January 28, 2014

HOUSE BILL No. 1009

DIGEST OF HB 1009 (Updated January 27, 2014 12:44 pm - DI 69)

Citations Affected: IC 34-30; IC 35-31.5; IC 35-33; IC 35-38; IC 35-46; noncode.

Synopsis: Search warrants and privacy. Prohibits the use of unmanned aerial vehicles and tracking devices to conduct warrantless searches, with certain exceptions. Prohibits the placement of cameras or electronic surveillance equipment on private property to conduct warrantless searches, with certain exceptions. Establishes additional requirements that must be met in order for a search warrant authorizing the use of a tracking device to be issued. Provides that, except for a law enforcement officer acting under a warrant and certain other persons under certain circumstances, a person who uses a tracking device without the consent of the person who is the object of the use commits a Class A misdemeanor. Provides that a person who knowingly or intentionally places a camera or electronic surveillance equipment that records images or data of any kind while unattended on the private property of another person without the written consent of the owner or tenant of the private property commits a Class A misdemeanor. Requires a search warrant to conduct a search of an electronic device or compel disclosure of an electronic communication service or electronic user data. Requires a search warrant to obtain geolocation information. Provides immunity from civil and criminal liability for certain entities that provide information pursuant to certain warrants. Provides an exception to certain search warrant and notice requirements before electronic mail owned, controlled, or used by the state and obtained by the office of inspector general or an investigator

(Continued next page)

Effective: July 1, 2014.

Koch, Pierce

January 7, 2014, read first time and referred to Committee on Courts and Criminal Code.
January 28, 2014, amended, reported — Do Pass.

for the inspector general is used in an administrative proceeding. Provides certain procedures for the issuance of search warrants concerning electronic communication service or remote computing service that affect the law concerning a journalist's privilege against disclosure of an information source. Urges the legislative council to assign to a study committee during the 2014 legislative interim the topic of digital privacy, including issues related to: (1) searches of electronic devices; (2) compelling the disclosure of electronic user data; (3) the collection and use of geolocation information; and (4) the collection and use of biometric information; by government agencies.

January 28, 2014

Second Regular Session 118th General Assembly (2014)

PRINTING CODE. Amendments: Whenever an existing statute (or a section of the Indiana Constitution) is being amended, the text of the existing provision will appear in this style type, additions will appear in **this style type**, and deletions will appear in ~~this style type.~~

Additions: Whenever a new statutory provision is being enacted (or a new constitutional provision adopted), the text of the new provision will appear in **this style type**. Also, the word **NEW** will appear in that style type in the introductory clause of each SECTION that adds a new provision to the Indiana Code or the Indiana Constitution.

Conflict reconciliation: Text in a statute in *this style type* or ~~*this style type*~~ reconciles conflicts between statutes enacted by the 2013 Regular Session and 2013 First Regular Technical Session of the General Assembly.

HOUSE BILL No. 1009

A BILL FOR AN ACT to amend the Indiana Code concerning criminal law and procedure.

Be it enacted by the General Assembly of the State of Indiana:

SECTION 1. IC 34-30-2-146.4 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 146.4. IC 35-33-5-15 (Concerning electronic communications services, remote computing services, and geolocation information services for compliance with warrant laws).**

SECTION 2. IC 35-31.5-2-9.5 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 9.5. "Adverse result", for purposes of IC 35-33-5, has the meaning set forth in IC 35-33-5-0.5(1).**

SECTION 3. IC 35-31.5-2-27.7 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 27.7. "Biometric information system", for purposes of IC 35-33-5, has the meaning set forth in IC 35-33-5-0.5(2).**

SECTION 4. IC 35-31.5-2-68.5 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 68.5. "Covered service", for purposes of IC 35-33-5, has the meaning set forth in IC 35-33-5-0.5(3).**

SECTION 5. IC 35-31.5-2-110.5 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 110.5. "Electronic communication service", for purposes of IC 35-33-5 and IC 35-46-10, means a service that provides users with the ability to send or receive wire or electronic communications.**

SECTION 6. IC 35-31.5-2-111.5 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 111.5. "Electronic storage", for purposes of IC 35-33-5, has the meaning set forth in IC 35-33-5-0.5(5).**

SECTION 7. IC 35-31.5-2-112.5 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 112.5. "Electronic user data", for purposes of IC 35-33-5, has the meaning set forth in IC 35-33-5-0.5(6).**

SECTION 8. IC 35-31.5-2-143.3 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 143.3. "Geolocation information" means data generated by an electronic device that can be used to determine the location of the device or the owner of the device. The term includes a cellular telephone, a wireless fidelity (wi-fi) equipped computer, or a GPS navigation or tracking unit. The term does not include the content of a communication.**

SECTION 9. IC 35-31.5-2-143.5 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 143.5. "Geolocation information service" means a person that offers or provides GPS service or other mapping, locational, or directional services to the public by means of an electronic device, including a cellular telephone, a wireless fidelity (wi-fi) equipped computer, or a GPS navigation or tracking unit.**

SECTION 10. IC 35-31.5-2-144, AS ADDED BY P.L.114-2012, SECTION 67, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: Sec. 144. **(a)** "Governmental entity" means:

(1) the United States or any state, county, township, city, town, separate municipal corporation, special taxing district, or public

school corporation;

(2) any authority, board, bureau, commission, committee, department, division, hospital, military body, or other instrumentality of any of those entities; or

(3) a state assisted college or state assisted university.

(b) For purposes of IC 35-33-5, "governmental entity" also includes a person authorized to act on behalf of a state or local agency

SECTION 11. IC 35-31.5-2-175.5 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 175.5. "Intercept", for purposes of IC 35-33-5, has the meaning set forth in IC 35-33-5-0.5(8).**

SECTION 12. IC 35-31.5-2-186, AS ADDED BY P.L.114-2012, SECTION 67, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: Sec. 186. (a) "Lawful detention" means:

(1) arrest;

(2) custody following surrender in lieu of arrest;

(3) detention in a penal facility;

(4) detention in a facility for custody of persons alleged or found to be delinquent children;

(5) detention under a law authorizing civil commitment in lieu of criminal proceedings or authorizing such detention while criminal proceedings are held in abeyance;

(6) detention for extradition or deportation;

(7) placement in a community corrections program's residential facility;

(8) electronic monitoring;

(9) custody for purposes incident to any of the above including transportation, medical diagnosis or treatment, court appearances, work, or recreation; or

(10) any other detention for law enforcement purposes.

(b) Except as provided in subsection (a)(7) and (a)(8), the term does not include supervision of a person on probation or parole or constraint incidental to release with or without bail.

(c) The term does not include electronic monitoring through the use of:

(1) an unmanned aerial vehicle under IC 35-33-5-9; or

(2) an electronic tracking device under IC 35-33-5-11.

SECTION 13. IC 35-31.5-2-273.8 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 273.8. "Remote computing service", for purposes of IC 35-33-5, has the meaning set forth in**

IC 35-33-5-0.5(9).

SECTION 14. IC 35-31.5-2-337.5 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 337.5. "Tracking device", for purposes of IC 35-33-5, IC 35-46-10, and this chapter, means an electronic or mechanical device that allows a person to remotely determine or track the position or movement of another person or an object. The term includes the following:**

(1) A device that stores geographic data for subsequent access or analysis.

(2) A device that allows real-time monitoring or movement.

(3) An unmanned aerial vehicle.

(4) A cellular telephone or other wireless or cellular communications device.

SECTION 15. IC 35-31.5-2-342.3 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 342.3. "Unmanned aerial vehicle", for purposes of IC 35-33-5, has the meaning set forth in IC 35-33-5-0.5(10).**

SECTION 16. IC 35-31.5-2-343.5 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 343.5. "Use of a tracking device", for purposes of IC 35-33-5 and IC 35-46-10, includes the installation, maintenance, and monitoring of a tracking device. The term does not include:**

(1) the capture, collection, monitoring, or viewing of images; or

(2) the use of a court ordered monitoring device on a person who has been charged with or convicted of a crime.

SECTION 17. IC 35-31.5-2-343.7 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 343.7. "Use of an unmanned aerial vehicle", for purposes of IC 35-33-5, has the meaning set forth in IC 35-33-5-0.5(11).**

SECTION 18. IC 35-31.5-2-343.8 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 343.8. "User", for purposes of IC 35-33-5, has the meaning set forth in IC 35-33-5-0.5(12).**

SECTION 19. IC 35-31.5-2-355.5 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 355.5. "Wireless communication device", for purposes of IC 35-33-5, has the meaning in**

IC 35-33-5-0.5(13).

SECTION 20. IC 35-33-5-0.5 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 0.5. The following definitions apply throughout this chapter:**

(1) "Adverse result" means:

(A) immediate dangers of death or serious bodily injury;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of a potential witness; or

(E) substantial jeopardy of a law enforcement investigation.

(2) "Biometric information system" means any tool, program, service, or system used to uniquely identify, verify identity of, and track individuals using retina and iris scans, fingerprints, voiceprints, or hand and face geometry, gait patterns, or other automated systems that can uniquely and independently identify an individual.

(3) "Covered service" means an electronic communication service, a geolocation information service, or a remote computing service.

(4) "Electronic communication service" means a service that provides users with the ability to send or receive wire or electronic communications.

(5) "Electronic storage" means any storage of electronic user data on a computer, computer network, or computer system regardless of whether the data is subject to recall, further manipulation, deletion, or transmission. "Electronic storage" includes any storage or electronic communication by an electronic communication service or a remote computing service.

(6) "Electronic user data" means any data or records that are in the possession, care, custody, or control of a provider of an electronic communication service, a remote computing service, or any other service or program that stores, uses, collects, or safeguards electronic user data.

(7) "Governmental entity" has the meaning set forth in IC 35-31.5-2-144. For purposes of this chapter, "governmental entity" also includes a person authorized to act on behalf of a state or local agency.

(8) "Intercept" means to acquire geolocation data through the use of an electronic device, mechanical device, or other device.

(9) "Remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communication service.

(10) "Unmanned aerial vehicle" means an aircraft that:

(A) does not carry a human operator; and

(B) is capable of flight under remote control or autonomous programming.

(11) "Use of an unmanned aerial vehicle" means the use of an unmanned aerial vehicle by a law enforcement officer to obtain evidence relevant to the enforcement of statutes, rules, or regulations. The term includes:

(A) the interception of wire, electronic, or oral communications; and

(B) the capture, collection, monitoring, or viewing of images.

(12) "User" means any person who:

(A) uses an electronic communication service, remote computing service, geolocation information service, or an electronic device; and

(B) may or may not be the person or entity having legal title, claim, or right to the electronic device or electronic user data.

(13) "Wireless communication device" means a device that enables access to, or use of, an electronic communication service or a covered service, if the device uses a radio or other wireless connection to access the system or service.

SECTION 21. IC 35-33-5-2, AS AMENDED BY P.L.2-2005, SECTION 117, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: Sec. 2. (a) Except as provided in section 8 of this chapter, **and subject to the requirements of sections 11 and 13 of this chapter, if applicable,** no warrant for search or arrest shall be issued until there is filed with the judge an affidavit:

(1) particularly describing:

(A) the house or place to be searched and the things to be searched for; or

(B) particularly describing the person to be arrested;

(2) alleging substantially the offense in relation thereto and that the affiant believes and has good cause to believe that:

(A) the things as are to be searched for are there concealed; or

(B) the person to be arrested committed the offense; and

(3) setting forth the facts then in knowledge of the affiant or information based on hearsay, constituting the probable cause.

(b) When based on hearsay, the affidavit must either:

(1) contain reliable information establishing the credibility of the source and of each of the declarants of the hearsay and establishing that there is a factual basis for the information furnished; or

(2) contain information that establishes that the totality of the circumstances corroborates the hearsay.

(c) An affidavit for search substantially in the following form shall be treated as sufficient:

STATE OF INDIANA)
) SS:
COUNTY OF _____)

A B swears (or affirms, as the case may be) that he believes and has good cause to believe (here set forth the facts and information constituting the probable cause) that (here describe the things to be searched for and the offense in relation thereto) are concealed in or about the (here describe the house or place) of C D, situated in the county of _____, in said state.

Subscribed and sworn to before me this _____ day of _____ 20__.

SECTION 22. IC 35-33-5-8 IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: Sec. 8. (a) A judge may issue a search or arrest warrant without the affidavit required under section 2 of this chapter, if the judge receives sworn testimony of the same facts required for an affidavit:

(1) in a nonadversarial, recorded hearing before the judge;

(2) orally by telephone or radio; or

(3) in writing by facsimile transmission (FAX).

(b) After reciting the facts required for an affidavit and verifying the facts recited under penalty of perjury, an applicant for a warrant under subsection (a)(2) shall read to the judge from a warrant form on which the applicant enters the information read by the applicant to the judge. The judge may direct the applicant to modify the warrant. If the judge agrees to issue the warrant, the judge shall direct the applicant to sign the judge's name to the warrant, adding the time of the issuance of the warrant.

(c) After transmitting an affidavit, an applicant for a warrant under subsection (a)(3) shall transmit to the judge a copy of a warrant form completed by the applicant. The judge may modify the transmitted warrant. If the judge agrees to issue the warrant, the judge shall transmit to the applicant a duplicate of the warrant. The judge shall

then sign the warrant retained by the judge, adding the time of the issuance of the warrant.

(d) If a warrant is issued under subsection (a)(2), the judge shall record the conversation on audio tape and order the court reporter to type or transcribe the recording for entry in the record. The judge shall certify the audio tape, the transcription, and the warrant retained by the judge for entry in the record.

(e) If a warrant is issued under subsection (a)(3), the judge shall order the court reporter to ~~the~~ retype or copy the facsimile transmission for entry in the record. The judge shall certify the transcription or copy and warrant retained by the judge for entry in the record.

(f) The court reporter shall notify the applicant who received a warrant under subsection (a)(2) or (a)(3) when the transcription or copy required under this section is entered in the record. The applicant shall sign the typed, transcribed, or copied entry upon receiving notice from the court reporter.

(g) This section does not apply to a warrant issued under the following:

(1) Section 9 of this chapter (concerning the use of an unmanned aerial vehicle).

(2) Section 11 of this chapter (concerning the use of a tracking device).

SECTION 23. IC 35-33-5-9 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 9. (a) Except as provided in subsection (b), a law enforcement officer must obtain a search warrant in order to use an unmanned aerial vehicle.**

(b) A law enforcement officer may use an unmanned aerial vehicle without obtaining a search warrant if the law enforcement officer determines that the use of the unmanned aerial vehicle is required due to:

(1) the existence of exigent circumstances necessitating a warrantless search; or

(2) the substantial likelihood of a terrorist attack.

SECTION 24. IC 35-33-5-10 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 10. The following are not admissible as evidence in an administrative or judicial proceeding:**

(1) A communication or an image that is obtained through the use of an unmanned aerial vehicle in violation of section 9 of this chapter.

(2) Evidence derived from a communication or an image

described in subdivision (1).

SECTION 25. IC 35-33-5-11 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 11. (a) Except as provided in subsection (e), a law enforcement officer must obtain a search warrant in order to use a tracking device to obtain evidence relevant to the enforcement of statutes, rules, and regulations.**

(b) An application for a search warrant required under subsection (a) must include an affidavit that contains the following information:

(1) The identity and, if known, the location of the object on which the tracking device will be installed.

(2) The identity of the owner of the object described in subdivision (1), if known.

(3) Material facts that show the existence of probable cause to believe that the information obtained through the use of the tracking device will be evidence relevant to the enforcement of one (1) or more specific statutes, rules, or regulations.

(4) Any additional information required under this chapter.

(c) A judicial officer may issue a warrant for the use of a tracking device if the judicial officer determines that the application for the warrant satisfies the requirements of subsection (b). The warrant must authorize the collection of tracking data contained in or obtained from the tracking device. The warrant may not authorize the interception of wire, electronic, or oral communications, or the capture, collection, monitoring, or viewing of images.

(d) A warrant issued under subsection (c) is valid for the period stated in the warrant, which may not exceed thirty (30) days from the date on which the law enforcement officer begins to obtain evidence through use of the tracking device.

(e) A law enforcement officer may use a tracking device without a warrant to obtain evidence relevant to the enforcement of statutes, rules, and regulations if the law enforcement officer determines that the use of the tracking device is required due to:

(1) the existence of exigent circumstances necessitating a warrantless search; or

(2) the substantial likelihood of a terrorist attack.

SECTION 26. IC 35-33-5-12 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 12. (a) Except as provided in subsection (b), a law enforcement officer must obtain a search**

warrant in order to place a camera or electronic surveillance equipment that records images or data of any kind while unattended on the private property of another person if the law enforcement officer does not have the consent of the other person to place the camera or electronic surveillance equipment on the other person's private property.

(b) A law enforcement officer may place a camera or electronic surveillance equipment that records images or data of any kind while unattended on the private property of another person if the law enforcement officer determines that the use of the camera or electronic surveillance equipment is required due to:

(1) the existence of exigent circumstances necessitating a warrantless search; or

(2) the substantial likelihood of a terrorist attack.

SECTION 27. IC 35-33-5-13 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 13. (a) Except as provided in subsection (b), a law enforcement officer or governmental entity may not conduct a search of an electronic device or compel disclosure of an electronic communication service or electronic user data that includes the content of a user's communications without a valid search warrant by a judge using search warrant procedures.**

(b) Information contained or stored in an electronic device is not subject to a search by a governmental entity incident to a lawful custodial arrest without a valid search warrant issued by a judge using search warrant procedures.

(c) A governmental entity may not compel a user to provide a passkey, password, or keycode to any electronic communication service, electronic device, or electronic storage, or any form of stored electronic user data, without a valid search warrant issued by a judge using search warrant procedures.

(d) A governmental entity may not obtain geolocation information without a valid search warrant issued by a judge using search warrant procedures. However, a law enforcement officer may use a tracking device without a warrant if the law enforcement officer determines that the use of the tracking device is required due to:

(1) the existence of exigent circumstances necessitating a warrantless search; or

(2) the substantial likelihood of a terrorist attack.

(e) A governmental entity may not track, monitor, or observe an

individual's electronic communications, electronic habits or routines, or an individual's habits or routines in public using a biometric information system without a valid search warrant issued by a judge using search warrant procedures.

(f) A judge may issue a search warrant under this section for electronic user data held in electronic storage, including the records and information related to a wire communication or electronic communication held in electronic storage, by a provider of an electronic communication service or a provider of a remote computing service regardless of whether the user data is held at a location in Indiana or at a location in another state.

(g) A judge may issue a search warrant under this section on a service provider that is a corporation or entity that is incorporated or organized under the laws of Indiana or a company or business entity doing business in Indiana under a contract or terms of a service agreement with an Indiana resident. The service provider shall produce all information sought, as required by the warrant.

(h) Any Indiana corporation that provides electronic communication services or remote computing services to the public shall comply with a valid warrant issued in another state that is seeking the information described in this section, if the warrant is served on the corporation.

(i) A judge may issue a warrant under this section for geolocation information of an electronic device for a period necessary to achieve the objective of the warrant, up to ten (10) days. A judge may grant an extension of a warrant under this section if the judge finds continuing probable cause and a finding that the extension is necessary to achieve the objective of the warrant, up to thirty (30) days.

SECTION 28. IC 35-33-5-14 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 14. (a) Except as provided in subsection (d), any electronic user data or geolocation information obtained in violation of section 13 of this chapter is not admissible as evidence in a civil, criminal, or administrative proceeding.**

(b) Except as provided in subsection (c) or (d), electronic user data or geolocation information obtained under section 13 of this chapter are admissible in a criminal, civil, or administrative action if each party before the trial, hearing, or procedure was furnished with the application for the search warrant and the subsequent court orders.

(c) If a party will not be prejudiced by not having the search

warrant and subsequent court orders prior to the trial, hearing, or proceeding, and the warrant and orders are not available, a court may order that the requirement of subsection (b) be waived.

(d) Electronic mail owned, controlled, or used by the state and obtained by the office of inspector general or an investigator for the inspector general is admissible in an administrative proceeding even if the electronic mail is obtained or admitted in violation of:

(1) subsection (b); or

(2) section 13 of this chapter.

SECTION 29. IC 35-33-5-15 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 15. An electronic communication service, remote computing service, and geolocation information service are immune from civil or criminal liability for providing information or evidence as required by a search warrant under this chapter.**

SECTION 30. IC 35-33-5-16 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 16. (a) For purposes of IC 34-46-4 (Journalist's Privilege Against Disclosure of Information Source) and subject to subsection (b), if:**

(1) a governmental entity requests that a court issue a search warrant to a provider of:

(A) electronic communication service; or

(B) remote computing service; and

(2) the search warrant seeks information or communications concerning a news media entity or a person otherwise described in IC 34-46-4-1;

the news media entity or person described in IC 34-46-4-1 shall be given reasonable and timely notice of the search warrant request and shall be given an opportunity to be heard by the court concerning the issuance of the search warrant before the search warrant is issued.

(b) If:

(1) the search warrant that would be issued to a provider described in subsection (a)(1) concerns a criminal investigation in which the news media entity or person described in IC 34-46-4-1 is a target of the criminal investigation; and

(2) the notice that would be provided to the news media entity or person described in IC 34-46-4-1 under subsection (a) would pose a clear and substantial threat to the integrity of

the criminal investigation;

the governmental entity shall certify the threat to the court and notice of the search warrant shall be given to the news media entity or person described in IC 34-46-4-1 as soon as the court determines that the notice no longer poses a clear and substantial threat to the integrity of the criminal investigation.

SECTION 31. IC 35-38-2.5-3, AS AMENDED BY P.L.31-2005, SECTION 2, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: Sec. 3. (a) As used in this chapter, "monitoring device" means an electronic device that:

(1) can record or transmit information twenty-four (24) hours each day regarding an offender's:

(A) presence or absence from the offender's home; or

(B) precise location;

(2) is minimally intrusive upon the privacy of the offender or other persons residing in the offender's home;

(3) with the written consent of the offender and with the written consent of other persons residing in the home at the time an order for home detention is entered, may record or transmit:

(A) a visual image;

(B) an electronic communication or any sound; or

(C) information regarding the offender's activities while inside the offender's home; and

(4) can notify a probation department, a community corrections program, or a contract agency if the offender violates the terms of a home detention order.

(b) The term includes any device that can reliably determine the location of an offender and track the locations where the offender has been, including a device that uses a global positioning system satellite service.

(c) The term does not include the following:

(1) An electronic tracking device (as defined in IC 35-31.5-2-337.5).

(2) An unmanned aerial vehicle (as defined in IC 35-31.5-2-342.3).

SECTION 32. IC 35-46-8.5 IS ADDED TO THE INDIANA CODE AS A **NEW** CHAPTER TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]:

Chapter 8.5. Unlawful Photography and Surveillance on Private Property

Sec. 1. (a) This section does not apply to a law enforcement officer who has obtained a search warrant or the consent of the

owner of private property as provided under IC 35-33-5-12 to place a camera or electronic surveillance equipment on private property.

(b) A person who knowingly or intentionally places a camera or electronic surveillance equipment that records images or data of any kind while unattended on the private property of another person without the written consent of the owner or tenant of the private property commits a Class A misdemeanor.

SECTION 33. IC 35-46-10 IS ADDED TO THE INDIANA CODE AS A **NEW** CHAPTER TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]:

Chapter 10. Unlawful Use of a Tracking Device

Sec. 1. (a) This chapter does not apply to the following:

(1) Geolocation information obtained by means of a search warrant.

(2) Geolocation information obtained or disclosed in the normal course of business by an officer, employee, or agent of an electronic communication service or a geolocation information service while engaged in an activity that is a necessary incident for the provision of service or the protection of the rights or property of the service provider.

(3) Geolocation information obtained by an officer, employee, or agent of the United States while lawfully conducting electronic surveillance under the Federal Foreign Intelligence Surveillance Act.

(4) Geolocation information relating to another person that is intercepted or disclosed with the consent of the other person.

(5) Geolocation information relating to a child if the information is intercepted or disclosed by or with the consent of the child's parent, guardian, or custodian.

(6) Geolocation information relating to another person that is available through a system that is configured to make the information readily available to the general public.

(7) Geolocation information relating to another person that is intercepted or disclosed by a law enforcement officer or emergency services provider if the information is used:

(A) to respond to a request for assistance by the person; or

(B) to assist the person under circumstances in which it is reasonable to believe that the life or safety of the person is threatened.

(8) Geolocation information relating to another person if the person intercepting or disclosing the information has a

reasonable belief that the other person has unlawfully taken the device transmitting the geolocation information.

(9) The parent or legal guardian of a minor when tracking the minor, or an authorized caretaker of the minor when the minor is under the sole care of the authorized caretaker.

(10) A legally authorized representative of an incapacitated adult.

(11) The owner of fleet vehicles, including a governmental entity, if the tracking device is used for the sole purpose of tracking the vehicles.

(12) A communications service provider (as defined in IC 8-1-32.5-4), if the communications service provider discloses the use of the tracking device in plain language to the customer.

(13) The owner of property, including a governmental entity, if the tracking device is used for the sole purpose of tracking the property.

(14) A law enforcement officer, if the law enforcement officer determines that the use of the tracking device is required due to:

(A) the existence of exigent circumstances necessitating a warrantless search; or

(B) the substantial likelihood of a terrorist attack.

(b) A person who intentionally uses, or causes to be used, a tracking device without the consent of the person who is the object of the use commits a Class A misdemeanor.

SECTION 34. [EFFECTIVE JULY 1, 2014] **(a) The general assembly urges the legislative council to assign to a study committee during the 2014 legislative interim the topic of digital privacy, including issues related to:**

(1) searches of electronic devices;

(2) compelling the disclosure of electronic user data;

(3) the collection and use of geolocation information; and

(4) the collection and use of biometric information;

by government agencies.

(b) If a study committee is assigned the topic described in subsection (a), the study committee shall issue to the legislative council a final report containing the study committee's findings and recommendations, including any recommended legislation concerning the topic, in an electronic format under IC 5-14-6 not later than November 1, 2014.

(c) This SECTION expires January 1, 2015.

COMMITTEE REPORT

Mr. Speaker: Your Committee on Courts and Criminal Code, to which was referred House Bill 1009, has had the same under consideration and begs leave to report the same back to the House with the recommendation that said bill be amended as follows:

Page 1, delete lines 1 through 8.

Page 1, line 11, delete "35-33-5-18" and insert "**35-33-5-15**".

Page 9, line 12, delete "A" and insert "**Except as provided in subsection (e), a**".

Page 9, between lines 39 and 40, begin a new paragraph and insert:

"(e) A law enforcement officer may use a tracking device without a warrant to obtain evidence relevant to the enforcement of statutes, rules, and regulations if the law enforcement officer determines that the use of the tracking device is required due to:

(1) the existence of exigent circumstances necessitating a warrantless search; or

(2) the substantial likelihood of a terrorist attack.".

Page 10, line 4, delete "person." and insert "**person if the law enforcement officer does not have the consent of the other person to place the camera or electronic surveillance equipment on the other person's private property.**".

Page 10, line 33, after "procedures." insert "**However, a law enforcement officer may use a tracking device without a warrant if the law enforcement officer determines that the use of the tracking device is required due to:**

(1) the existence of exigent circumstances necessitating a warrantless search; or

(2) the substantial likelihood of a terrorist attack.".

Page 11, delete lines 22 though 42.

Delete page 12.

Page 13, delete lines 1 through 25.

Page 13, line 26, delete "35-33-5-17" and insert "35-33-5-14".

Page 13, line 28, delete "17." and insert "**14.**".

Page 13, line 28, delete "Any" and insert "**Except as provided in subsection (d), any**".

Page 13, line 32, delete "(c)," and insert "**(c) or (d),**".

Page 13, line 33, delete "sections 13 and 14" and insert "**section 13**".

Page 13, between lines 41 and 42, begin a new paragraph and insert:

"**(d) Electronic mail owned, controlled, or used by the state and obtained by the office of inspector general or an investigator for the inspector general is admissible in an administrative proceeding**

even if the electronic mail is obtained or admitted in violation of:

(1) subsection (b); or

(2) section 13 of this chapter.".

Page 13, line 42, delete "35-33-5-18" and insert "35-33-5-15".

Page 14, line 2, delete "18." and insert "**15.**".

Page 14, delete lines 7 through 16, begin a new paragraph and insert:

"SECTION 30. IC 35-33-5-16 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2014]: **Sec. 16. (a) For purposes of IC 34-46-4 (Journalist's Privilege Against Disclosure of Information Source) and subject to subsection (b), if:**

(1) a governmental entity requests that a court issue a search warrant to a provider of:

(A) electronic communication service; or

(B) remote computing service; and

(2) the search warrant seeks information or communications concerning a news media entity or a person otherwise described in IC 34-46-4-1;

the news media entity or person described in IC 34-46-4-1 shall be given reasonable and timely notice of the search warrant request and shall be given an opportunity to be heard by the court concerning the issuance of the search warrant before the search warrant is issued.

(b) If:

(1) the search warrant that would be issued to a provider described in subsection (a)(1) concerns a criminal investigation in which the news media entity or person described in IC 34-46-4-1 is a target of the criminal investigation; and

(2) the notice that would be provided to the news media entity or person described in IC 34-46-4-1 under subsection (a) would pose a clear and substantial threat to the integrity of the criminal investigation;

the governmental entity shall certify the threat to the court and notice of the search warrant shall be given to the news media entity or person described in IC 34-46-4-1 as soon as the court determines that the notice no longer poses a clear and substantial threat to the integrity of the criminal investigation.".

Page 15, line 10, after "warrant" insert "**or the consent of the owner of private property as provided**".

Page 16, line 17, after "vehicles," insert "**including a governmental**

entity,".

Page 16, line 23, after "property," insert "**including a governmental entity,**".

Page 16, between lines 24 and 25, begin a new line block indented and insert:

"**(14) A law enforcement officer, if the law enforcement officer determines that the use of the tracking device is required due to:**

(A) the existence of exigent circumstances necessitating a warrantless search; or

(B) the substantial likelihood of a terrorist attack.".

Page 16, after line 27, begin a new paragraph and insert:

"SECTION 34. [EFFECTIVE JULY 1, 2014] **(a) The general assembly urges the legislative council to assign to a study committee during the 2014 legislative interim the topic of digital privacy, including issues related to:**

(1) searches of electronic devices;

(2) compelling the disclosure of electronic user data;

(3) the collection and use of geolocation information; and

(4) the collection and use of biometric information;

by government agencies.

(b) If a study committee is assigned the topic described in subsection (a), the study committee shall issue to the legislative council a final report containing the study committee's findings and recommendations, including any recommended legislation concerning the topic, in an electronic format under IC 5-14-6 not later than November 1, 2014.

(c) This SECTION expires January 1, 2015.".

Renumber all SECTIONS consecutively.

and when so amended that said bill do pass.

(Reference is to HB 1009 as introduced.)

MCMILLIN, Chair

Committee Vote: yeas 6, nays 1.