

DRAFT: IoTAB Privacy Recommendations October 2023

R13 to R14

The recommendations below are based on the presentations made to the IoTAB

- Data sanitization is recommended for government vehicles (Benson+Debbie)
- Support of the Government's effort to enact Federal Data Privacy Regulation based on CTIA letter (Dan+Debbie)

R13 - Mandate NIST Sanitization Standards for Government Automobiles Before Resell

- Description of recommendation to the US government:
 - a. Before reselling, the government should require that agencies adhere to NIST's media sanitization guidelines
- Justification for the recommendation:
 - a. Aligns with the e-Stewards Standard, supported by the Environmental Protection Agency (EPA) Recycling Program.
 - b. Proper data sanitization can protect consumer privacy and prevent unauthorized access to sensitive information stored in modern vehicle systems.
- Implementation Considerations that the US government needs to consider:
 - a. Cost of implementation for the government
 - b. Training and awareness programs for government agencies about guidelines
 - c. Technology infrastructure required to support the sanitization processes
 - d. Monitoring and compliance mechanisms

DRAFT: IoTAB Privacy Recommendations October 2023 R13 to R14

- Potential implementation barriers to the US government:
 - a. The expense of procuring and deploying data sanitization tools across the entire fleet of government vehicles
 - b. Ensuring compatibility of sanitization solutions with various vehicle models makes, and embedded systems
 - c. Training of government staff and contractors on new data sanitization procedures might be resource-intensive
- Possible participating agencies in the US government who could assist or champion this recommendation:
 - a. National Institute of Standards and Technology (NIST)
 - b. Department of Transportation (DOT)
 - c. Environmental Protection Agency (EPA)
- Things that the US Federal government should consider when implementing this recommendation:
 - a. Use National Cybersecurity Strategy Implementation Plan July 2013 - Initiative Number: 1.1.3 Initiative Title: Increase agency use of frameworks and international standards to inform regulatory alignment
 - b. Use NIST Cybersecurity Framework - PROTECT - Secure Data - 800-88 Rev. 1 - Guidelines for Media Sanitization
 - c. Use The EPA's Implementation (Electronics Recycling Standards: R2 and e-Stewards)

DRAFT: IoTAB Privacy Recommendations October 2023

R13 to R14

R14 - Support Federal Data Privacy Regulation

- Description of recommendation to the US government:
 - a. Support Federal Data Privacy Regulation
- Justification for the recommendation:
 - a. Uniform standards across the nation
 - b. Harmonize the patchwork of state regulations
 - c. Reduced complexity and legal uncertainty for businesses
- Implementation Considerations that the US government needs to consider:
 - a. Addresses data collection, storage, use, and sharing
 - b. Costs associated with implementing and enforcing the regulation
 - c. Transition period and compliance deadlines for businesses currently operating under different state laws.
- Potential implementation barriers to the US government:
 - a. Legislative gridlock and potential
 - b. Opposition from various interest groups
 - c. Managing Preemption & Private Right of Action
 - d. Need for inter-agency cooperation

DRAFT: IoTAB Privacy Recommendations October 2023 R13 to R14

- Possible participating agencies in the US government who could assist or champion this recommendation:
 - a. Federal Trade Commission (FTC)
 - b. Department of Commerce
 - c. House Committee on Energy and Commerce

[REDACTED]

- Things that the US Federal government should consider when implementing this recommendation:
 - a. US State Laws on Privacy to date:
 - i. California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
 - ii. Virginia Consumer Data Protection Act (VCDPA)
 - iii. Colorado Privacy Act (CPA)
 - iv. Utah Consumer Privacy Act (UCPA)
 - v. Connecticut Data Privacy Act (CTDPA)
 - vi. Iowa Consumer Data Protection Act (ICDPA)
 - vii. Indiana Consumer Data Protection Act
 - viii. Tennessee Information Protection Act
 - ix. Montana Consumer Data Privacy Act
 - x. Texas Data Privacy and Security Act (TDPSA)
 - xi. Oregon Consumer Privacy Act (OCPA)

Main document changes and comments

Page 1: Commented [1] Benson Chan 10/22/2023 11:49:00 PM

I recall this recommendation came up during our discussion on privacy for cars. However, as I am reading this now, is there a case to apply this broadly to other things outside of government vehicles. For example, the government has other equipment that it disposes of, and if those things have IoT or other kind of capability to store information, they should also apply this process. I believe for computers the government has something that it does to wipe the information. I don't know about other things like building automation systems, security systems, other types of controllers, etc.

Page 3: Commented [2] Benson Chan 10/22/2023 11:52:00 PM

Can you give examples of how the federal government should support federal data privacy regulation? i.e. in what way(s) should the agency support this? How? I'm just putting myself in the shoes of the readers of our report, and they may ask.. is there a specific thing I should be doing?