings, or gather information in a public space. The bill creates several new crimes: using UAS to interfere with manned aircraft, a class H felony; possessing an unmanned aircraft with an attached weapon, a class E felony; the unlawful fishing or hunting with UAS, a class 1 misdemeanor; harassing hunters or fisherman with a UAS, a class 1 misdemeanor; unlawful distribution of images obtained with a UAS, a class 1 misdemeanor for; and operating a UAS commercially without a license, a class 1 misdemeanor. The law addresses launch and recovery sites of UAS, prohibiting their launch or recovery from any State or private property without consent. In addition the law extends the state's current regulatory framework, administered by the chief information officer, for state use of UAS from July to December 31, 2015.

Ohio enacted HB 292 creating the aerospace and aviation technology committee. One of the committee's duties is to research and develop aviation technology including unmanned aerial vehicles.

Tennessee has enacted two new laws in 2014. The first, SB 1777, makes it a class C misdemeanor for any private entity to use a drone to conduct video surveillance of a person who is hunting or fishing without their consent. SB 1892 makes it a Class C misdemeanor for a person to use UAS to intentionally conduct surveillance of an individual or their property. It also makes it a crime to possess those images (Class C Misdemeanor) or distribute and otherwise use them (Class B Misdemeanor). The law also identifies 18 lawful uses of UAS, including the commercial use of UAS under FAA regulations, professional or scholarly research and for use in oil pipeline and well safety.

Utah enacted SB 167, regulating the use of UAS by state government entities. A warrant is now required for a law enforcement agency to "obtain, receive or use data" derived from the use of UAS. The law also establishes standards for when it is acceptable for an individual or other non-governmental entity to submit data to law enforcement. The new law provides standards for law enforcement's collection, use, storage, deletion and maintenance of data. If a law enforcement agency uses UAS, the measure requires that agency submit an annual report on their use to the Department of Public Safety and also to publish the report on the individual agency's website. The new law notes that it is not intended to "prohibit or impede the public and private research, development or manufacture of unmanned aerial vehicles."

Wisconsin enacted SB 196, requiring law enforcement to obtain a warrant before using drones in a place where an individual has a reasonable expectation of privacy. The law also creates two new crimes; "possession of a weaponized drone" and "use of a drone." Use of a drone creates a class A misdemeanor for a person who, with intent, observes another individual in a place where they have a reasonable expectation of privacy. Possession of a weaponized drone is a class H felony.

4

2013 Laws Enacted

Florida SB 92 defines what a drone is and limits their use by law enforcement. Under this legislation, law enforcement may use a drone if they obtain a warrant, there is a terrorist threat, or "swift action" is needed to prevent loss of life or to search for a missing person. The law also enables someone harmed by an inappropriate use of drones to pursue civil remedies and prevents evidence gathered in violation of this code from being admitted in any Florida court.

On April 11, 2013, **Idaho** became the second state to enact a drone law. SB 1134 defines an "Unmanned Aircraft System," requires warrants for their use by law enforcement, establishes guidelines for their use by private citizens and provides civil penalties for damages caused by improper use.

Illinois has enacted two new laws in 2013. Both measures define "drone" as any aerial vehicle that does not carry a human operator. Illinois HB 1652 prohibits anyone from using a drone to interfere with hunters or fisherman. SB 1587 allows drones to be used by law enforcement with a warrant, to counter a terrorist attack, to prevent harm to life or to prevent the imminent escape of a suspect among other situations. If a law enforcement agency uses a drone, the agency must destroy all information gathered by the drone within 30 days, except that a supervisor at the law enforcement agency may retain particular information if there is reasonable suspicion it contains evidence of criminal activity.

The law also requires the Illinois Criminal Justice Information Authority (CJIA) to report on its website every law enforcement agency that owns a drone and the number they own. Each law enforcement agency is responsible for giving this information to the Illinois CJIA.

Maryland's legislature, through HB 100, appropriated \$500,000 for the state's unmanned aerial system test site.

Montana SB 196 limits when information gained from the use of unmanned aerial vehicles may be admitted as evidence in any prosecution or proceeding within the state. The information can be used when it was obtained pursuant to a search warrant, or through a judicially recognized exception to search warrants. The new law defines "unmanned aerial vehicle" as "an aircraft that is operated without direct human intervention from on or within the aircraft," not including satellites.

North Carolina SB 402 places a moratorium on UAS use by state and local personnel unless the use is approved by the Chief Information Officer for the Department of Transportation (CIO). Any CIO granted exception has to be reported immediately to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division. The CIO may determine that there is a need to develop a UAS program within the State of North Carolina. This effort must include the CIO and the Department of

Tennessee law SB 796 addresses the use of drones by law enforcement. The new law enables law enforcement to use drones in compliance with a search warrant, to counter a high-risk terrorist attack and if swift action is needed to prevent imminent danger to life. Evidence obtained in violation of this law is not admissible in state criminal prosecutions. Additionally, those wronged by such evidence can seek civil remedy.

#2
HB1328
2-18-15

PROPOSED AMENDMENTS TO HOUSE BILL NO. 1328

Page 1, line 1, replace "aircraft" with "aerial vehicle"

Page 1, line 6, after "1." insert "Flight data" means imaging or other observation recording.

2. "Flight information" means flight duration, flight path, and mission objective.

3."

Page 1, line 6, after "agency" insert "or agents"

Page 1, line 6, remove "means a person authorized by law, or funded by the state."

Page 1, line 7, replace "to investigate or prosecute offenses against the state" with "has the meaning provided for law enforcement officer in section 12.1-01-04"

Page 1, line 8, replace "2." with "4."

Page 1, line 8, replace the first "aircraft" with "aerial vehicle"

Page 1, line 8, replace the second "aircraft" with "aerial vehicle"

Page 1, line 9, replace "aircraft" with "aerial vehicle. The term does not include satellites."

Page 1, line 10, replace "3." with "5."

Page 1, line 10, replace the first "aircraft" with "aerial vehicle"

Page 1, line 10, replace the second "aircraft" with "aerial vehicle"

Page 1, line 11, replace "aircraft" with "aerial vehicle"

Page 1, replace lines 15 through 24 with:

"Limitations on use of unmanned aerial vehicle system.

1. Information obtained from an unmanned aerial vehicle is not admissible in a prosecution or proceeding within the state unless the information was obtained:

a. Pursuant to the authority of a search warrant; or

b. In accordance with exceptions to the warrant requirement.

2. Information obtained from the operation of an unmanned aerial vehicle may not be used in an affidavit of probable cause in an effort to obtain a search warrant"

Page 2, line 3, replace "aircraft" with "aerial vehicle"

Page 2, line 5, replace "aircraft" with "aerial vehicle"

Page 2, line 6, replace "aircraft" with "aerial vehicle"

Page 2, line 7, replace "aircraft" with "aerial vehicle"

Page 2, line 9, replace "aircraft" with "aerial vehicle"

Page 2, line 11, replace "aircraft" with "aerial vehicle"

Page 2, line 12, replace "aircraft" with "aerial vehicle"

Page 2, line 21, replace "aircraft" with "aerial vehicles"

Page 2, line 23, replace "aircraft" with "aerial vehicles"

Page 2, line 26, replace "aircraft" with "aerial vehicles"

Page 3, line 1, replace "aircraft" with "aerial vehicle"

Page 3, line 2, after "state" insert "or local"

Page 3, line 6, replace "Testing, training, education, and research of unmanned aircraft systems." with "Research, education, training, testing, or development efforts undertaken by or in conjunction with a school or institution of higher education within the state and its political subdivisions, nor to public and private collaborators engaged in mutually supported efforts involving research, education, training, testing, or development related to unmanned aerial vehicle systems or unmanned aerial vehicle system technologies and potential applications."

Page 3, line 8, replace "surveillance" with "use"

Page 3, line 9, replace "aircraft" with "aerial vehicle"

Page 3, line 10, remove "Use of force."

Page 3, line 10, replace "state" with "law enforcement"

Page 3, line 11, replace "aircraft" with "aerial vehicle"

Page 3, line 11, remove "or nonlethal"

Page 3, line 11, remove the second comma

Page 3, line 12, remove "including firearms, pepper spray, bean bag guns, mace, and sound-based weapons"

Page 3, line 13, replace "state" with "law enforcement"

Page 3, line 14, replace "aircraft" with "aerial vehicle"

Page 3, remove lines 22 through 31

Page 4, remove lines 1 through 19

Page 4, line 21, replace "aircraft surveillance" with "aerial vehicle use"

Page 4, line 23, replace "aircraft" with "aerial vehicle"

Page 4, line 24, remove ", including the names of place"

Page 4, line 25, remove "or persons authorized to be subject to surveillance"

Page 4, line 26, replace "certified" with "verified"

PROPOSED AMENDMENTS TO HOUSE BILL NO. 1328

Page 1, line 1, after "A BILL" replace the remainder of the bill with "for an Act to create and enact a new section to chapter 12.1-31 of the North Dakota Century Code, relating to restrictions on the use of unmanned aerial vehicle systems; and to provide a penalty.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

SECTION 1. A new section to chapter 12.1-31 of the North Dakota Century Code is created and enacted as follows:

Prohibited uses of unmanned aerial vehicle systems - Exceptions.

1. For purposes of this section, "unmanned aerial vehicle system" means an unmanned aerial vehicle and associated elements, including communication links and the components that control the unmanned aerial vehicle, which are required for the pilot in command to operate safely and efficiently in state airspace. The term does not include:
 - a. Model flying airplanes or rockets including those that are radio controlled or otherwise remotely controlled and which are used purely for sport or recreational purposes; and
 - b. An unmanned aerial vehicle system used in mapping or resource management.
2. Except as otherwise provided in this section and when used for an emergency response for safety or search and rescue, a person is guilty of a class B misdemeanor if, without the other person's or the owner's written consent, the person uses an unmanned aerial vehicle system to intentionally:
 - a. Conduct surveillance of, gather evidence or collect information about, or photographically or electronically record specifically targeted persons or specifically targeted private property including:
 - (1) An individual or a dwelling owned by an individual and that dwelling's curtilage; and
 - (2) Rural or agricultural land.
 - b. Photograph or otherwise electronically record a person for the purpose of publishing or otherwise publicly disseminating the photograph or recording.
3. a. In any criminal or civil proceeding within the state, information from an unmanned aerial vehicle system is not admissible as evidence unless the information was obtained:
 - (1) Pursuant to the authority of a search warrant; or

- (2) In accordance with judicially recognized exceptions to the warrant requirement.
- b. Information obtained from the operation of an unmanned aerial vehicle system may not be used to obtain a search warrant unless the information was obtained under the circumstances described in this subsection or was obtained through the monitoring of public lands or international borders.
4. The section does not apply to research, education, training, testing, or development efforts undertaken by or in conjunction with a school or educational institution within the state and its political subdivisions, nor to public and private collaborators engaged in mutually supported efforts involving research, education, training, testing, or development related to unmanned aerial vehicle systems or unmanned aerial vehicle system technologies and potential applications."

Renumber accordingly

Per your request--suggested amendments to HB 1328 from UND

Walton, Susan [susan.walton@email.und.edu]

Sent: Friday, February 13, 2015 11:35 AM

To: Delmore, Lois M.

Attachments: 0979DBEC-E318-4C25-9E90-6E~1.png (10 KB)

Dear Representative Delmore:

I hope you're doing well. In response to your request, here are recommended amendments to HB 1328, submitted by the University of North Dakota.

Please let us know if you need any additional information.

Regards,

Susan Walton

Suggested amendments below:

Under Section 1, Definitions, we suggest retitling this section as "Definitions and Applications," and adding two subparagraphs following subparagraph 3:

4. This Act applies only to law enforcement agencies of and within the state of North Dakota and its political subdivisions.

5. This Act does not apply to, or restrict in any way, research, education, training, testing, or development efforts undertaken by or in conjunction with a school or educational institution of or within the state of North Dakota and its political subdivisions, nor to public and private collaborators engaged in mutually supported efforts involving research, education, training, testing, or development related to unmanned aircraft systems or unmanned aircraft system technologies and potential applications thereof.

Under Section 8, we suggest the removal of subparagraph 6, which currently reads:

6. The documentation required by this section applies to all uses of unmanned aircraft systems, including testing, training, education and research.

(end suggested amendments)

Thank you again.

①

Susan

Susan Balcom Walton, M.A., APR
Vice President for University and Public Affairs

University of North Dakota
Twamley Hall, Room 409
264 Centennial Drive, Stop 8179
Grand Forks, North Dakota 58202-8179
Direct line: (701) 777-2501
Fax: (701) 777-2325



②

mephi

CONTACT

Sheriff Bob Rost Demonstrates Why Law Enforcement UAS Usage Needs Regulation

Posted on March 7, 2015 [Leave a Comment](#)

Sheriff Bob Rost's Op-Ed in the March 8th edition of the Grand Forks Herald illustrates why the legislating of Unmanned Aircraft Systems (UAS) is necessary. His article invites readers to blindly accept his arguments while providing only an opaque and convoluted glimpse at the realities of House Bill 1328.

Read Sheriff Bob Rost's Op-Ed: <http://www.grandforksherald.com/opinion/op-ed-columns/3694479-rost-grand-forks-countys-uas-unit-already-protects-privacy>

Read House Bill 1328: <http://www.legis.nd.gov/assembly/64-2015/documents/15-0259-03000.pdf?20150313132143>

Rost begins by arguing that HB 1328 will require the retention of "a wide variety of data and images associated with flights for a period of five years", blatantly misrepresenting of the bill's actual phrasing. In reality, the bill says is that "flight information", which the bill defines as "flight duration, flight path, and mission objective", not data or images, must be retained for five years. This requires the Grand Forks Sheriff Department put into writing where and why they conduct UAS operations, and acts as a check to ensure the technology's power is not abused.

Additionally, the bill says that any imaging or other forms of data lawfully obtained, which do not contain evidence of a crime, may not be retained for more than ninety days. In an attempt to bolster his argument, Rost points to President Obama's presidential directive, which directs federal agencies to delete images and data obtained through UAS flights after 180 days. If Rost is so concerned with Grand Forks resident's privacy, as he demonstrates when he says "our privacy would be much more secure if such images and data were deleted sooner than later", surely he should embrace HB 1328's proposal of only retaining data and images 90 days, half the time that Obama's directive mandates.

Rost continues on to dubiously question why a different set of rules is necessary for unmanned aircraft. He points the US Supreme Court decision which "found that observations that occur from 400 feet above ground level or higher are constitutional". Rost fails to mention that this ruling applied to manned aircraft, not unmanned aircraft. Due to the quick progression of unmanned technology, UAS legislation is lagging behind; this is the very reason HB 1328 is important - it creates a framework in which law enforcement can operate UAS without infringing on citizen's constitutional rights.

In a 2011 presentation at the Unmanned Aircraft System Conference, Alan Frazier, an Associate Professor at the Odegard School of Aerospace Sciences at the University of North Dakota and part-time Deputy Sheriff with the Grand Forks Sheriff Department, spoke openly about potential uses of UAS, including the deployment of a hovering drone that was "not audible or visible" to people below, in order to collect real-time intelligence video, something that would be impossible with a manned aircraft. Rost clearly understands that there is a difference between the ability of manned aircraft, such as helicopters, and UAS.

While the use of UAS is inevitable and while there are many valid uses for the technology in security, law enforcement, and for commercial reasons, this does not discredit the creation of a clear legal framework in which unmanned systems are utilized. Trusting law enforcement to self-restrict and self-regulate has been proven futile throughout history. At the November 16, 2012 Unmanned Aircraft Systems Research and Compliance Committee (UASRCC) meeting, Alan Frazier himself, suggested that the committee look to the American Civil Liberties Union's (ACLU)

HB 1328
3/23/15

1-3

suggested privacy safeguards in developing how the committee protects citizen's privacy. The ACLU suggests that "drones should be deployed by law enforcement only with a warrant, in an emergency, or when there are specific and articulable grounds to believe that the drone will collect evidence relating to a specific criminal act." This suggestion is what Bill 1328 proposes. Additionally, and somewhat ironically, an ACLU representative testified in front of the House Judiciary Committee in February in support of the bill.

To conclude, Bob Rost's Op-Ed exemplified why HB 1328 is an unquestionably important piece of legislature. He glossed over multiple important details and omitted information that the public requires in order to have an informed opinion. North Dakota is a national leader in the UAS industry and it now has the opportunity to be a leader in UAS regulation. We must create a legal framework that allows for both the use of unmanned systems in legitimate law enforcement, while ensuring that the technology does not violate American's right to privacy, assembly, and association.

Posted in: [Domestic Drones](#)

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Comment

HB 1328
3/23/15

2-1

Testimony of the American Civil Liberties Union of North Dakota
In Support of HB 1328 -- An Act to provide for limitations on the use of
~~unmanned~~ aircraft for surveillance

Senate Judiciary Committee

March 23, 2015

On behalf of the ACLU of North Dakota and its members and activists statewide, we commend the effort to regulate the use of unmanned aerial vehicles (UAVs), more commonly referred to as drones, through legislation.

Let there be no mistake: the ACLU of North Dakota is not against the use of advanced technologies in policing. The work of our law enforcement agents is important and we all have an interest in it being done effectively. However, we have serious concerns about the use of unmanned aerial vehicle surveillance technology to collect information about individuals. The pace at which surveillance technology has evolved in recent years has far exceeded the pace at which laws have adapted to protect individuals' privacy. Unregulated, warrantless use of drones could have a chilling effect on the use of public spaces for First Amendment protected activities and could result in discriminatory targeting, institutional abuse, and automated law enforcement. Strict controls are needed to help guide law enforcement in using surveillance technology.

The ACLU of North Dakota testified in full support of the passage of HB 1328 during the bill's hearing before the House Judiciary Committee. Today, I rise in support of HB 1328, but with reservations about the bill as it was amended by the House.

First, I will address the legal reasoning for requiring law enforcement to procure a court issued warrant for targeted surveillance use of an unmanned aerial vehicle and then I will discuss the policy arguments for reinserting language from page 1, Section 2, lines 16-21 that was struck from the original of version of 1328, which prohibits the use of drones for general surveillance.

Many of the most significant potential harms from unchecked use of drones come from the government. Unfortunately, we won't know for many years whether the constitutional protections enshrined in the Fourth Amendment will be able to provide meaningful protections against abuse. There are no Supreme Court cases ruling on drones although the court has allowed some warrantless aerial surveillance from manned aircraft.

In the 1986 decision *California v. Ciraolo*¹, the Supreme Court focused on whether an individual has a privacy interest in being free from aerial surveillance of his backyard. In spite of the defendant's high fence, the court stated there was not a privacy intrusion because "[a]ny member of the public flying in this airspace who glanced down

¹ *California v. Ciraolo*, 476 U.S. 207 (1986).

could have seen everything that these officers observed.” However, the key points to focus on in *Ciraulo* was the court’s focus on the fact that the aircraft was “manned” and the observations of law enforcement only involved “what can be seen with the naked eye.”

Similarly in *Dow Chemical Co. v. United States*², the Supreme Court held that a precision aerial mapping camera taking photographs of a chemical plant was simply conventional photography and “not so revealing of intimate details as to raise constitutional concerns.”³² Notably, the court’s analysis in *Dow* involved the expectation of privacy for a commercial industrial complex, which is less private than a home. More importantly, the ruling in *Dow* can be distinguished here, because drones can be equipped with technology that far exceeds the capabilities of conventional photography. A surveillance drone—which would of course be camera-equipped—differs greatly from the naked human eye. For one thing, the drone can record and store imagery with permanence and accuracy far beyond what the human memory would offer. This storage allows for in-depth and detailed analysis, both at the time of collection and far in the future.

In *Florida v. Riley*³, the court authorized a search where a police officer flew over a greenhouse and spotted marijuana through a broken pane in a greenhouse roof.³³ Unsurprisingly, many law enforcement agencies, including the FBI, read this case law as granting them almost unfettered authority to collect information using drones.³⁴ However, in *Kyllo v. United States*⁴, a case involving law enforcement use of thermal imaging technology for surveillance, the court held that a warrant was required for such surveillance as “heat seeking technology would almost certainly shrink the realm of guaranteed privacy.” The *Kyllo* court also recognized that it would be required in the future to take into account “more sophisticated systems that are already in use or development.”

Additionally, a recent decision in *U.S. v. Jones*⁵, a concurrence joined by five justices held that ubiquitous, long term tracking of an individual raised constitutional concerns. Five justices in that case agreed that “the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society’s expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual’s car for a very long period.” While this case involved tracking through a GPS device, the underlying reasoning could well apply to drone technology.

Drones are not like helicopters or any other police vehicle. They are not subject to the same practical limitations as helicopters, which are costly and require trained, human pilots, launch pads and flight and ground crews. Rather, drones are less

² *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986).

³ *Florida v. Riley*, 488 U.S. 445 (1989).

⁴ *Kyllo v. United States*, 533 U.S. 27 (2001).

⁵ *United States v. Jones*, 132 S. Ct. 935 (2011).

expensive, can be small and quiet, and therefore – unlike helicopters – every single town and city in the state could conceivably afford to fly multiple drones. Because of these fundamental differences, they are particularly well-suited to secret surveillance, so they need specific legal controls.

Drones can be an extremely powerful surveillance tool, and their use by law enforcement must be subject to strict limitations, as should all government power. In addition to the courts, this legislative body has a duty to uphold the Constitution and should enact statutory protections that bolster those found in the Fourth Amendment.

Drones should be subject to strict regulation to ensure that their use does not eviscerate the privacy that North Dakotans have traditionally enjoyed and rightly expect. Innocent North Dakotans should not have to worry that police will scrutinize their activities with drones.

Prior to its amendment and passage in the House, HB 1328 struck the right balance between individual privacy protections and law enforcement use of drones, by permitting law enforcement to use drones only in emergencies or with a probable cause warrant issued by a judge. The bill as you see it today has been stripped of language that we believe is necessary to protecting the privacy of North Dakotans in their everyday lives guaranteed to them by the Fourth Amendment.

Although the current bill correctly provides that information obtained without a warrant is not admissible in a legal proceeding, it must be recognized that the protections enshrined in the Fourth Amendment extend beyond the admissibility of evidence in court. Specifically, the Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]” This right exists independently from any court proceeding. Accordingly, while the exclusion of unlawfully obtained evidence is a proper remedy within the context of a court proceeding, the underlying harm that remedy is designed to protect against is the violation of a citizen’s Fourth Amendment rights in the first instance.

As such we strongly encourage this committee to amend HB 1328 to reinsert the language found in the original version of the bill on page 1, section 2, lines 16-21. Simply doing so will ensure law enforcement can only use drones to conduct surveillance of persons or property within North Dakota if permitted by a court issued warrant, exigent circumstances, and other exceptions to warrant requirements. In short it prevents the use of drones as day-to-day automated law enforcement officers.

Before drones become ubiquitous in our airspace, we need clear privacy rules so that we can enjoy this new technology without sacrificing our privacy. HB 1328 would provide rules and ensure that drones are prohibited for indiscriminate mass surveillance, with their use by police only permitted where there are grounds to believe they will collect evidence relating to a specific instance of criminal wrongdoing, or in emergencies. North Dakota should join Florida, Idaho, Illinois, Montana, North Carolina, Oregon,

2-4

Tennessee, Texas and Virginia in passing legislation to regulate government deployment of this powerful technology.

On behalf of ACLU of North Dakota and its members and activists statewide, we urge you to give HB 1328 a Do Pass recommendation.

HB 1328
3/23/15

3-1
3/23/15
HB1328

The Technology

There are hundreds of different types of Unmanned Aerial Vehicles (UAVs), as drones are formally known. They can be as large as commercial aircraft or as small as hummingbirds, and include human remotely guided aircraft as well as autonomous, self-guided vehicles. They include:

- **Large fixed-wing aircraft.** The largest drones currently in use, such as the Israeli-made Eitan, are about the size of a Boeing 737 jetliner. The Eitan's wingspan is 86 feet, and it can stay aloft for 20 hours and reach an altitude of 40,000 feet.² In Pakistan and Afghanistan, the U.S. military and CIA deploy Predators and Reapers armed with surveillance capability as well as missiles capable of destroying a moving vehicle from thousands of feet in the air.
- **Small fixed-wing aircraft.** Smaller fixed-wing aircraft are the current favorite for domestic deployment. The Houston police department, for example, recently tested the ScanEagle, made by Boeing subsidiary Insitu.⁴ The ScanEagle is 5 ½ feet long with a wingspan of 10 feet, and it can climb to 19,500 feet and stay aloft for more than 24 hours.
- **Backpack craft.** Another class of craft is designed to be carried and operated by a single person. The hand-launched AeroVironment Raven, for example, weighs 4 pounds, has a wingspan of 4.5 feet and a length of 3 feet, can fly up to 14,000 feet and stay aloft for up to 110 minutes. Individual hobbyists have also built a number of drones in this size range.
- **Hummingbirds.** A tiny drone called the Nano Hummingbird was developed for the Pentagon's Defense Advanced Research Projects Agency (DARPA) by AeroVironment. Intended for stealth surveillance, it can fly up to 11 miles per hour and can hover, fly sideways, backwards and forwards, for about 8 minutes. It has a wingspan of 6.5 inches and weighs only 19 grams—less than a single AA battery.
- **Blimps.** Some blimps are envisioned as high-altitude craft, up to 300 feet in diameter, that would compete with satellites, while others would be low-altitude craft that would allow the police to monitor the streets. Supporters say they are more cost-effective than other craft due to their ability to stay aloft for extended periods.

Sixty-fourth
Legislative Assembly
of North Dakota

HOUSE BILL NO. 1328

4-1
3/23/15

Introduced by

Representatives Rick C. Becker, Beadle, Boehning, Kasper, Klemin, Ruby, Thoreson, Toman
Senators Anderson, Hogue, Larsen, Unruh

1 A BILL for an Act to provide for limitations on the use of unmanned aircraft for surveillance.

2 **BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:**

3 **SECTION 1.**

4 **Definitions.**

5 As used in this Act:

- 6 1. "Law enforcement agency" means a person authorized by law, or funded by the state,
7 to investigate or prosecute offenses against the state.
8 2. "Unmanned aircraft" means any aircraft that is operated without the possibility of direct
9 human intervention within or on the aircraft.
10 3. "Unmanned aircraft system" means an unmanned aircraft and associated elements,
11 including communication links and the components that control the unmanned aircraft,
12 which are required for the pilot in command to operate safely and efficiently in state
13 airspace.

14 **SECTION 2.**

15 **Prohibited use of unmanned aircraft system.**

- 16 1. Except as provided in section 4 of this Act, a law enforcement agency may not use an
17 unmanned aircraft for surveillance of a person within the state or for the surveillance of
18 personal or business property located within the borders of the state to gather
19 evidence or other information pertaining to criminal conduct, or conduct in violation of
20 a statute or regulation except to the extent authorized in a warrant issued by a court
21 which satisfies the requirements of the Constitution of North Dakota.
22 2. Warrants to conduct surveillance with an unmanned aircraft may be issued only in the
23 investigation of a felony. Unmanned aircraft may not be used to conduct investigations
24 of misdemeanors, traffic infractions, or other non-felony violations of law.

Testimony for Senate Judiciary Committee
Regarding House Bill 1328

March 23, 2015

Sara Nelson

Good morning Mister Chairman and members of the committee and thank you for hearing my testimony in favor of House Bill 1328. My name is Sara Nelson and I am journalist and soon-to-be graduate student in Washington DC. I have been researching the use of domestic Unmanned Aircraft Systems in law enforcement for many months and have focused the crux of my research on the testing of systems in North Dakota. I spent my formative years here in Bismarck, graduating from Century High School. After university, I began working as a journalist in Berlin, focusing on privacy issues related to indiscriminate surveillance by the National Security Agency.

In a recent Op-Ed in the Grand Forks Herald, a member of law enforcement questioned why it is necessary to have different regulations for unmanned and manned aircraft systems. The op-ed pointed to a Supreme Court decision in which observations that occur from 400 feet about ground level or higher were found to be constitutional (1). The Op-Ed failed to mention, however, that this 1989 Supreme Court decision applies to manned aircraft, not unmanned aircraft (2). While the difference in surveillance capability between manned and unmanned aircraft systems is apparent, I will illustrate their difference with the following example. In a 2011 presentation at the Unmanned Aircraft System Conference, a member of law enforcement who is also a member of UND's Unmanned Aircraft Research and Compliance Committee, spoke openly about potential uses of unmanned systems in North Dakota. The list included the deployment of a hovering drone that was "not audible or visible" to people below, in order to collect real-time intelligence video (3). This example demonstrates one way in which unmanned systems' surveillance capabilities differ greatly from manned systems such as helicopters.

It was also argued by law enforcement that Bill 1328 will require the retention of "a wide variety of data and images associated with flights for a period of five years", pointing out that the retention of such data would infringe on people's right to privacy (1). The Op-Ed pointed to the federal government's presidential directive, which directs federal agencies to delete images and data obtained through unmanned aircraft flights after 180 days. In reality, Bill 1328 says is that "flight information", which the bill defines as "flight duration, flight path, and mission objective", not data or images, must be retained for five years (4). In fact, the bill says that any imaging or other forms of data lawfully obtained, which do not contain evidence of a crime, may **not** be retained for more than ninety days. To clarify, House Bill 1328's proposed retention of data and images is half the time that the federal directive mandates.

When grappling with how to regulate powerful technologies, it is a common practice of both law enforcement and the larger intelligence community to say that the technologies are being used only on very bad people in very extreme cases. This is an effective strategy because the public sees themselves as vastly different from those bad people. In response to this argument, I would urge the committee to remember that liberty is eroded at the ~~fringes~~ *fringes*.

While the use of unmanned systems is inevitable and while there are many valid uses for the technology in border and national security, law enforcement, and for commercial reasons, this does not discredit the creation of a clear legal framework in which the systems are to be utilized. The bill includes within it exceptions which allow law enforcement to remain agile and quickly respond to exigent circumstances. North Dakota is a national leader in the unmanned aircraft industry and it now has the opportunity to be a leader in unmanned aircraft regulation. We must create a legal framework that allows for both the use of unmanned systems in legitimate law enforcement, while ensuring that the technology does not violate American's

right to privacy, assembly, and association. While I am disappointed by the bill's noticeable lack of regulation regarding the arming of the unmanned systems, I strongly urge you to vote for this bill. Thank you for your time.

Sources:

- 1) <http://www.grandforksherald.com/opinion/op-ed-columns/3694479-rost-grand-forks-countys-uas-unit-already-protects-privacy>
- 2) <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=488&invol=445>
- 3) http://www.uasresearch.com/playavid5/PlayAVid.aspx?path=AI_Frazier_-_Small_UAS_and_LE_-_UAS_Conference_Oct_2011&nam=&titl=AI%20Frazier **Begins around 8:24 mark**
- 4) [http://www.legis.nd.gov/assembly/64-2015/documents/15-0259-02000.pdf?](http://www.legis.nd.gov/assembly/64-2015/documents/15-0259-02000.pdf?20150307193659)
20150307193659

Testimony
House Bill 1328
Senate Judiciary Committee
Fort Lincoln Room

March 23, 2015

Thomas K. Kenville

Good Morning Mr. Chairman and members of the Judiciary Committee. For the record my name is Thomas K. Kenville, Tommy to most, from Grand Forks. I have been involved in the aviation industry the past 28 years in North Dakota and more importantly directly involved in the UAS industry since 2006. I appreciate the opportunity to testify in opposition to HB 1328.

Background

Consultant to the Center for Innovation since 2007
Organized the first Team North Dakota UAS tradeshow in 2007 with the Department of Commerce
In 2010 founded Unmanned Applications Institute International (UAI), a UAV company
Founded the Great Plains Chapter of Association of Unmanned Vehicles Systems International (trade group)
Initiated the North Dakota Airspace Integration Team
Raised equity to move UAS manufacturing from Florida to North Dakota, Governor's Announcement on February 13, 2015 (Altavian/Comdel)

Section 1

Why does this bill single out UAS (unmanned aerial vehicle system) by placing limitations on an industry that the state has systematically invested in since 2006?

Currently in this room we have a minimum of 18 cameras, video, or data recording devices yet we want to single out UAS data?

Today we have laws in place and a previous case set the standard for privacy protection. Dow Chemical Co. V. United States: Aerial Surveillance (1986) and the Fourth Amendment (copy provided to chair)

Website: <https://supreme.justia.com/cases/federal/us/476/227/>

Section 2

N/A

Section 3

Current law requires **CAUSE** to obtain a warrant no matter what type of vehicle or means of gathering information is utilized. A piloted aircraft can gather the data with the same camera and unmanned ground vehicles can gather the same data.

The attempt to put limitations on the use of UAS is a national effort that is on the second attempt in North Dakota. North Dakota is still the leader in the UAS industry because of forward looking leadership, including

6-2

legislators, supporting this growing industry since the mid 2000's and supporting it still today. The people of North Dakota are protected currently through the case stated above. North Dakota does not need additional red tape or red flags to slow progress for the growth of the UAS industry in North Dakota.

Section 4

Why create a different set of regulations for one method of gathering data ... Who is going to manage the new law?

Are we assuming only government or law enforcement will use UAS? Is a private investigator allowed to use UAS without these new rules? Today a manned aircraft can be used to collect data and information --- the public is protected by the Fourth Amendment. Again North Dakota should not single out any one area as there are rules in place to protect the privacy of North Dakotans.

Section 5

N/A

Section 6

Documentation: The Federal Aviation Administration (FAA) controls the use of all aircraft. As for data, there currently are rules in place for data and law enforcement agencies – the Fourth Amendment. It is not necessary to single out a specific method of obtaining the data.

In summary, North Dakota is a leader in the UAS industry thanks to the vision of politicians like yourselves, over the years, doing what is right to support this new industry. North Dakota does not need to join the minority of other states to pass laws that will put up barriers to the growth of the UAS industry. The citizens of North Dakota are currently protected from new technology like UAV's under the Fourth Amendment as proven by the Supreme Court ruling of 1986.

Thank you for the opportunity to testify today in opposition to HB 1328.

Tommy Kenville
UAI International
4200 James Ray Drive
Grand Forks ND 58203
Tom@Uaiinternational.com
Cell-218.779.9950

HB 1328
3/23/15

FAA NOTICE OF PROPOSED RULE MAKING

A forty-eight page notice to develop rules for conducting UAS operations and defining requirements for operation.

The FAA also notes that, because UAS-associated technologies are rapidly evolving at this time, new technologies could come into existence after this rule is issued or existing technologies may evolve to the extent that they establish a level of reliability sufficient to allow those technologies to be relied on for risk mitigation. These technologies may alleviate some of the risk concerns that underlie the provisions of this rulemaking like the line of sight rule. Accordingly, the FAA invites comments as to whether the final rule should relax operating restrictions on small UAS equipped with technology that addresses the concerns underlying the operating limitations of this proposed rule, for instance through some type of deviation authority (such as a letter of authorization or a waiver).

The FAA also notes that privacy concerns have been raised about unmanned aircraft operations. Although these issues are beyond the scope of this rulemaking, recognizing the potential implications for privacy and civil rights and civil liberties from the use of this technology, and consistent with the direction set forth in the Presidential Memorandum, Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (February 15, 2015), the Department and FAA will participate in the multi-stakeholder engagement process led by the National Telecommunications and Information Administration (NTIA) to assist in this process regarding privacy, accountability, and transparency issues concerning commercial and private UAS use in the NAS. **We also note that state law and other legal protections for individual privacy may provide recourse for a person whose privacy may be affected through another person's use of a UAS.**

The FAA conducted a **privacy impact assessment (PIA)** of this rule as required by section 522(a)(5) of division H of the FY 2005 Omnibus Appropriations Act, Public Law 108-447, 118 Stat. 3268 (Dec. 8, 2004) and section 208 of the E-Government Act of 2002, Public Law 107-347, 116 Stat. 2889 (Dec. 17, 2002). The assessment considers any impacts of the proposed rule on the privacy of information in an identifiable form. The FAA has determined that this proposed rule would impact the FAA's handling of personally identifiable information (PII). **As part of the PIA that the FAA conducted as part of this rulemaking, the FAA analyzed the effect this impact might have on collecting, storing, and disseminating PII and examined and evaluated protections and alternative**

HB 1328
3/23/15

information handling processes in developing the proposed rule in order to mitigate potential privacy risks.

As proposed, the process for granting unmanned aircraft operator certificates with a small UAS rating would be brought in line with the process for granting traditional airman certificates. Thus, the privacy implications of this rule to the privacy of the information that would be collected, maintained, stored, and disseminated by the FAA in accordance with this rule are the same as the privacy implications of the FAA's current airman certification processes. These privacy impacts have been analyzed by the FAA in the following Privacy Impact Assessments for the following systems: Civil Aviation Registry Applications (AVS Registry); the Integrated Airman Certification and Ratings Application (IACRA); and Accident Incident Database. These Privacy Impact Assessments are available in the docket for this rulemaking and at <http://www.dot.gov/individuals/privacy/privacy-impact-assessments#FederalAviationAdministration> (FAA).

5. Public Aircraft Operations

This proposed rule would also not apply to public aircraft operations with small UAS that are not operated as civil aircraft. This is because public aircraft operations, such as those conducted by the Department of Defense, the National Aeronautics and Space Administration, and the National Oceanic and Atmospheric Administration, are not required to comply with civil airworthiness or airman certification requirements to conduct operations. However, these operations are subject to the airspace and air-traffic rules of part 91, which include the "see and avoid" requirement of § 91.113(b).

Because unmanned aircraft operations currently are incapable of complying with § 91.113(b), the FAA has required public aircraft operations that use unmanned aircraft to obtain an FAA-issued Certificate of Waiver or Authorization (COA) providing the public aircraft operation with a waiver/deviation from the "see and avoid" requirement of § 91.113(b).

The existing COA system has been in place for over eight years, and has not caused any significant human injuries or other significant adverse safety impacts. Accordingly, this proposed rule would not abolish the COA system. However, this proposed rule would provide public aircraft operations with greater flexibility by giving them the option to declare an operation to be a civil operation and comply with the provisions of proposed part 107 instead of seeking a COA from the FAA. Because proposed part 107 would address the risks associated with small UAS

operations, there would be no adverse safety effects from allowing public aircraft operations to be voluntarily conducted under proposed part 107.

PART 91—GENERAL OPERATING AND FLIGHT RULES

Subpart E—Special Rule for Model Aircraft

101.41

Applicability

This subpart prescribes the rules governing the operation of a model aircraft that meets all of the following conditions as set forth in section 336 of Public Law 112–95:

- (a) The aircraft is flown strictly for hobby or recreational use;
- (b) The aircraft is operated in accordance with a community-based set of safety guidelines and within the programming of a nationwide community-based organization;
- (c) The aircraft is limited to not more than 55 pounds unless otherwise certified through a design, construction, inspection, flight test, and operational safety program administered by a community-based organization;
- (d) The aircraft is operated in a manner that does not interfere with and gives way to any manned aircraft; and (e) When flown within 5 miles of an airport, the operator of the aircraft provides the airport operator and the airport air traffic control tower (when an air traffic facility is located at the airport) with prior notice of the operation.

§ 101.43

Endangering the safety of the National Airspace System.

No person may operate model aircraft so as to endanger the safety of the national airspace system.

of seeking a COA from the FAA. Because proposed part 107 would address the risks associated with small UAS operations, there would be no adverse safety effects from allowing public aircraft operations to be voluntarily conducted under proposed part 107.³⁴

6. Model Aircraft

Proposed part 107 would not apply to model aircraft that satisfy all of the criteria specified in section 336 of Public Law 112–95. Section 336 of Public Law 112–95 defines a model aircraft as an “unmanned aircraft that is—(1) capable of sustained flight in the atmosphere; (2) flown within visual line of sight of the person operating the aircraft; and (3) flown for hobby or recreational purposes.”³⁵ Because section 336 of Public Law 112–95 defines a model aircraft as an “unmanned aircraft,” a model aircraft that weighs less than 55 pounds would fall into the definition of small UAS under this rule.

However, Public Law 112–95 specifically prohibits the FAA from promulgating rules regarding model aircraft that meet all of the following statutory criteria:³⁶

- The aircraft is flown strictly for hobby or recreational use;
- The aircraft is operated in accordance with a community-based set of safety guidelines and within the programming of a nationwide community-based organization;
- The aircraft is limited to not more than 55 pounds unless otherwise certified through a design, construction, inspection, flight test, and operational safety program administered by a community-based organization;
- The aircraft is operated in a manner that does not interfere with and gives way to any manned aircraft; and
- When flown within 5 miles of an airport, the operator of the aircraft provides the airport operator and the airport air traffic control tower (when an air traffic facility is located at the airport) with prior notice of the operation.

Because of the statutory prohibition on FAA rulemaking regarding model aircraft that meet the above criteria, model aircraft meeting these criteria would not be subject to the provisions of proposed part 107. Likewise, operators of model aircraft excepted from part 107 by the statute would not

need to hold an unmanned aircraft operator's certificate with a small UAS rating. However, the FAA emphasizes that because the prohibition on rulemaking in section 336 of Public Law 112–95 is limited to model aircraft that meet all of the above statutory criteria, model aircraft weighing less than 55 pounds that fail to meet all of the statutory criteria would be subject to proposed part 107.

In addition, although Public Law 112–95 excepted certain model aircraft from FAA rulemaking, it specifically states that the law's exception does not limit the Administrator's authority to pursue enforcement action against those model aircraft operators that “endanger the safety of the national airspace system.”³⁷ This proposed rule would codify the FAA's enforcement authority in part 101 by prohibiting model aircraft operators from endangering the safety of the NAS.

The FAA also notes that it recently issued an interpretive rule explaining the provisions of section 336 and concluding that “Congress intended for the FAA to be able to rely on a range of our existing regulations to protect users of the airspace and people and property on the ground.”³⁸ In this interpretive rule, the FAA gave examples of existing regulations the violation of which could subject model aircraft to enforcement action. Those regulations include:

- Prohibitions on careless or reckless operation and dropping objects so as to create a hazard to persons or property (14 CFR 91.13 and 91.15);
- Right-of-way rules for converging aircraft (14 CFR 91.113);
- Rules governing operations in designated airspace (14 CFR part 73 and §§ 91.126 through 91.135); and
- Rules relating to operations in areas covered by temporary flight restrictions and notices to airmen (NOTAMs) (14 CFR 91.137 through 91.145).³⁹

The FAA notes that the above list is not intended to be an exhaustive list of all existing regulations that apply to model aircraft meeting the statutory criteria of Public Law 112–95, section 336. Rather, as explained in the interpretive rule, “[t]he FAA anticipates that the cited regulations are the ones

that would most commonly apply to model aircraft operations.”⁴⁰

7. Moored Balloons, Kites, Amateur Rockets, and Unmanned Free Balloons

Lastly, proposed part 107 would not apply to moored balloons, kites, amateur rockets, and unmanned free balloons. These types of aircraft currently are regulated by the provisions of 14 CFR part 101. Because these aircraft are already incorporated into the NAS through part 101 and because the safety risks associated with these specific aircraft are already mitigated by the regulations of part 101, there is no need to make these aircraft subject to the provisions of proposed part 107.

C. Definitions

Proposed part 107 would create a new set of definitions to address the unique aspects of a small UAS. Those proposed definitions are as follows.

1. Control Station

Proposed part 107 would define a “control station” as an interface used by the operator to control the flight path of the small unmanned aircraft. In a manned aircraft, the interface used by the pilot to control the flight path of the aircraft is a part of the aircraft and is typically located inside the aircraft flight deck. Conversely, the interface used to control the flight path of a small unmanned aircraft is typically physically separated from the aircraft and remains on the ground during aircraft flight. Defining the concept of a control station would clarify the interface that is considered part of the small UAS under this regulation.

2. Corrective Lenses

Proposed part 107 would also define “corrective lenses” as spectacles or contact lenses. As discussed in the Operating Rules section of this preamble, this proposed rule would require the operator and/or visual observer to have visual line of sight of the small unmanned aircraft with vision that is not enhanced by any device other than corrective lenses. This is because spectacles and contact lenses do not restrict a user's peripheral vision while other vision-enhancing devices may restrict that vision. Because peripheral vision is necessary in order for the operator and/or visual observer to be able to see and avoid other air traffic in the NAS, this proposed rule would limit the circumstances in which vision-enhancing devices other than spectacles or contact lenses may be used.

³⁴ The FAA notes that section 334(b) of Public Law 112–95 requires the FAA to develop standards regarding the operation of public UAS by December 31, 2015.

³⁵ Sec. 336(c) of Public Law 112–95.

³⁶ Sec. 336(a) of Public Law 112–95.

³⁷ Sec. 336(b) of Public Law 112–95.

³⁸ *Interpretation of the Special Rule for Model Aircraft*, 79 FR 36172, 36175 (June 25, 2014). This document was issued as a notice of interpretation and has been in effect since its issuance on June 25, 2014. However, we note that the FAA has invited comment on this interpretation, and may modify the interpretation as a result of comments that were received.

³⁹ *Id.* at 36175–76.

⁴⁰ *Id.* at 36176.

HB 1328
3/23/15

7-5

3. Operator and Visual Observer

Because of the unique nature of small UAS operations, this proposed rule would create two new crewmember positions: The operator and the visual observer. These positions are discussed further in section III.D.1 of this preamble.

4. Small Unmanned Aircraft

Public Law 112-95 defines a "small unmanned aircraft" as "an unmanned aircraft weighing less than 55 pounds."⁴¹ This statutory definition of small unmanned aircraft does not specify whether the 55-pound weight limit refers to the total weight of the aircraft at the time of takeoff (which would encompass the weight of the aircraft and any payload on board), or simply the weight of an empty aircraft.

This proposed rule would define a small unmanned aircraft as an unmanned aircraft weighing less than 55 pounds, including everything that is on board the aircraft. The FAA proposes to interpret the statutory definition of small unmanned aircraft as referring to total weight at the time of takeoff because heavier aircraft generally pose greater amounts of public risk in the event of an accident. In the event of a crash, a heavier aircraft can do more damage to people and property on the ground. The FAA also notes that this approach would be similar to the approach that the FAA has taken with other aircraft, such as large aircraft, light-sport aircraft, and small aircraft.⁴²

5. Small Unmanned Aircraft System (Small UAS)

This proposed rule would define a small UAS as a small unmanned aircraft and its associated elements (including communication links and the components that control the small unmanned aircraft) that are required for the safe and efficient operation of the small unmanned aircraft in the NAS. Except for one difference, this proposed definition would be similar to the definition of "unmanned aircraft system" provided in Public Law 112-95.⁴³ The difference between the two definitions is that the proposed definition in this rule would not refer to a pilot-in-command because, as

discussed further in this preamble, this proposed rule would create a new position of operator to replace the traditional manned-aviation positions of pilot and pilot-in-command for small UAS operations.

6. Unmanned Aircraft

Lastly, this proposed rule would define an unmanned aircraft as an aircraft operated without the possibility of direct human intervention from within or on the aircraft. This proposed definition would codify the definition of "unmanned aircraft" specified in Public Law 112-95.⁴⁴

D. Operating Rules

As discussed earlier in this preamble (section III.A), instead of a single omnibus rulemaking that applies to all small UAS operations, the FAA has decided to proceed incrementally and issue a rule governing small UAS operations that pose the least amount of risk. Subpart B of this proposed rule would specify the operating constraints of these operations. The FAA emphasizes that it intends to conduct future rulemaking(s) to incorporate into the NAS small UAS operations that pose a greater level of risk than the operations that would be permitted by this proposed rule. However, those operations present additional safety issues that the FAA needs more time to address. In the meantime, under this proposed rule, operations that could be conducted within the proposed operational constraints would be incorporated into the NAS.

The FAA also considered whether to further subdivide small UAS into different categories of unmanned aircraft that would be regulated differently based on their weight, operational characteristics, and operating environment. This subdivision would have been based on five category groups (Groups A through E). Each of these groups would have been regulated based on its specific weight and operating characteristics.

This is the framework that the FAA used in its initial approach to this rulemaking. However, because this framework attempted to integrate a wide range of UAS operations posing different risk profiles whose integration raised policy questions on which data was either limited or unavailable, the FAA's initial approach would have been unduly burdensome on all UAS groups that would have been covered under that approach. For example, UAS in Group A, which posed the least safety risk under the FAA's initial framework,

would have been required to: (1) Obtain a permit to operate (PTO) from the FAA, which would have to be renewed after one year; (2) file quarterly reports with the FAA providing their operational data; (3) establish a level of airworthiness that would be sufficient to obtain an airworthiness certification (the initial approach would have merged airworthiness certification into the PTO); (4) obtain a pilot certificate by passing a knowledge test, a practical test, and completing required ground training with an FAA-certificated instructor; (5) obtain a NOTAM from the FAA prior to conducting certain UAS operations (the operator would do this by filing notice with the FAA); and (6) maintain records documenting the complete maintenance history of the UAS.

After extensive deliberation, the FAA ultimately determined that such a regulatory framework was too complex, costly, and burdensome for both the public and the FAA. The FAA then examined the entire small UAS category of aircraft (unmanned aircraft weighing less than 55 pounds) in light of the new authority provided for under section 333 of Public Law 112-95 and determined that appropriate operational risk mitigations could be developed to allow the entire category of small UAS to avoid airworthiness certification and be subject to the least burdensome level of regulation that is necessary to protect the safety and security of the NAS. Furthermore, the FAA decided to also substantially simplify the operational limitations and airman (operator) certification requirements in a manner that would equally accommodate all types of small UAS business users with the least amount of complexity and regulatory burden.

The FAA believes that treating small UAS as a single category without airworthiness certification would accommodate a large majority of small UAS businesses and other non-recreational users of UAS. The operational limits in this proposed rule would mitigate risk associated with small UAS operations in a way that would provide an equivalent level of safety to the NAS with the least amount of burden to business and other non-recreational users of even the smallest UAS. The FAA invites comments, with supporting documentation, on whether the regulation of small UAS should be further subdivided based on the size, weight, and operating environment of the small UAS.

1. Micro UAS Classification

In addition to part 107 as proposed, the FAA is considering including a

⁴¹ Sec. 331(6) of Public Law 112-95.

⁴² See 14 CFR 1.1 (referring to "takeoff weight" for large, light-sport, and small aircraft in the definitions for those aircraft).

⁴³ Sec. 331(9) of Public Law 112-95. Public Law 112-95 defines an "unmanned aircraft system" as "an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system."

⁴⁴ Sec. 331(8) of Public Law 112-95.

HB 1328
3/23/15

micro UAS classification. This classification would be based on the UAS ARC's recommendations, as well as approaches adopted in other countries that have a separate set of regulations for micro UAS.

In developing this micro UAS classification, the FAA examined small UAS policies adopted in other

countries. In considering other countries' aviation policies, the FAA noted that each country has its unique aviation statutory and rulemaking requirements, which may include that country's unique economic, geographic, and airspace density considerations. Canada is our only North American neighbor with a regulatory framework

for small UAS. The chart below summarizes Transport Canada's operational limitations for micro UAS (4.4 pounds (2 kilograms) and under) and compares it with the regulatory framework in proposed part 107 as well as the micro UAS classification that the FAA is considering.

COMPARISON OF CANADIAN RULES GOVERNING MICRO UAS CLASS WITH PROVISIONS OF PROPOSED PART 107 AND MICRO UAS SUB-CLASSIFICATION

Provision	Canada	Small UAS NPRM	Micro UAS Sub-classification
Definition of Small UAS	Up to 4.4 lbs (2 kg)	Up to 55 lbs (24 kg)	Up to 4.4 lbs (2 kg).
Maximum Altitude Above Ground	300 feet	500 feet	400 feet.
Airspace Limitations	Only within Class G airspace	Allowed within Class E in areas not designated for an airport. Otherwise, need ATC permission. Allowed within Class B, C and D with ATC permission. Allowed in Class G with no ATC permission.	Only within Class G airspace.
Distance from people and structures	100 feet laterally from any building, structure, vehicle, vessel or animal not associated with the operation and 100 feet from any person.	Simply prohibits UAS operations over any person not involved in the operations (unless under a covered structure).	Flying over any person is permitted.
Ability to extend operational area	No	Yes, from a waterborne vehicle	No.
Autonomous operations	No	Yes	No.
Aeronautical knowledge required	Yes; ground school	Yes; applicant would take knowledge test.	Yes; applicant would self-certify.
First person view permitted	No	Yes, provided operator is visually capable of seeing the small UAS.	No.
Operator training required	Yes, ground school	No	No.
Visual observer training required	Yes	No	No.
Operator certificate required	No	Yes (must pass basic UAS aeronautical test).	Yes (no knowledge test required).
Preflight safety assessment	Yes	Yes	Yes.
Operate within 5 miles of an airport	No	Yes	No.
Operate in a congested area	No	Yes	Yes.
Liability insurance	Yes, \$100,000 CAN	No	No.
Daylight operations only	Yes	Yes	Yes.
Aircraft must be made out of frangible materials.	No	No	Yes.

The FAA is considering the following provisions for the micro UAS classification:

- The unmanned aircraft used in the operation would weigh no more than 4.4 pounds (2 kilograms). This provision would be based on the ARC's recommendations and on how other countries, such as Canada, subdivide their UAS into micro or lightweight UAS;
- The unmanned aircraft would be made out of frangible materials that break, distort, or yield on impact so as to present a minimal hazard to any person or object that the unmanned aircraft collides with. Examples of such materials are breakable plastic, paper, wood, and foam. This provision would be based on the ARC's recommendations;
- During the course of the operation, the unmanned aircraft would not exceed

an airspeed of 30 knots. This provision would be based on the ARC's recommendation, which was concerned with damage that could be done by unmanned aircraft flying at higher speeds;

- During the course of the operation, the unmanned aircraft would not travel higher than 400 feet above ground level (AGL). This provision would be based on the ARC's recommendations;
- The unmanned aircraft would be flown within visual line of sight; first-person view would not be used during the operation; and the aircraft would not travel farther than 1,500 feet away from the operator. These provisions would be based on ARC recommendations and Canada's requirements for micro UAS;
- The operator would maintain manual control of the flight path of the unmanned aircraft at all times, and the operator would not use automation to

control the flight path of the unmanned aircraft. This provision would be based on ARC recommendations and Canada's requirements for micro UAS;

- The operation would be limited entirely to Class G airspace. This provision would be based on Canada's requirements for micro UAS; and
- The unmanned aircraft would maintain a distance of at least 5 nautical miles from any airport. This provision would be based on Canada's requirements for micro UAS.

The operational parameters discussed above may provide significant additional safety mitigations. Specifically, a very light (micro) UAS operating at lower altitudes and at lower speeds, that is made up of materials that break or yield easily upon impact, may pose a much lower risk to persons, property, and other NAS users than a UAS that does not operate within these

HB1328
3/23/15

parameters. Additionally, limiting the micro UAS operation entirely to Class G airspace, far away from an airport, and in close proximity to the operator (as well as limiting the unmanned aircraft's flight path to the operator's constant manual control) would significantly reduce the risk of collision with another aircraft. Accordingly, because the specific parameters of a micro UAS operation described above would provide additional safety mitigation for those operations, the FAA's micro UAS approach would allow micro UAS to operate directly over people not involved in the operation. Under the FAA's micro UAS approach, the operator of a micro UAS also would be able to operate using a UAS airman certificate with a different rating (an unmanned aircraft operator certificate with a micro UAS rating) than the airman certificate that would be created by proposed part 107. No knowledge test would be required in order to obtain an unmanned aircraft operator certificate with a micro UAS rating; instead, the applicant would simply submit a signed statement to the FAA stating that he or she has familiarized him or herself with all of the areas of knowledge that are tested on the initial aeronautical knowledge test that is proposed under part 107.

The FAA is also considering whether to require, as part of the micro UAS approach, that the micro UAS be made out of frangible material. A UAS that is made out of frangible material presents a significantly lower risk to persons on the ground, as that UAS is more likely to shatter if it should impact a person rather than injuring that person. Without the risk mitigation provided by frangible-material construction, the FAA would be unable to allow micro UAS to operate directly over a person not involved in the operation. The FAA notes that, currently, a majority of fixed-wing small UAS are made out of frangible materials that would satisfy the proposed requirement. The FAA invites comments on whether it should eliminate frangibility from the micro UAS framework.

The FAA also invites commenters to submit data and any other supporting documentation on whether the micro UAS classification should be included in the final rule, and what provisions the FAA should adopt for such a classification. The FAA invites further comments, with supporting documentation, estimating the costs and benefits of implementing a micro UAS approach in the final rule. Finally, the FAA invites comments to assess the risk to other airspace users posed by the lesser restricted integration of micro

UAS into the NAS. The FAA notes, however, that due to statutory constraints, the FAA would be unable to eliminate the requirement to hold an airman certificate and register the unmanned aircraft even if it were to adopt a micro UAS approach in the final rule.

During the course of this rulemaking, the FAA also received a petition for rulemaking from UAS America Fund LLC. This petition presented the FAA with an alternative approach to regulating micro UAS, complete with a set of regulatory provisions that would be specific to micro UAS operations. Because the FAA was already in the process of rulemaking at the time this petition was filed, pursuant to 14 CFR 11.73(c), the FAA will not treat this petition as a separate action, but rather, will consider it as a comment on this rulemaking. Accordingly, the FAA has placed a copy of UAS America Fund's rulemaking petition in the docket for this rulemaking and invites comments on the suggestions presented in this petition. Any comments received in response to the proposals in the petition will be considered in this rulemaking.

2. Operator and Visual Observer

As briefly mentioned earlier, this proposed rule would create two new crewmember positions: An operator and a visual observer. The FAA proposes these positions for small UAS operations instead of the traditional manned-aircraft positions of pilot, flight engineer, and flight navigator. This is being proposed because, by their very nature, small UAS operations are different from manned aircraft operations, and this necessitates a different set of qualifications for crewmembers.

i. Operator

The FAA proposes to define an operator as a person who manipulates the flight controls of a small UAS. Flight controls include any system or component that affects the flight path of the aircraft. The position of operator would be somewhat analogous to the position of a pilot who controls the flight of a manned aircraft. However, the FAA proposes to create the position of an operator rather than expand the existing definition of pilot to emphasize that, even though the operator directly controls the flight of the unmanned aircraft, the operator is not actually present on the aircraft.

The FAA notes that even though a small UAS operator is not a pilot, the operator would still be considered an airman and statutorily required to obtain an airman certificate. The

statutory flexibility provided in section 333 of Public Law 112-95 is limited to airworthiness certification and does not extend to airman certification. Thus, as mentioned previously, the FAA's statute prohibits a person without an airman certificate from serving in any capacity as an airman with respect to a civil aircraft used or intended to be used in air commerce.⁴⁵ The statute defines an "airman," in part, as an individual who, as a member of the crew, navigates the aircraft when under way.⁴⁶ Because under this proposed rule the operator would be a member of the crew and would navigate the small unmanned aircraft when that aircraft is under way, an operator would be an airman as defined in the FAA's statute.

Accordingly, the operator would statutorily be required to obtain an airman certificate in order to fly the small unmanned aircraft.

The FAA proposes to codify this statutory requirement in § 107.13(a), which would require a person who wishes to serve as an operator to obtain an unmanned aircraft airman certificate with a small UAS rating. An unmanned aircraft airman certificate would be a new type of airman certificate that would be created by this proposed rule specifically for UAS operators to satisfy the statutory requirement for an airman certificate. The certificate necessary to operate small UAS would have a small UAS rating. The FAA anticipates that certificates used to operate UAS not subject to this proposed rule would have different certification requirements. The specific details of this certificate are discussed further in section III.E of this preamble.

The FAA also proposes to give each operator the power and responsibility typically associated with a pilot-in-command (PIC) under the existing regulations. Under the existing regulations, the PIC "is directly responsible for, and is the final authority as to the operation of [the] aircraft."⁴⁷ The PIC position provides additional accountability for the safety of an operation by: (1) Ensuring that a single person on board the aircraft is accountable for that operation; and (2) providing that person with the authority to address issues affecting operational safety.

An accountability system, such as the existing PIC concept, would provide similar benefits for small UAS operations. Accordingly, the FAA proposes, in § 107.19(a), to make each operator: (1) Directly responsible for the

⁴⁵ 49 U.S.C. 44711(a)(2)(A).

⁴⁶ 49 U.S.C. 40102(a)(8)(A).

⁴⁷ 14 CFR 91.3(a).

HB 1328
3/23/15

small UAS operation, and (2) the final authority as to the small UAS operation. To provide further clarity as to the operator's authority over the small UAS operation, proposed § 107.49(b) would require that each person involved in the small UAS operation perform the duties assigned by the operator.

The FAA also considered providing the operator with the emergency powers available to the PIC under 14 CFR 91.3(b). Under § 91.3(b), a PIC can deviate from FAA regulations to respond to an in-flight emergency. However, the FAA does not believe that this power is necessary for the operator because a small unmanned aircraft is highly maneuverable and much easier to land than a manned aircraft. Thus, in an emergency, an operator should be able to promptly land the small unmanned aircraft in compliance with FAA regulations. Accordingly, the FAA proposes not to provide an operator with the emergency powers available to the PIC under § 91.3(b). The FAA invites comments on this issue.

The FAA also does not believe that it is necessary to create a separate "operator-in-command" position for small UAS operations. The existing regulations create a separate PIC position because many manned aircraft are operated by multiple pilots. Thus, it is necessary to designate one of those pilots as the accountable authority for the operation. By contrast, only one operator is needed for a small UAS flight operation even though additional non-operator persons could be involved in the operation. Thus, at this time, it is not necessary to create an operator-in-command position. The FAA invites comments on whether a separate operator-in-command position should be created for small UAS operations.

The FAA finally notes that the term "operate" is currently a defined term in 14 CFR 1.1 that is used in manned-aircraft operations. While, for purposes of proposed part 107, the proposed definition of "operator" would supersede any conflicting definitions in § 1.1, the FAA invites comments as to whether defining a new crewmember position as an "operator" would cause confusion with the existing terminology. If so, the FAA invites suggestions as to an alternative title for this crewmember position.

ii. Visual Observer

To assist the operator with the proposed see-and-avoid and visual-line-of-sight requirements discussed in the next section of this preamble, the FAA proposes to create the position of a visual observer. Under this proposed rule, a visual observer would be defined

as a person who assists the small unmanned aircraft operator in seeing and avoiding other air traffic or objects aloft or on the ground. The visual observer would do this by augmenting the operator as the person who must satisfy the see-and-avoid and visual-line-of-sight requirements of this proposed rule. As discussed in more detail below, an operator must always be capable of seeing the small unmanned aircraft. However, if the operation is augmented by at least one visual observer, the operator is not required to exercise this capability, as long as the visual observer maintains a constant visual-line-of-sight of the small unmanned aircraft.

The FAA emphasizes that, as proposed, a visual observer is not a required crewmember, as the operator could always satisfy the pertinent requirements him- or herself. Under this proposed rule, an operator could, at his or her discretion, use a visual observer to increase the flexibility of the operation. The FAA notes, however, that as discussed in III.D.3.i of this preamble, even if a visual observer is used to augment the operation, a small unmanned aircraft would still be required by § 107.33(c) to always remain close enough to the control station for the operator to be capable of seeing that aircraft.

To ensure that the visual observer can carry out his or her duties, the FAA proposes, in § 107.33(b), that the operator be required to ensure that the visual observer is positioned in a location where he or she is able to see the small unmanned aircraft in the manner required by the proposed visual-line-of-sight and see-and-avoid provisions of §§ 107.31 and 107.37. The operator can do this by specifying the location of the visual observer. The FAA also proposes to require, in § 107.33(d), that the operator and visual observer coordinate to: (1) Scan the airspace where the small unmanned aircraft is operating for any potential collision hazard; and (2) maintain awareness of the position of the small unmanned aircraft through direct visual observation. This would be accomplished by the visual observer maintaining visual contact with the small unmanned aircraft and the surrounding airspace and then communicating to the operator the flight status of the small unmanned aircraft and any hazards which may enter the area of operation so that the operator can take appropriate action.

To make this communication possible, this proposed rule would require, in § 107.33(a), that the operator and visual observer maintain effective

communication with each other at all times. This means that the operator and visual observer must work out a method of communication prior to the operation that allows them to understand each other, and utilize that method in the operation. The FAA notes that this proposed communication requirement would permit the use of communication-assisting devices, such as radios, to facilitate communication between the operator and visual observer from a distance. The FAA considered requiring the visual observer to be stationed next to the operator to allow for unassisted oral communication, but decided that this requirement would be unduly burdensome, as it is possible to have effective oral communication through a communication-assisting device. The FAA invites comments on whether the visual observer should be required to stand close enough to the operator to allow for unassisted verbal communication.

Under this proposed rule, the visual observer would not be permitted to manipulate any controls of the small UAS, share in operational control, or exercise operation-related judgment independent of the operator. Because the visual observer's role in the small UAS operation would be limited to simply communicating what he or she is seeing to the operator, the visual observer would not be an "airman" as defined in the FAA's statute.⁴⁸ Consequently, as proposed, the visual observer would not statutorily be required to obtain an airman certificate.⁴⁹

While an airman certificate for a visual observer is not statutorily mandated, the FAA considered requiring that the visual observer obtain an airman certificate.⁵⁰ However, due to the fact that this proposed rule would not permit the visual observer to

⁴⁸ 49 U.S.C. 40102(a)(8). This statute defines an "airman" as an individual: "(A) in command, or as pilot, mechanic, or member of the crew, who navigates aircraft when under way; (B) except to the extent the Administrator of the Federal Aviation Administration may provide otherwise for individuals employed outside the United States, who is directly in charge of inspecting, maintaining, overhauling, or repairing aircraft, aircraft engines, propellers, or appliances; or (C) who serves as an aircraft dispatcher or air traffic control-tower operator." The visual observer's limited role in the operation of a small UAS would not meet any of these criteria.

⁴⁹ See 49 U.S.C. 44711(a)(2)(A) (prohibiting a person without an airman certificate from serving in any capacity as an airman with respect to a civil aircraft used or intended to be used in air commerce).

⁵⁰ This requirement would be imposed pursuant to 49 U.S.C. 44701(a)(5), which gives FAA the power to prescribe regulations that it finds necessary for safety in air commerce.

HB 1328
3/23/15

manipulate the small UAS controls or exercise any independent judgment or operational control, the FAA believes that certification of visual observers would not result in significant safety benefits. Accordingly, the FAA is not proposing to require airman certification for visual observers. The FAA invites comments on whether an airman certificate should be required to serve as a visual observer. If so, what requirements should an applicant meet in order to obtain a visual observer airman certificate? The FAA also invites comments regarding the costs and benefits of requiring airman certification for visual observers.

3. See-and-Avoid and Visibility Requirements

Turning to the see-and-avoid and visibility requirements mentioned in the previous section, one of the issues with small UAS operations is that the small UAS operator cannot see and avoid other aircraft in the same manner as a pilot who is inside a manned aircraft. Because at this time there is no technology that can provide an acceptable see-and-avoid replacement for human vision for small UAS operations, this proposed rule would limit small UAS operations to within the visual line of sight of the operator and a visual observer. This proposed rule would also impose requirements to ensure maximum visibility for the operation of the small UAS and ensure that small unmanned aircraft always yield the right-of-way to other users of the NAS.

i. See-and-Avoid

Currently, 14 CFR 91.113(b) imposes a requirement on all aircraft operations that, during flight, "vigilance shall be maintained by each person operating an aircraft so as to see and avoid other aircraft." This see-and-avoid requirement is at the heart of the FAA's regulatory structure mitigating the risk of aircraft colliding in midair. As such, in crafting this proposed rule, the FAA sought a standard under which the small UAS operator would have the ability to see and avoid other aircraft similar to that of a manned-aircraft pilot.

The FAA considered proposing that a UAS operator be permitted to exercise his or her see-and-avoid responsibilities through technological means, such as onboard cameras. We recognize that technology is developing that could provide an acceptable substitute for direct human vision in UAS operations. FAA does not, however, believe this technology has matured to the extent that would allow it to be used safely in

small UAS operations in lieu of visual line of sight. The FAA has not identified an acceptable technological substitute for the safety protections provided by direct human vision in small UAS operations at this time. For these reasons and consistent with the statutory direction provided for in section 333, the FAA proposes to require, in §§ 107.31 and 107.37(a)(1), that the operator (and visual observer, if used) must be capable of maintaining a visual line of sight of the small unmanned aircraft throughout that aircraft's entire flight with human vision that is unaided by any device other than spectacles or contact lenses.

If a visual observer is not used, the operator must exercise this capability and maintain watch over the small unmanned aircraft during flight. However, if an operation is augmented by at least one visual observer, then the visual observer can be used to satisfy the visual-line-of-sight requirements, as long as the operator always remains situated such that he or she can exercise visual-line-of-sight capability.

The FAA notes that this proposed requirement does not require the person maintaining visual line of sight to constantly watch the unmanned aircraft for every single second of that aircraft's flight. The FAA understands and accepts that this person may lose sight of the unmanned aircraft for brief moments of the operation. This may be necessary either because the small UAS momentarily travels behind an obstruction or to allow the person maintaining visual line of sight to perform actions such as scanning the airspace or briefly looking down at the small UAS control station. The visual-line-of-sight requirement of this proposed rule would allow the person maintaining visual line of sight brief moments in which he or she cannot directly see the small unmanned aircraft provided that the person is able to see the surrounding operational area sufficiently well to carry out his or her visual-line-of-sight-related responsibilities. Anything more than brief moments during which the person maintaining visual line of sight is unable to see the small unmanned aircraft would be prohibited under this proposed rule.

To ensure that the operator's vision (and that of a visual observer, if used) of the small unmanned aircraft is sufficient to see and avoid other aircraft in the NAS, the proposed rule would require that the operator's or visual observer's vision of the small unmanned aircraft must be sufficient to allow him or her to: (1) Know the small unmanned aircraft's location; (2) determine the

small unmanned aircraft's attitude, altitude, and direction; (3) observe the airspace for other air traffic or hazards; and (4) determine that the small unmanned aircraft does not endanger the life or property of another. Because maintaining this type of awareness in real-time is a concentration-intensive activity, proposed § 107.35 would limit an operator or visual observer to operating no more than one small UAS at the same time.⁵¹

Binoculars, onboard cameras, and other vision-enhancing devices (aside from spectacles or contact lenses) cannot be used to satisfy this proposed requirement because those devices restrict the user's peripheral field of vision. Since a pilot often uses peripheral vision to identify other aircraft in the NAS,⁵² a device that restricts peripheral vision hinders the user's ability to see other aircraft. However, the FAA recognizes that there are advantages to using vision-enhancing devices, such as those used when utilizing camera video transmitted to a screen at the operator's station (also known as first person view) when conducting inspections of bridges or towers. This proposed rule is not intended to prohibit the use of those devices. Rather, the proposed visual-line-of-sight requirement requires simply that at least one person involved in the operation, either the operator or a visual observer, must maintain an unenhanced visual line of sight of the small unmanned aircraft. Anyone else involved in the operation may use a vision-enhancing device (including first-person view) so long as that device is not used to meet the proposed requirements of §§ 107.31 and 107.37. The FAA invites comments on this proposed visual-line-of-sight requirement. The FAA also invites suggestions, with supporting documentation, for other ways in which a first-person-view device could be used by the operator without compromising the risk mitigation provided by the proposed visual-line-of-sight requirement. The FAA also invites comments on whether it should permit operations beyond visual line of sight in its final rule, for example through deviation authority, once the pertinent technology matures to the extent that it

⁵¹ The use of a visual observer would not be sufficient to allow an operator to operate more than one small UAS because the operator would still need to maintain sufficient concentration to react to the information provided to him or her by the visual observer.

⁵² Pilot Safety brochure: "Pilot Vision." http://www.faa.gov/pilots/safety/pilotsafetybrochures/media/pilot_vision.pdf. A copy of this document is also available in the docket for this rulemaking.

HB 1382
3/23/15

7-10

can be used to safely operate beyond visual line of sight. If so, what level of validation should the technology be subject to in order to demonstrate reliability? For example, should the FAA use its existing certification or validation methodologies to evaluate UAS technology?

ii. Additional Visibility Requirements

To further ensure that a small UAS operator/visual observer can see and avoid other aircraft, the FAA proposes (1) to limit the operation of small UAS to daylight-only operations, and (2) to impose weather-minimum visibility requirements

First, the FAA proposes, in § 107.29, to prohibit the operation of a small UAS outside the hours of official sunrise and sunset. The Federal Air Almanac provides tables which are used to determine sunrise and sunset at various latitudes. The FAA considered proposing to allow small UAS operations outside the hours of official sunrise and sunset, recognizing that this would integrate a greater quantity of small UAS operations into the NAS. However, the FAA has decided to propose limiting small UAS use to daylight-only operations due to the relatively small size of the small unmanned aircraft and the difficulty in being able to see it in darker environments to avoid other airspace users. The FAA also notes that most small unmanned aircraft flights under this proposed rule would take place at low altitudes, and flying at night would limit the small UAS operator's ability to see people on the ground and take precautions to ensure that the small unmanned aircraft does not pose a hazard to those people. Moreover, allowing small UAS operations outside of daylight hours would require equipment specifications (such as a lighting system emitting a certain minimum amount of light) and airworthiness certification requirements that are contrary to the FAA's goal of a minimally burdensome rule for small unmanned aircraft. The FAA also notes that, for manned aircraft operations, the regulations provide for very specific lighting systems necessary to safely operate in the NAS. Those regulations require, among other things: (1) Lighting system angles; (2) lighting system intensity; (3) lighting system color and position; (4) lighting system installation; and (5) lighting system configuration.⁵³ This level of regulation and airworthiness certification would be beyond the level of a minimally burdensome rule encompassing low-risk

operation that is contemplated by section 333 of Public Law 112-95.

The FAA realizes the proposed daylight-only operations requirement may affect the ability to use small unmanned aircraft in more northern latitudes (specifically Alaska), and is willing to consider any reasonable mitigation which would ensure that an equivalent level of safety is maintained while operating in low-light areas. The FAA welcomes public comments with suggestions on how to effectively mitigate the risk of operations of small unmanned aircraft during low-light or nighttime operations.

In addition, to ensure that small UAS operators and visual observers have the ability to see and avoid other aircraft, the FAA is proposing to require, in § 107.51(c), a minimum flight visibility of 3 statute miles (5 kilometers) from the control station for small UAS operations. A visibility of 3 statute miles currently is required for aircraft operations in controlled airspace.⁵⁴ The FAA also requires a 3-mile visibility in the context of other unmanned aircraft operations (moored balloons and kites).⁵⁵ The reason for the increased visibility requirement is to provide the small UAS operator with additional time after seeing a manned aircraft to maneuver and avoid an accident or incident with the manned aircraft.

In addition, the FAA is proposing to require, in § 107.51(d), that the small unmanned aircraft must be no less than: (1) 500 feet (150 meters) below clouds; and (2) 2,000 feet (600 meters) horizontal from clouds. This is similar to the requirements imposed by 14 CFR 91.155 on aircraft operating in controlled airspace under visual flight rules. The FAA proposes to impose these cloud-clearance requirements on small UAS operations because, as mentioned previously, small UAS operators do not have the same see-and-avoid capability as manned-aircraft pilots.

iii. Yielding Right of Way

Now that we have discussed how a small UAS operator sees other users of the NAS, we turn to how that operator avoids those users. In aviation, this is accomplished through right-of-way rules, which pilots are required to follow when encountering other aircraft. These rules specify how pilots should respond to other NAS users based on the types of aircraft or the operational scenario.

The operation of small UAS presents challenges to the application of the

traditional right-of-way rules. The smaller visual profile of the small unmanned aircraft makes it difficult for manned pilots to see and, therefore, avoid the unmanned aircraft. This risk is further compounded by the difference in speed between manned aircraft and the often slower small unmanned aircraft. Because of these challenges, the FAA proposes to require, in § 107.37(a)(2), that the small UAS operator must always be the one to initiate an avoidance maneuver to avoid collision with any other user of the NAS. Optimally, the small UAS operator should give right-of-way to all manned aircraft in such a manner that the manned aircraft is never presented with a see-and-avoid decision or the impression that it must maneuver to avoid the small UAS.

When a small UAS operator encounters another unmanned aircraft, each operator must exercise his or her discretion to avoid a collision between the aircraft. In extreme situations where collision is imminent, the small UAS operator must always consider the safety of people, first and foremost, over the value of any equipment, even if it means the loss of the unmanned aircraft. To further mitigate the risk of a mid-air collision, the FAA also proposes to codify, in § 107.37(b), the existing requirement in 14 CFR 91.111(a), which prohibits a person from operating an aircraft so close to another aircraft as to create a collision hazard.

4. Containment and Loss of Positive Control

As discussed above, one of the issues unique to UAS operations is the possibility that during flight, the UAS operator may become unable to directly control the unmanned aircraft due to a failure of the control link between the aircraft and the operator's control station. This failure is known as a loss of positive control. Because the UAS operator's direct connection to the aircraft is funneled through the control link, a failure of the control link could have significant adverse results.

To address this issue, the FAA proposes a performance-based operator-responsibility standard built around the concept of a confined area of operation. Confining the flight of a small unmanned aircraft to a limited area would allow the operator to become familiar with the area of operation and to create contingency plans for using the environment in that area to mitigate the risk associated with possible loss of positive control. For example, the operator could mitigate loss-of-control risk to people on the ground by setting up a perimeter and excluding people

⁵³ See 14 CFRs 23.1381 through 23.1401.

⁵⁴ See 14 CFR 91.115.

⁵⁵ 14 CFR 101.13(a)(3).

HB 1328
3/23/15

7-11

not involved with the operation from the operational area. The operator could also mitigate risk to other aircraft by notifying the local air traffic control of the small UAS operation and the location of the confined area in which that operation will take place. As a result of risk-mitigation options that are available to the operator in a confined area of operation, the FAA proposes to mitigate the risk associated with loss of aircraft control by confining small unmanned aircraft to a limited area of operation.

As an alternative method of addressing this issue, the FAA considered technological approaches such as requiring a flight termination system that would automatically terminate the flight of the small unmanned aircraft if the operator lost positive control of that aircraft. However, as previously discussed, due to the size and weight of a small UAS, operations subject to this proposed rule would not pose the same level of risk as other operations regulated by the FAA. Since small UAS operations subject to this rule pose a lower level of risk, there are operational alternatives available to mitigate their risk to an acceptable level without imposing an FAA requirement for technological equipment and airworthiness certification requirements. Therefore, this proposed rule would not mandate the use of a flight termination system nor would this proposed rule mandate the equipment of any other navigational aid technology. Instead, the FAA invites comments on whether a flight termination system or other technological equipment should be required and how it would be integrated into the aircraft for small UAS that would be subject to this proposed rule. The FAA also invites comments, with supporting documentation, as to the costs and benefits of requiring a flight termination system or other technological equipment.

i. Confined Area of Operation Boundaries

The FAA notes that the proposed visual-line-of-sight requirement in § 107.31 would create a natural horizontal boundary on the area of operation. Due to the distance limitations of human vision, the operator or visual observer would be unable to maintain visual line of sight of the small unmanned aircraft sufficient to satisfy proposed § 107.31 if the aircraft travels too far away from them. Accordingly, the proposed visual-line-of-sight requirement in proposed § 107.31 would effectively confine the horizontal area of operation to a circle around the person maintaining visual

contact with the aircraft with the radius of that circle being limited to the farthest distance at which the person can see the aircraft sufficiently to maintain compliance with proposed § 107.31.

The FAA notes that there are two issues with defining the horizontal boundary of the area of operation in this manner. First, a small UAS operation could use multiple visual observers to expand the outer bounds of the horizontal circle created by the visual-line-of-sight requirement. To address this issue, the FAA proposes to require, in § 107.33(c), that if an operation uses a visual observer, the small unmanned aircraft must remain close enough to the operator at all times during flight for the operator to be capable of seeing the aircraft with vision unaided by any device other than corrective lenses. This approach would prevent the use of visual observers to expand the horizontal outer bounds of the confined area of operation. This approach would also create a safety-beneficial redundancy in that, while the operator is not required to look at the small unmanned aircraft in an operation that uses a visual observer, should something go wrong, the operator would be able to look up and see for him- or herself what is happening with the aircraft.

As an alternative method of addressing this issue, the FAA considered imposing a numerical limit on how far away a small unmanned aircraft can be from the operator. The FAA ultimately decided not to propose this approach, as it currently lacks sufficient data to designate a specific numerical limit. However, the FAA invites comments on whether the horizontal boundary of the contained area of operation should be defined through a numerical limit. If the boundary is defined through a numerical limit, what should that limit be?

The second way that the horizontal boundary of the confined operational area could be expanded is by stationing the operator on a moving vehicle or aircraft. If the operator is stationed on a moving vehicle, then the horizontal area-of-operation boundary tied to the operator's line of sight would move with the operator, thus increasing the size of the small unmanned aircraft's area of operation. To prevent this scenario, the FAA proposes, in § 107.25, consistent with the ARC recommendations,⁵⁶ to prohibit the operation of a small UAS from a moving aircraft or land-borne vehicle. However, proposed § 107.25

would make an exception for water-borne vehicles. This is because there are far less people and property located over water than on land. Consequently, a loss of positive control that occurs over water would have a significantly smaller chance of injuring a person or damaging property than a loss of positive control that occurs over land. Allowing use of a small UAS from a water-borne vehicle would also increase the societal benefits of this proposed rule without sacrificing safety by incorporating small UAS operations such as bridge inspections and wildlife nesting area evaluations into the NAS.

The FAA is considering alternatives for regulation of the operation of small UAS from moving land vehicles, while protecting safety. It invites comments, with supporting documentation, on whether small UAS operations should be permitted from moving land-based vehicles, and invites comment on a regulatory framework for such operations. The FAA specifically invites comments as to whether distinctions could be drawn between different types of land-based vehicles or operating environments such that certain operations from moving land-based vehicles could be conducted safely. The FAA also invites comments on whether deviation authority should be included in the final rule to accommodate these types of operations.

Next, we turn to the vertical boundary of the confined area of operation. With regard to the vertical boundary, the FAA proposes, in § 107.51(b), to set an altitude ceiling of 500 feet above ground level (AGL) for small UAS operations that would be subject to this proposed rule. The FAA chose to propose 500 feet as the vertical area-of-operation boundary because most manned aircraft operations take place above 500 feet. Specifically, most manned aircraft operations conducted over uncongested areas must be flown at an altitude above 500 feet AGL, while most manned aircraft operations conducted over congested areas must be flown at an even higher altitude.⁵⁷ Thus, a 500-foot altitude ceiling for small UAS operations would create a buffer between a small unmanned aircraft and most manned aircraft flying in the NAS.

The FAA notes that while most manned aircraft operations fly above the 500-foot ceiling proposed in this rule, there are some manned-aircraft operations that could fly below this altitude. For example, aerial applicators, helicopter air ambulance services, and military operations conducted on military training routes often fly at an

⁵⁶ ARC report and recommendations, Sec. 6.11

⁵⁷ See 14 CFR 91.119(b) and (c).

HB 1328
3/23/15

7-12

altitude below 500 feet. However, even though some manned aircraft operations take place at an altitude below 500 feet, there is significantly less air traffic at or below 500 feet than there is above 500 feet altitude. As a result of this difference in air-traffic density, the FAA has determined that small UAS operations would not pose a significant risk to manned aircraft operations taking place below 500 feet altitude if proper precautions are taken by the small UAS operator.

The FAA also considered whether the vertical boundary should be set at a higher level. However, because most manned-aircraft operations transit the airspace above the 500-foot level, UAS operations at that altitude would likely require greater levels of operator training, aircraft equipage, and some type of aircraft certification in order to avoid endangering other users of the NAS. Since these provisions would be contrary to the goal of this rulemaking, which is to regulate the lowest-risk small UAS operations while imposing a minimal regulatory burden on those operations, this proposed rule would not allow small UAS to travel higher than 500 feet AGL. The FAA invites comments, with supporting documentation, on whether this proposed 500-foot ceiling should be raised or lowered.

ii. Mitigating Loss-of-Positive-Control Risk

Now that we have defined the confined area of operation, we turn to the question of how loss-of-positive-control risk can be mitigated within that area of operation. The FAA notes that there is significant diversity in both the types of small UAS that are available and the types of operations that those small UAS can be used in. Accordingly, small UAS operators need significant flexibility to mitigate hazards posed by their individual small UAS operation, as a mitigation method that works well for one type of small UAS used in one type of operation may not work as well in another operation that uses another type of small UAS. For example, in a loss-of-positive-control situation, a rotorcraft that loses operator inputs or power to its control systems would tend to descend straight down or at a slight angle while a fixed wing aircraft would glide for a greater distance before landing. Since the loss-of-positive-control risk posed by different types of small unmanned aircraft in various operations is different, the FAA proposes to create a performance-based standard under which, subject to certain broadly-applicable constraints, small UAS operators would have the flexibility to

create operational and aircraft-specific loss-of-control mitigation measures.

The broadly applicable constraints that the FAA proposes to impose on a small UAS operator's risk-mitigation decisions are as follows. First, the FAA proposes to require, in § 107.49(a)(3), that prior to flight, the operator must ensure that all links between the control station and the small unmanned aircraft are working properly. The operator can do this by verifying control inputs from the control station to the servo actuators⁵⁸ in the small unmanned aircraft. If the operator finds, during this preflight check, that a control link is not functioning properly, the operator would not commence flight until the problem with the control link is resolved. This proposed constraint would significantly mitigate the risk of a loss-of-positive-control scenario by reducing the possibility that small unmanned aircraft flight commences with a malfunctioning control link.

Second, the FAA proposes to impose a speed limit of 87 knots (100 miles per hour) on small unmanned aircraft calibrated airspeed at full power in level flight. This is because, if there is a loss of positive control, an aircraft traveling at a high speed poses a higher risk to persons, property, and other aircraft than an aircraft traveling at a lower speed. A speed limit would also have safety benefits outside of a loss-of-positive-control scenario because a small unmanned aircraft traveling at a lower speed is generally easier to control than a higher-speed aircraft.

In determining the specific speed limit, the FAA decided to propose 87 knots (100 mph) as the limit. This proposed speed limit is based on the ARC recommendation of a 100 mph speed limit for small UAS operations. The ARC determined that "aircraft flying faster than 100 mph are considered a high performance aircraft" that "are perceived as having greater risks."⁵⁹ Accordingly, the FAA proposes to limit the speed of small unmanned aircraft to 87 knots (100 mph). The FAA invites comments on whether this speed limit should be raised or lowered or whether a speed limit is necessary.

Third, the FAA proposes, in § 107.39, to prohibit the operation of a small unmanned aircraft over a person who is not directly participating in the operation of that small unmanned aircraft. One of the possible

consequences of loss-of-positive-control is that the aircraft will immediately crash into the ground upon loss of control inputs from the operator. Because a loss of positive control can happen at any moment, the FAA's proposed prohibition on operating small unmanned aircraft over most persons will minimize the risk that a person is standing under a small unmanned aircraft if that aircraft terminates flight and returns to the surface. This prohibition would not apply to persons inside or underneath a covered structure that would protect the person from a falling small unmanned aircraft.

The FAA's proposed prohibition on operating over people would provide an exception for persons directly participating in the operation of the small unmanned aircraft. The FAA considered prohibiting the operation of a small unmanned aircraft over any person, but rejected this approach as unduly burdensome because the operator or visual observer may, at some points of the operation, need to stand under the small unmanned aircraft in order to maintain visual line of sight and/or comply with other provisions of this proposed rule. As an alternative to prohibiting these persons from standing under the small unmanned aircraft, the FAA proposes, in § 107.49(a)(2), that prior to flight, the operator must ensure that all persons directly involved in the small unmanned aircraft operation receive a briefing that includes operating conditions, emergency procedures, contingency procedures, roles and responsibilities, and potential hazards. A person is directly involved in the operation when his or her involvement is necessary for the safe operation of the small unmanned aircraft. By receiving a pre-flight briefing on the details of the operation and the hazards involved, the persons involved in the operation would be made aware of the small unmanned aircraft's location at all times and would be able to avoid the flight path of the small unmanned aircraft if the operator were to lose control or the aircraft were to experience a mechanical failure.

Within these constraints, the FAA proposes the following performance-based standards for mitigating loss-of-positive-control risk. First, the FAA proposes, in § 107.49(a)(1), that, prior to flight, the operator must become familiar with the confined area of operation by assessing the operating environment and assessing risks to persons and property in the immediate vicinity both on the surface and in the air. As part of this preflight assessment, the operator would need to consider conditions that could pose a hazard to

⁵⁸ A "servo actuator" is generally defined as a device used to provide a wide range of remote movement based on signals from the system on which it is used.

⁵⁹ ARC Report, p. 20, section 6.12.

HB 1328
3/23/15

7-13

the operation of the small UAS as well as conditions in which the operation of the small UAS could pose a hazard to other aircraft or persons or property on the ground. Accordingly, the FAA proposes to require that the preflight assessment include the consideration of: (1) Local weather conditions; (2) local airspace and any flight restrictions; (3) the location of persons and property on the ground; and (4) any other ground hazards.

Second, the FAA proposes that, after becoming familiar with the confined area of operation and conducting a preflight assessment, the operator be required, by § 107.19(b), to ensure that the small unmanned aircraft will pose no undue hazard to other aircraft, people, or property in the event of a loss of control of the aircraft for any reason. This proposed requirement would provide the operator with significant flexibility to choose how to mitigate the hazards associated with loss of aircraft control. For example, in addition to the examples mentioned previously, if the operation takes place in a residential area, the operator could ask everyone in the area of operation to remain inside their homes while the operation is conducted.⁶⁰ If the operation takes place in an area where other air traffic could pose a hazard, the operator would advise local air traffic control as to the location of his or her area of operation and add extra visual observers to the operation so that they can notify the operator if other aircraft are approaching the area of operation.

The above are just some examples of mitigation strategies that could be employed by the operator to ensure that the small unmanned aircraft will pose no hazard to other aircraft, people or property in the event of lost positive control. These examples are not intended to provide an exhaustive list, as there are different ways to mitigate loss of positive control. The proposed requirement in § 107.19(b) would provide the operator with the flexibility to choose which mitigation method is appropriate for his/her specific operation to ensure any hazards posed by loss of positive aircraft control are sufficiently mitigated. The FAA also anticipates creating guidance that provides additional examples of how operators can mitigate loss of positive control in small UAS operations. However, the FAA emphasizes that no matter what mitigation option(s) the

operator employs under this proposed rule, the operator must strive to always maintain positive control of the small unmanned aircraft. The operator would be in violation of proposed § 107.19(b) if he or she intentionally operates the small unmanned aircraft in a location where he or she will not have positive control over that aircraft.

5. Limitations on Operations in Certain Airspace

This proposed rule would place limitations small UAS operations in three areas related to airspace: (1) Controlled airspace (airspace other than Class G); (2) prohibited or restricted airspace; and (3) airspace where aviation activity is limited by a Notice to Airmen (NOTAM). The FAA is proposing these requirements to reduce the threat to other users of the NAS in busy airspace or where most or all aviation activities would otherwise be limited.

i. Controlled Airspace

The FAA is seeking to limit the exposure of the small unmanned aircraft to other users of the NAS to minimize the risk of collision, which can occur both during controlled flight of the UAS or if the operator loses positive control of the small unmanned aircraft. This proposed rule would prohibit small unmanned aircraft operations in Class A airspace. Class A airspace starts at 18,000 feet mean sea level and extends up to 60,000 feet (Flight Level 600). As discussed above, this rule would prohibit small UAS operations above 500 feet AGL and outside of visual line of sight. Operations in Class A airspace would be inconsistent with that requirement, and therefore this proposed rule would prohibit operations in Class A airspace.

Small UAS operations would also be prohibited in Class B, Class C, Class D, and within the lateral boundaries of the surface area of Class E airspace designated for an airport without prior authorization from the ATC facility having jurisdiction over the airspace. The FAA factors information such as traffic density, the nature of operations, and the level of safety required when determining whether to designate controlled airspace.⁶¹ Pilots must have an ATC clearance to enter certain controlled airspace. In other words, the FAA requires ATC to have knowledge of aviation operations in the airspace due to the greater amount of activity in that area compared to uncontrolled airspace.

The FAA believes that restricting use of controlled airspace to approved operations would reduce the risk of interference with other aircraft activities. Interference could occur for many reasons, including the location of the proposed small UAS operation in the airspace, or how the small unmanned aircraft would behave if there is a loss of positive control. These limitations would also be consistent with the general requirement for aircraft operating in controlled airspace to have ATC approval prior to entering the airspace. Therefore, the FAA proposes that small UAS receive approval from the ATC facility with jurisdiction over the airspace in which the operator would like to conduct operations. That ATC facility would have the best understanding of local airspace, its usage, and traffic patterns and would be in the best position to ascertain whether the proposed small UAS operation would pose a hazard to other users or the efficiency of the airspace, and procedures to implement to mitigate hazards. This proposed rule would not establish equipment requirements for small UAS operating in controlled airspace as the FAA does for other users of controlled airspace. Rather, the FAA believes that local ATC approval would provide a safer and more efficient operating environment at less cost to the operator.

The FAA notes that normal aircraft operations inside controlled airspace in the vicinity of an airport require prior authorization from ATC. Per part 91, ATC currently requires two-way radio communication for departures, through flights, arrivals, and operations inside the airspace. The FAA understands that not all small UAS will be able to comply with the provisions of part 91, and that is why this proposed rule would not require strict compliance with part 91. However, because the air-traffic provisions of part 91 are intended to ensure safe operation in the NAS, a small UAS operator that intends to operate in controlled airspace must ensure that the proposed operations are planned and conducted in the safest manner possible. The small UAS operator can do this by working closely with the ATC facility that controls the airspace.

The ATC facility has the authority to approve or deny aircraft operations based on traffic density, controller workload, communication issues, or any other type of operations that could potentially impact the safe and expeditious flow of air traffic in that airspace. The more that a small UAS is able to show that it would satisfy the provisions of part 91 and comply with

⁶⁰ The FAA notes that this proposed requirement would not require people not involved with the operation to comply with the operator's warnings. The operator would simply be unable to commence the operation until the pertinent area has been made safe for operation.

⁶¹ See FAA Aeronautical Information Manual, Para. 3-1-1.

HB1328
3/23/15

7-14

the local operating procedures, the easier the access to the airspace would be. These items should be outlined in a prior agreement with the ATC facility to identify shortfalls and establish operating procedures for small UAS to integrate into the existing air traffic operation. This agreement would ensure all parties involved are aware of limitations and special interest items and would enable the safe flow of aircraft operations in that airspace. The FAA seeks comments related to part 91 compliance issues small UAS operators may encounter.

ii. Prohibited or Restricted Areas

The proposed rule would prohibit small UAS operations in prohibited and restricted areas without permission from the using or controlling agency as applicable. Prohibited and restricted areas are designated in 14 CFR part 73. Prohibited areas are established when necessary to prohibit flight over an area on the surface in the interest of national security or welfare. No person may operate an aircraft without permission of the using agency in a prohibited area.⁶² Restricted areas are areas established when determined necessary to confine or segregate activities considered hazardous to non-participating aircraft. Although aircraft flight is not wholly prohibited in these areas, it is subject to restriction.⁶³ The proposed provision concerning prohibited and restricted areas would be similar to the part 91 restriction on operations in these areas.⁶⁴

iii. Areas Designated by Notice to Airmen

This proposed rule would also prohibit operation of small UAS in airspace restricted by NOTAMs unless authorized by ATC or a certificate of waiver or authorization. This would include NOTAMs issued to designate a temporary flight restriction (TFR). NOTAMs contain time-critical aeronautical information that is either temporary in nature, or not sufficiently known in advance to permit publication on aeronautical charts or other publications.⁶⁵ For example, NOTAMs may be used to limit or restrict aircraft operations during emergency situations or presidential or VIP movements. They may also be used to limit aircraft operations in the vicinity of aerial demonstrations or sporting events.

NOTAMs are available to the public on the FAA's Web site.⁶⁶

Like other users of the airspace, small UAS operators would be required to review and comply with NOTAMs. As with other airspace restrictions in this rule, an operator could seek authorization from ATC or through a certificate of waiver or authorization to conduct operations in otherwise restricted airspace. The FAA believes that this process would permit an assessment of the operation in relation to the airspace restriction to determine whether the operation can be safely conducted.

6. Airworthiness, Inspection, Maintenance, and Airworthiness Directives

i. Inspections and Maintenance

As discussed in section III.J.3 of this preamble, pursuant to section 333(b)(2) of Public Law 112–95, we have determined that a small UAS should not be required to obtain airworthiness certification if satisfying the provisions of this proposal. However, without an airworthiness certification process, the FAA still needs to ensure that a small UAS is in a condition for safe operation. In considering how to address this issue, the FAA notes that the current regulations applicable to manned civil aircraft generally require an annual aircraft inspection every 12 months.⁶⁷ The inspection and any maintenance that might be necessary as a result of the inspection currently are governed by the provisions of 14 CFR part 43. Part 43 requires that the inspection examine every component of the aircraft in detail to determine whether any hazardous characteristics are present that would render the aircraft unairworthy.⁶⁸ If the inspection reveals any hazardous characteristics that would render the aircraft unairworthy, then maintenance, conducted pursuant to the regulations of part 43, must be performed in order to return the aircraft to an airworthy condition.

In addressing the issue of airworthiness for small UAS, the FAA

considered several approaches, including requiring small UAS operators to comply with the existing inspection and maintenance requirements of this chapter. The FAA also considered requiring a separate permit to operate (PTO) in addition to aircraft registration and airman certification. A PTO would have included airworthiness certification requirements that would have required an applicant to:

- Describe the entire small UAS, including airframe, control station, and communications link;
- Comply with a set of unvalidated consensus standards;
- Test the design features required by the unvalidated consensus standards and determine that the UAS satisfies those standards;
- Inspect the aircraft for compliance with the manufacturer's requirements;
- Determine whether the aircraft has been manufactured in compliance with unvalidated production acceptance and quality assurance consensus standards acceptable to the FAA;
- Complete ground and flight testing of required UAS components and determine whether they demonstrated acceptable performance and safe operation.
- Create a process for addressing unsafe conditions in the aircraft; and
- Create a monitoring program to identify and correct safety-of-flight issues.

After further consideration, the FAA decided that neither of these approaches is proportionate to the risk posed by small UAS. FAA noted that, as mentioned previously, due to their light weight, small unmanned aircraft generally pose a significantly lower risk to people and property on the ground than manned aircraft. This relatively low risk is mitigated even further by the see-and-avoid and loss-of-positive-control provisions of this proposed rule, which are discussed above.

Accordingly, based on existing information, the FAA believes that requiring small UAS operators to conduct inspection and maintenance of the small UAS pursuant to the existing regulations of part 43, or to obtain a PTO, would not result in significant safety benefits. As a result, this proposed rule would not require small UAS compliance with part 43 or the application for, or issuance of, a PTO.

Instead, this proposed rule would require, in § 107.21(b), that prior to each flight, the operator must inspect the small UAS to ensure that it is in a condition for safe operation. The operator could do this by, for example, performing a manufacturer-

⁶² See 14 CFR 1.1.

⁶³ See *id.*

⁶⁴ See 14 CFR 91.133.

⁶⁵ See FAA Aeronautical Information Manual, para. 5–1–3.

⁶⁶ See, e.g., <https://www.notams.faa.gov/dinsQueryWeb/> and http://www.faa.gov/pilots/ft_plan/notams/.

⁶⁷ See 14 CFR 91.609. Different components of the aircraft are also currently subject to additional component-specific inspection schedules. For example, in addition to the above general inspection requirements, altimeter instruments on airplanes and helicopters operating in controlled airspace under instrument flight rules must be inspected every 24 months. See 14 CFR 91.411(a)(1).

⁶⁸ See 14 CFR part 43, Appendix D (listing aircraft components that must be inspected and the hazardous characteristics that the inspection should look for).

HB1328
3/23/15

PROPOSED AMENDMENTS TO HB 1328
(Sen. Hogue)

1-1
3/31/15

SECTION 7. Section 29-01-20 of the North Dakota Century Code is amended and reenacted as follows:

29-01-20. Stolen property held by peace officer.

Except for consumer goods as defined in section 44-09-02(1)(y), when property alleged to have been stolen or embezzled comes into the custody of a peace officer, the peace officer shall hold it subject to the order of the magistrate authorized by section 29-01-21 to direct the disposal thereof.

Not added to the bill.

15.0259.03001
Title.

Prepared by the Legislative Council staff for
Representative K. Koppelman
March 10, 2015

21
3/31/15

PROPOSED AMENDMENTS TO ENGROSSED HOUSE BILL NO. 1328

Page 2, line 2, after "warrant" insert "unless the information was obtained under the circumstances described in subdivision a or b of subsection 1 or was obtained through the monitoring of public lands or international borders."

Page 3, line 27, after "the" insert "lawful"

Page 3, line 27, after "rights" insert ", unless the surveillance is otherwise allowed under this chapter"

Page 3, line 27, remove "A state agency may not authorize"

Page 3, remove lines 28 through 30

Renumber accordingly