Privacy Subteam Recommendations

NIST
National Institute of Standards and Technology

May 2023

Internet of Things Advisory Board (IoTAB)

Privacy Subteam Members

- Subteam Members: Debbie Reynolds, Kevin Kornegay, Maria Rerecich, Mike Bergman
- Advisor: Barbara Cuthill
- Contractors: Brad Hoehn, Greg Witte
- Chair: Debbie Reynolds

Opportunities

- Policy and / or Regulation should be considered in the US
- Privacy by Design throughout the IoT lifecycle
- Enable International data-sharing agreements
- Promote best practices for data collection and data sharing
- Education about the use of IoT devices (user or worker)
- Standardization of Privacy Policies
- Investigate the cybersecurity label program for privacy
- Incentives regarding liability protections for compliance
- Metrics to assess the risks of how the user interacts with IoT

Barriers

- Lack of transparency about IoT
- Lack of Trust in IoT
- Lack of education about the use of IoT devices, including hazards (user or worker)
- Lack of understanding of the data being collected by IoT devices
- Lack of control or agency in data collection
- Re-identification of individuals from data sources
- Digital divide (not everyone has access to 5G, IoT, etc.)

Recommendations list (summary list)

1. Simplifying Privacy Policies for Reading Accessibility
2. Establish “Data Use” basics for Data Privacy Policies
3. Learning from CCPA, GDPR, and other Privacy Regulations
4. Create a National Privacy Framework for Innovation and Data Protection
5. Implementing US Federal Privacy Regulation
6. Privacy Label Creation for IoT
7. Establish “Third-Party” Data Sharing and Data Use Policies
8. Create IoT-focused educational initiatives for workforce development and consumer privacy/trust

Recommendation #1

Simplifying Privacy Policies for Reading Accessibility for IoT

Recommendation

- 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

- 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

Recommendation #1 (details)

Implementation considerations

- 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 consumer advocacy groups, to ensure widespread adoption.

Implementation barriers

- 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

Recommendation #1 (details cont'd)

Possible participating federal agencies

- Federal Trade Commission (FTC)
- 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.

Federal considerations

- Procurement: Prioritize companies with simplified privacy policies in government contracts
- Tax incentives: Provide tax benefits to companies that simplify their privacy policies
- Promotion: Highlight companies that are leading in this area
- Legislation: Create legislation requiring simplified privacy policies
- Regulation: Create regulations for readability standards
- Partnership: Collaborate with industry leaders to develop best practices

Recommendation #1 (Benefits)

Benefits

- The law already exists
- All US government agencies already have a plain language policy
- The US government could extend these requirements to organizations that do business with the government

Recommendation #1 (References)

References

- Public Law 111 - 274 - Plain Writing Act of 2010 GovInfo. https://www.govinfo.gov/app/details/PLAW-111publ274. Accessed 17 Apr. 2023

Recommendation #2

Establish “data use” basics for privacy policies

Recommendation

- Create a set of "data use" basics that must be included in privacy policies for IoT devices
- Ensure that these policies are designed with the consumers' needs and understanding in mind

Justification

- Provides consumers with a standardized baseline of information regarding data use, making it easier for them to compare and understand different policies
- Enhances trust in IoT technology by ensuring transparency and consistent communication of data practices

Recommendation #2

Implementation considerations

- Create guidelines on how to effectively communicate these basics in privacy policies
- Encourage or require IoT device manufacturers to adopt these "data use" basics in their privacy policies

Implementation barriers

- Ensuring broad adoption and compliance with the established "data use" basics across different industries and sectors
- Balancing the need for standardized information with the unique characteristics and data practices of individual IoT devices and services

Recommendation #2 (details)

Possible participating federal agencies

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

Federal considerations

- Procurement: Prefer companies that clearly define data use in their privacy policies
- Tax incentives: Offer tax breaks for comprehensive data use transparency
- Promotion: Publicize the importance of clear data use policies
- Legislation: Mandate clear data use disclosures
- Regulation: Set standards for data use disclosures
- Partnership: Work with industry leaders to establish data use guidelines

Recommendation #3

Learning from CCPA, GDPR, and other Privacy Regulations

Recommendation

- Analyze and learn from existing privacy regulations, such as the California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR), and others
- Develop a high-level privacy framework for IoT devices, incorporating successful elements and lessons learned from these regulations

Justification

- Leveraging the experience and knowledge gained from implementing existing privacy regulations can help create a more effective and efficient IoT privacy framework
- Provides a foundation for a harmonized approach to privacy in the IoT sector, reducing confusion and fragmentation for both consumers and businesses

Recommendation #3 (details)

Implementation considerations

- Conduct a thorough analysis of the CCPA, GDPR, and other privacy regulations to identify best practices, potential improvements, and lessons learned
- Ensure that the IoT privacy framework is adaptable and scalable to accommodate the rapidly evolving nature of IoT technology and the data privacy landscape

Implementation barriers

- Achieving consensus among stakeholders on the most effective elements and practices to incorporate into the IoT privacy framework
- Overcoming potential resistance from industry participants who may perceive new regulations as burdensome or restrictive
- Ensuring compatibility with existing privacy regulations at the state and international level
- Balancing between protecting 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

Recommendation #3 (details cont'd)

Possible participating federal agencies

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

Federal considerations

- Procurement: Favor companies adhering to proposed privacy regulations
- Tax incentives: Give tax incentives to companies following privacy standards
- Promotion: Encourage the adoption of privacy standards
- Legislation: Incorporate elements of privacy standards into federal law proposals
- Regulation: Implement regulatory measures to include key elements of privacy standards that are not already being considered in Federal privacy proposals (like standrization and use of the CCPA data categories)
- Partnership: Collaborate with international and US State bodies to learn from their experiences

Recommendation #4

Create a National Privacy Framework for Innovation and Data Protection

Recommendation

- Develop a National 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 the develops or implements IoT

Justification

- Provides a consistent, unified approach to data privacy and security in the IoT sector, reducing confusion and fragmentation for both consumers and businesses
- Encourages innovation by providing clear guidelines and expectations for IoT device manufacturers, fostering a competitive and growth-oriented environment

Recommendation #4 (details)

Implementation considerations

- 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

Implementation barriers

- Achieving consensus among stakeholders on the most effective elements and practices to incorporate into the National Privacy Framework
- Overcoming potential resistance from industry participants who may perceive new regulations as burdensome or restrictive
- Ensuring compatibility with existing privacy regulations at the state and international level
- Balancing between protecting consumers' Data Privacy and fostering innovation in the IoT sector
- Providing resources, guidance, and support to businesses for the adoption and implementation of the National Privacy Framework
- Reviewing and updating the National Privacy Framework to ensure it remains relevant and effective in addressing emerging Data Privacy challenges and technological advancements

Recommendation #4 (details cont'd)

Possible participating federal agencies

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

Federal considerations

- Procurement: Favor companies that adhere to the National Privacy Framework
- Tax incentives: Offer tax incentives for adopters of the National Privacy Framework
- Promotion: Publicize the benefits of the National Privacy Framework
- Partnership: Develop the National Privacy Framework in partnership with industry and privacy experts

Recommendation #5

Implementing US Federal Privacy Regulation

Recommendation

- Develop and implement a comprehensive US Federal Privacy Regulation that addresses data privacy concerns for IoT devices and services
- Create a unified legal framework that supersedes state-level regulations, providing clarity and consistency for both consumers and businesses
- The Federal Privacy Regulation should be a baseline (instead of a ceiling) to create harmonization of terminology and support foundational principles in the US

Justification

- Streamlines and harmonizes data privacy regulations across the nation, reducing fragmentation and confusion
- Ensures that IoT device manufacturers adhere to a consistent set of privacy standards, enhancing consumer trust and protection
- Facilitates innovation by providing clear guidelines and expectations for IoT businesses, fostering a competitive and growth-oriented environment

Recommendation #5 (details)

Implementation considerations

- Use information gathered from stakeholders, including IoT device manufacturers, privacy experts, and consumer advocacy groups, on the development of the Federal Privacy Regulation
- Consider state-level regulations to ensure a unified federal regulation
- Regularly review and update the Federal Privacy Regulation to address emerging data privacy challenges and technological advancements

Implementation barriers

- Overcoming potential resistance from industry participants who may perceive new regulations as burdensome or restrictive
- Achieving consensus among stakeholders and state-level regulators on the most effective elements and practices to incorporate into the Federal Privacy Regulation
- Ensuring compatibility with existing international privacy regulations, such as the GDPR, for businesses operating in global markets
- Providing resources, guidance, and support to businesses for the adoption and implementation of the Federal Privacy Regulation
- Collaborating with international partners to ensure global alignment and interoperability of privacy regulations, fostering global trust and cooperation in IoT Data Privacy and security

Recommendation #5 (details cont'd)

Possible participating federal agencies

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

Federal considerations

- Procurement: Prioritize companies that follow Federal Privacy Regulations
- Tax incentives: Provide tax benefits to companies that demonstrate regulatory compliance
- Promotion: Publicize the importance and benefits of privacy regulation compliance
- Legislation: Create legislation to implement federal privacy regulations
- Regulation: Enforce federal privacy regulations across all applicable sectors

Recommendation #6

Privacy Label Creation for IoT

Recommendation

- Develop and implement a privacy label system for IoT devices, similar to nutrition labels on food products (similar to the White House initiative for cybersecurity labeling)
- Display essential privacy information in an easily understandable format for consumers, enhancing transparency and trust
- Cybersecurity and Data Privacy are not the same, so this distinction should be evident in this labeling scheme

Justification

- Empowers 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 consumer awareness of privacy practices

Recommendation #6 (details)

Implementation considerations

- Consider input from privacy experts, industry stakeholders, and consumer advocacy groups to develop the privacy label system, including content and design
- Develop guidelines and standards for privacy labels, including required information, format, and placement on packaging or product information
- Encourage or require IoT device manufacturers to adopt privacy labels and provide resources to help them comply with the new requirements
- Consider the potential impact on market competition and innovation if privacy labels are perceived as overly restrictive or burdensome
- Educate consumers about the importance of privacy labels and how to use them effectively when making purchasing decisions
- Reviewing and updating the privacy label system to ensure it remains relevant and effective as IoT technology evolves and new Data Privacy concerns emerge

Implementation barriers

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

Recommendation #6 (details cont'd)

Possible participating federal agencies

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

Federal considerations

- Procurement: Choose IoT products with clear privacy labels compliance for government use
- Tax incentives: Give tax benefits to companies that implement privacy labels
- Promotion: Publicize the benefits of privacy labels
- Legislation: Create legislation requiring privacy labels on IoT devices
- Regulation: Regulate the standards for privacy labels
- Partnership: Work with industry leaders to develop privacy labels

Recommendation #7

Establish “Third-Party” Data Sharing and Data Use Policies

Recommendation

- Formulate clear and robust policies regarding data sharing and data usage involving third parties in the IoT ecosystem

Justification

- Ensures transparency, enhancing user trust in IoT devices and services
- Protects user data from misuse and unauthorized access
- Promotes regulatory compliance and responsible data practices among third parties Ensuring the policies are adaptable to evolving IoT technologies and practices
- Engaging stakeholders in the development and implementation process
- Establishing a clear timeline and process for businesses to adapt to the new policies

Recommendation #7 (details)

Implementation considerations

- Defining what constitutes "third-party" in different IoT contexts
- Setting guidelines for obtaining user consent for data sharing and usage
- Instituting penalties for non-compliance

Implementation barriers

- Resistance from businesses due to potential impact on operations and revenue
- Technical challenges in monitoring and enforcing compliance
- Balancing privacy protection with innovation and industry growth

Recommendation #7 (details cont'd)

Possible participating federal agencies

- Department of Commerce (DoC)
- Federal Trade Commission (FTC)

Federal considerations

- Procurement: Prefer companies with clear third-party data sharing policies
- Tax incentives: Offer tax breaks to companies that regulate third-party data sharing
- Promotion: Promote responsible third-party data sharing practices
- Legislation: Propose legislation regulating third-party data sharing
- Regulation: Set standards for third-party data sharing and usage in the US
- Partnership: Collaborate with industry to establish third-party data sharing guidelines for IoT

Recommendation #8

Create IoT-focused educational initiatives for workforce development and consumer privacy/trust

Recommendation

- Develop educational initiatives that focus on IoT, targeting workforce development and enhancing consumer privacy and trust

Justification

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

Recommendation #8 (details)

Implementation considerations

- Defining the scope and content of educational initiatives
- Identifying key target audiences (schools, universities, businesses, general public)
- 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

Implementation barriers

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

Recommendation #8 (details cont'd)

Possible participating federal agencies

- Department of Commerce (DoC)
- National Institute of Standards and Technology (NIST)
- Department of Education (DoE)?

Federal considerations

- Procurement: Purchase educational materials and services from providers focused on IoT
- Tax incentives: Provide tax benefits to companies that invest in IoT education
- Promotion: Publicize the importance of IoT education for workforce development and consumer trust
- Legislation: Create legislation to incorporate IoT education in public and private sectors
- Regulation: Set standards for IoT education initiatives
- Partnership: Collaborate with educational institutions, technology companies, and workforce development organizations to create and deliver effective IoT-focused education initiatives

Additional Recommendations to explore

- International Agreements

QUESTIONS