



MARCH 14, 2019

OPPONENT TESTIMONY ON HB 2191

TESTIMONY OF

Letitia Harmon

POLICY DIRECTOR, AMERICAN CIVIL LIBERTIES UNION OF KANSAS

KANSAS SENATE COMMITTEE ON JUDICIARY

Thank you, Chair Wilborn, and members of the Committee for affording us the opportunity to provide testimony on HB 2191.

The American Civil Liberties Union (ACLU) of Kansas is a non-partisan, non-political membership organization dedicated to preserving and strengthening the constitutional liberties afforded to every resident of Kansas. We work to preserve and strengthen our constitutional rights and freedoms through policy advocacy, litigation, and education. We proudly serve over 40,000 supporters in Kansas and represent more than 1.7 million supporters nationwide.

We urge you to vote no on HB 2191, as it has numerous privacy concerns and would infringe on 4th Amendment rights. Nothing in this bill limits the scope of review or examination of the data by outside parties. Nothing in this bill limits the amount of time outside parties can hold on to these records and there is no destruction process once the material is no longer being used in a search. Nothing in this bill protects people who have had false information shared with outside parties. Nothing in this bill prevents sharing of information with ICE or federal agencies.

Law Enforcement may interpret the proposed language in this bill as a license to seize more data than what is identified in the warrant.

- The language in the bill covers a broad category of materials, including any device which could store electronic information, any media with electronically stored information, etc. This seems to grant an unspecified license that could be interpreted as seizing *any* electronically stored information, even beyond that which is identified in the warrant itself. The Fourth Amendment requires items subject to search and seizure be identified with particularity.
- Permitting law enforcement to essentially copy and transfer this data to review at a later time/date gives them the opportunity to do a much more comprehensive search than would otherwise be available and that search will very likely go beyond the scope of the warrant.

Government collection of private data bears with it a concomitant responsibility to protect that data

- In a society where so much of our information is stored online, on electronic devices, and in databases over which we may have little or no control, privacy is a constant concern for every citizen. If the government puts itself in the position of holding private data, then it must also provide protections to prevent that data from being accessed and used by any unauthorized party. This bill gives broad discretion and indicates this information

- A data breach is the unauthorized disclosure of information compromising the confidentiality of personally identifiable information. The state of Kansas itself, in fact, defines “security breach” as the “unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information...” The federal Health Insurance Portability and Accountability Act (HIPAA) also defines a breach as the “unauthorized acquisition, access, use or disclosure” of protected health information—not merely the compromise of that information by hackers.
- Kansas does not have a good track record with this. For example, after a Crosscheck open records request, an independent auditor found the site exposed the private information of more than 900 Kansans, compromising everything from partial social security numbers in combination with full names and birthdates to home addresses and relationships. This information was stored on the Secretary of State website (sos.ks.gov) which researchers found is better managed than many other networks associated with the ks.gov domain are. Experts said even this more secure network within the ks.gov system was “significantly exposed.” Ultimately, the researchers found that infiltration of the larger Kansas government, by even a modestly proficient hacker, would be all but guaranteed.¹

HB 2191 may permit cross-agency sharing that is illegal, according to the United States District Court of South Dakota in United States v. Hulscher.

- If a police agency gets a search warrant and seizes a target’s iPhone, can the agency share a copy of all of the phone’s data with other government agencies in the spirit of “collaborative law enforcement among different agencies”? Not without the Fourth Amendment being violated, a federal court ruled in United States v. Hulscher, 2017 WL 657436 (D.S.D. February 17, 2017).² This case makes it clear that private electronic information must remain just that.
- The court’s conclusion stated: “The government’s review of Hulscher’s unsegregated iPhone data constituted a search under the Fourth Amendment. Because the Leon good faith exception and the plain view doctrine do not apply, the government’s search of Hulscher’s iPhone data violated Hulscher’s Fourth Amendment rights.”³

Summary

The proposed language poses serious potential privacy violations and opens confidential information to illegal seizure. The bill does not specify how the information will be stored or destroyed to protect privacy. Rather, it allows for broad sharing and distribution to other states and agencies. Due to the decision in United States v. Hulscher, the state of Kansas may be inviting similar litigation. Considering its previous record with exposing private information, the opinion of researchers and experts is that any private electronically stored data managed through a ks.gov network is vulnerable. Kansas does not currently possess the safeguards to prevent such breaches. We urge you to oppose this bill.

¹ Findings were outlined in a Gizmodo exposé which can be found here: <https://gizmodo.com/as-crosscheck-moves-to-secure-voter-data-hacking-fears-1822344007>

² A summary of the case and of the 4th Amendment implications can be found here: https://www.washingtonpost.com/news/volokh-conspiracy/wp-content/uploads/sites/14/2017/02/Hulscher_Order-adopting-report.pdf?tid=a_inl_manual

³ United States v. Hulscher, 2017 WL 657436 (D.S.D. February 17, 2017)