DRAFT: IoTAB Privacy Recommendations July 2023 1 to 7

1. Use Plain Language in Privacy Policies for IoT

Description of recommendation to the US government:

- Use Plain Language in Privacy Policies as part of the Federal Acquisition Regulation (FAR) requirements per the Internet of Things (IoT) Cybersecurity Improvement Act of 2020

- Advocate for the simplification of privacy policies, privacy notices, and data use policies to enhance accessibility and comprehension for users

- Promote the adoption of the "Plain Writing Act of 2010" (Public Law 111-274) as a means for the government to enforce this recommendation on organizations that provide IoT technology to the government

Justification for the recommendation:

- Improved understanding of Data Privacy policies for users, leading to more informed decisions when using IoT devices
- Enhanced public trust in IoT devices and related technologies
- Simplified policies may lead to increased compliance and reduced legal disputes

Implementation Considerations that the US government needs to consider:

- Develop guidelines and best practices for organizations to follow when simplifying privacy policies
- Establish high-level guidance for evaluating and assessing the readability of privacy policies
- Coordinate with relevant stakeholders, including the private sector and business, government, and consumer data advocacy groups, to ensure widespread adoption

Potential implementation barriers to the US government:

- Resistance from organizations that may perceive simplification as a limitation on their legal protections
- Possible challenges in defining the appropriate level of simplification while maintaining accuracy and comprehensiveness
- Monitoring and updating the simplification guidelines to account for technological advancements and emerging privacy concerns

Possible participating agencies in the US government who could assist or champion this recommendation:

- National Institute of Standards and Technology (NIST)
- Department of Commerce (DoC)
- The Office of Management and Budget (OMB) is responsible for overseeing the implementation of the Act and ensuring that each agency has a Plain Writing program in place
- Office of the National Cyber Director (ONCD)

Things that the US Federal government should consider when implementing this recommendation:

- Procurement: Create requirements for IoT providers to implement simplified privacy policies for government contracts
- Use National Cybersecurity Strategy Implementation Plan July 2013 - Initiative Number: 3.2.1 Initiative Title: Implement Federal Acquisition Regulation (FAR) requirements per the Internet of Things (IoT) Cybersecurity Improvement Act of 2020
- Use National Cybersecurity Strategy Implementation Plan July 2013 -Initiative Number: 1.1.1 Initiative Title: Establish an initiative on cyber regulatory harmonization
- Plain Writing Act of 2010" (Public Law 111-274)

---

2. Establish "Third-Party" Data Sharing and Data Use Policies

Description of recommendation to the US government:

- Establish clear policies for third-party data sharing and IoT device data use.
- Outline IoT manufacturers' and service providers' responsibilities and obligations when dealing with third-party entities.
- Emphasize user consent and secure data practices.

Justification for the recommendation:

- Increased interconnectivity and data-sharing capabilities of IoT devices present significant privacy risks.
- Policies safeguard users' personal data and ensure transparency.
- Clear policies foster trust and encourage IoT adoption.

Implementation Considerations that the US government needs to consider:

- Create guidelines on how to effectively communicate third-party data sharing and data use in privacy policies
- Implement public awareness campaigns about these policies to educate users about their data rights

Potential implementation barriers to the US government:

- Resistance from IoT companies who rely on third-party data sharing for business operations
- Challenges in aligning these policies with existing privacy regulations and international data protection standards

Possible participating agencies in the US government who could assist or champion this recommendation:

- National Institute of Standards and Technology (NIST)
- Federal Trade Commission (FTC)
- Department of Energy (DOE)
- United States Department of Agriculture (USDA)
- Office of the National Cyber Director (ONCD)

Things that the US Federal government should consider when implementing this recommendation:

- Policies & Frameworks: Work with industry leaders to establish data use guidelines for Third-Party" Data Sharing and Data Use Policies
- Use National Cybersecurity Strategy Implementation Plan July 2013 -Initiative Number: 1.1.1 Initiative Title: Establish an initiative on cyber regulatory harmonization
- 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

---

3. Create an IoT Privacy Framework for Innovation and Data Protection

Description of recommendation to the US government:

- Develop an IoT Privacy Framework for Innovation and Data Protection specifically tailored to the unique challenges posed by IoT devices

- Ensure that the framework balances the need for Data Privacy and security with fostering innovation in the IoT sector
- The goal of the framework is that it can be used as a voluntary guideline across any sector that develops or implements IoT

Justification for the recommendation:

- Provides a consistent, unified approach to Data Privacy and security in the IoT sector, reducing confusion and fragmentation for business, government, and consumers

- Several US States have passed comprehensive privacy laws, and several other states are in the process of advancing privacy legislation.

- Encourages innovation by providing clear guidelines and expectations for IoT device manufacturers, fostering a competitive and growth-oriented environment

Implementation Considerations that the US government needs to consider:

- Incorporate lessons learned from existing privacy regulations, such as the CCPA and GDPR, to create a more effective and efficient framework
- Ensure that the framework is adaptable and scalable to accommodate the rapidly evolving nature of IoT technology and the Data Privacy Landscape

Potential implementation barriers to the US government:

- Balancing between protecting business, government, and consumers Data Privacy and fostering innovation in the IoT sector
- Providing resources, guidance, and support to businesses for the adoption and implementation of the IoT Privacy Framework
- Reviewing and updating the IoT Privacy Framework to ensure it remains relevant and effective in addressing emerging Data Privacy challenges and technological advancements

Possible participating agencies in the US government who could assist or champion this recommendation:

- National Institute of Standards and Technology (NIST)

Things that the US Federal government should consider when implementing this recommendation:

- Partnership: Develop the IoT Privacy Framework in partnership with industry and privacy experts
- Working with US States: Collaboration with US States who have already passed privacy laws or are in the process of advancing legislation would be key for regulatory alignment
- Use National Cybersecurity Strategy Implementation Plan July 2013 -Initiative Number: 1.1.1 Initiative Title: Establish an initiative on cyber regulatory harmonization
- 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

---

4. Include IoT in US Federal Privacy Regulation Proposal

Description of recommendation to the US government:

- Add IoT Data Retention Transparency: Establish guidelines for manufacturers to establish clear policies on how long business, government, and consumer data is retained

- Supports US Federal Privacy Legislation

Justification for the recommendation:

- Supports contemplated federal legislation, e.g., American Data Privacy and Protection Act (ADPPA) H. R. 8152 legislation

- Adds IoT-specific language to the ADPPA related to IoT Data Retention Transparency

- Ensures that IoT device manufacturers share a consistent set of privacy standards, enhancing business, government, and consumer data trust and protection

- Facilitates innovation by providing clear guidelines and expectations for IoT businesses, fostering a competitive and growth-oriented environment

Implementation Considerations that the US government needs to consider:

- Update the American Data Privacy and Protection Act (ADPPA) H. R. 8152 legislation to address emerging Data Privacy challenges and technological advancements related to IoT

Potential implementation barriers to the US government:

- Achieving consensus among stakeholders and state-level regulators on the most effective elements and practices to incorporate into the Federal Privacy legislation
- Ensuring compatibility with existing national and international privacy regulations
- Balancing between protecting business, government, and consumer Data Privacy and fostering innovation in the IoT sector
- Providing resources, guidance, and support to businesses for the adoption and implementation of the IoT specific requirements

Possible participating agencies in the US government who could assist or champion this recommendation:

- Congress
- Department of Commerce (DoC)
- National Institute of Standards and Technology (NIST)
- Federal Trade Commission (FTC)

Things that the US Federal government should consider when implementing this recommendation:

- Legislation: Support IoT addition to contemplated Federal Data Privacy legislation (e.g., the American Data Privacy and Protection Act, or ADPPA)

---

5. Privacy Transparency for IoT

Description of recommendation to the US government:

- Develop and implement a privacy transparency system for IoT devices, using the “U.S. Cyber Trust Mark” for business, government, and consumer data for Connected Devices and other transparency programs as a guide

Justification for the recommendation:

- Empowers businesses, governments, and consumers to make informed decisions about IoT devices based on their privacy features and practices
- Encourages IoT device manufacturers to prioritize privacy, fostering competition and innovation in privacy-enhancing technologies
- Enhances overall Cybersecurity and data protection by promoting greater business, government, and consumer data awareness of privacy practices

Implementation Considerations that the US government needs to consider:

- Consider input from privacy experts, industry stakeholders, and business, government, and consumer data advocacy groups to develop privacy transparency, including content and design
- Develop guidelines and standards for privacy transparency, including required information, format, and or product information
- Encourage IoT device manufacturers to adopt privacy transparency and provide resources to help them align with the new recommendations

Potential implementation barriers to the US government:

- Ensuring broad adoption and compliance with the privacy transparency system across different industries and sectors
- Incentivizing IoT device manufacturers who may perceive privacy transparency as burdensome, costly, or restrictive
- Balancing the need for comprehensive privacy information with simplicity and ease of understanding for businesses, the government, and consumers

Possible participating agencies in the US government who could assist or champion this recommendation:

- Department of Commerce (DoC)
- National Institute of Standards and Technology (NIST)
- Federal Trade Commission (FTC)

Things that the US Federal government should consider when implementing this recommendation:

- Promotion: Publicize the benefits of IoT privacy transparency
- Partnership: Work with industry leaders to develop privacy transparency

- Use National Cybersecurity Strategy Implementation Plan July 2013 -Initiative Number: 1.1.1 Initiative Title: Establish an initiative on cyber regulatory harmonization
- Use National Cybersecurity Strategy Implementation Plan July 2013 - Initiative Number: 3.2.2 Initiative Title: Initiate a U.S. Government IoT security labeling program “U.S. Cyber Trust Mark”

---

6. Recommendation #6: Create IoT-focused educational initiatives for workforce development and business, government, and consumer data privacy/trust

Description of recommendation to the US government:

- Develop educational initiatives that include IoT, targeting workforce development, and enhancing business, government, and consumer data privacy and trust

Justification for the recommendation:

- Increase in the understanding and safe use of IoT technologies
- Development of a highly skilled workforce capable of addressing IoT privacy challenges
- Boosting business, government, and consumer data trust and adoption of IoT devices and services

Implementation Considerations that the US government needs to consider:

- Defining the scope and content of educational initiatives
- Identifying key target audiences (schools, universities, businesses, general public)
- Workforce development to encompass personas, including manufacturers, Implementors, service providers, and workers.
- Collaborating with educational institutions and industry leaders
- Ensuring the relevancy and practicality of the educational content
- Regularly updating the initiatives to keep pace with technological changes
- Evaluating the effectiveness of the initiatives through regular assessments and feedback

Potential implementation barriers to the US government:

- Difficulty in keeping up with the fast-paced advancements in IoT
- Challenges in reaching and engaging the targeted audiences
- Securing sufficient funding and resources

Possible participating agencies in the US government who could assist or champion this recommendation:

- National Institute of Standards and Technology (NIST)
- Office of the National Cyber Director (ONCD)

Things that the US Federal government should consider when implementing this recommendation:

- Promotion & Education: Publicize the importance of IoT education and promote the adoption of educational programs for workforce development and business, government, and consumer data trust
- Use National Cybersecurity Strategy Implementation Plan July 2013 - Initiative Number: 4.6.1 Initiative Title: Publish a National Cyber Workforce and Education Strategy and track its implementation

7. **Recommendation #7: Promote the implementation of Privacy-Enhancing Technologies (PETs) in IoT systems**

Description of Recommendation to the US Government: Promote the implementation of Privacy-Enhancing Technologies (PETs) in IoT systems.

Justification for the Recommendation:

- PETs protect privacy while extracting valuable insights from the vast IoT data
- They align with responsible data use without compromising user privacy
- PETs support broader U.S. goals of leveraging technology for societal benefits
- Their use fosters trust and promotes acceptance of IoT solutions
- Implementation of PETs can prevent data breaches and associated legal issues

Implementation Considerations that the US Government Needs to Consider:

- Ensuring robust security measures for PETs to prevent unauthorized data access
- Conducting comprehensive technical and ethical evaluations of PETs before their adoption
- Enhancing public understanding and Trust in PETs
- Encouraging interoperability between different PETs systems
- Establishing a framework for monitoring the effectiveness and impacts of PETs in IoT

Potential Implementation Barriers to the US Government:

- Limited technical expertise to understand, implement, and manage PETs
- Possible resistance from private sectors due to perceived risks or costs
- The complexity of developing universally accepted privacy standards for IoT

Possible Participating Agencies in the US Government:

- The Office of Science and Technology Policy (OSTP)
- National Institute of Standards and Technology (NIST)

Things that the US Federal Government Should Consider When Implementing This Recommendation:

- Internet of Things (IoT) Cybersecurity Improvement Act of 2020
- The White House's Advancing a Vision for Privacy-Enhancing Technologies proposal (June 2022)
- Use National Cybersecurity Strategy Implementation Plan July 2013 - Initiative Number: 1.2.1 Initiative Title: Scale public-private partnerships to drive development and adoption of secure-by-design and secure-by-default technology