Privacy Subteam Recommendations September 2023

Privacy Subteam Members:

Debbie Reynolds
Maria Rerecich
Kevin Kornegay
Mike Bergman

Image: https://www.simplilearn.com/iot-devices-article

Chair: Debbie Reynolds
Advisor: Barbara Cuthill
Contractors: Brad Hoehn, Greg Witte

Internet of Things Advisory Board (IoTAB)

NEW - Summary of Recommendations – Privacy Subgroup

R09 - Include IoT Privacy Information on New Car Automobile “Monroney Stickers”

R10 - Mandate NIST Sanitization Standards for Used Automobiles Before Resell

R11 - Endorse Universal Opt-Out Signals for IoT Devices and Companion Apps

R12 - Add "Location Tracking Enabled" notice to U.S. Cyber Trust Mark IoT devices

The recommendations created as a result of ideas from presentations made to the IoTAB regarding Data Privacy and IoT:

Andrea Amico, Privacy 4 Cars
Topic - Privacy in Automobiles
IoTAB Subgroup - privacy

Jeff Jockisch (Avantis Privacy), Colby Scullion (Avantis Privacy)
Topic - Location Data Privacy
IoTAB Subgroup - Privacy

Mozilla Foundation Automobile Privacy Report “Privacy Not Included” - Sept 2024

- 100% of the 25 car brands reviewed by The Mozilla Foundation collect personal data
- 84% of car brands share or sell your data
- 92% give drivers little to no control over their personal data
- 68% of the car brands earn the “bad track record” ding for leaks, hacks, and breaches that threatened their drivers’ privacy
- 0% of car brands that are part of the ALLIANCE FOR AUTOMOTIVE INNOVATION follow voluntary Consumer Protection Principles and pledges to provide consumers with privacy-preserving principles such as “data minimization,” “transparency,” and “choice.

https://foundation.mozilla.org/en/privacynotincluded

Photo: Spencer Nugent

R09 - Include IoT Privacy Information on New Car Automobile “Monroney Stickers”

R09

Include IoT Privacy Information on “Monroney Stickers” for New Car Automobiles Sold in the US

Justification

- Monroney Stickers already offer crucial information like fuel efficiency and safety ratings, making them a logical platform for additional disclosures
- Providing IoT privacy information helps consumers make informed decisions regarding their personally identifiable information, including 1) data collection, 2) data retention, and 3) data sale
- Aligns with broader initiatives to enhance consumer protection and data privacy
- Addresses growing public concern about how personal data is used and shared by IoT devices in automobiles

Implementation

- Standardization Privacy Information: The language used for IoT privacy statements should be clear, concise, and standardized to prevent confusion.
- Regulatory Alignment: Existing privacy laws must be reviewed to ensure that the sticker amendments align with current legal frameworks.
- Periodic Updates: As IoT technologies evolve, the criteria for what must be disclosed should also be updated periodically.

Barriers

- Resistance from Automakers: Automakers may resist this change due to the costs of modifying Monroney Stickers.
- Consumer Education: There's a possibility that consumers may not fully understand the added IoT information.
- Complex Regulatory Environment: The landscape of IoT and privacy is complex, making standardization challenging.

Agencies

- Federal Trade Commission (FTC)
- National Highway Traffic Safety Administration (NHTSA)
- Federal Communications Commission (FCC)\Department of Transportation (DOT)
- Cybersecurity and Infrastructure Security Agency (CISA)

Federal considerations

- Update to Automobile Information Disclosure Act of 1958, 15 U.S.C. §§ 1231–1233 (Public Law 85-506)

Monroney Sticker Example

Credit: https://futureclassic.us/products/future-classic-bmw-custom-window-sticker

R10 - Mandate NIST Sanitization Standards for Used Automobiles Before Resell

R10

Before reselling, the government should require that car seller organizations adhere to NIST's media sanitization guidelines.

Justification

- Aligns with the e-Stewards Standard, supported by the Environmental Protection Agency (EPA) Recycling Program.
- Proper data sanitization can protect consumer privacy and prevent unauthorized access to sensitive information stored in modern vehicle systems.

Implementation

- Cost of implementation for car sellers
- Training and awareness programs for the car sellers about NIST guidelines
- Technology infrastructure required to support the sanitization processes
- Monitoring and compliance mechanisms

Barriers

- Resistance from car-selling organizations due to increased operational costs
- Potential technological limitations in older vehicle models
- Legal challenges concerning data privacy and compliance

Agencies

- National Institute of Standards and Technology (NIST)
- Department of Transportation (DOT)
- Federal Trade Commission (FTC)
- Environmental Protection Agency (EPA)

Federal considerations

- 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
- Use NIST Cybersecurity Framework - PROTECT - Secure Data - 800-88 Rev. 1 - Guidelines for Media Sanitization
- Use The EPA's Implementation (Electronics Recycling Standards: R2 and e-Stewards)

R11 - Endorse Universal Opt-Out Signals for IoT Devices and Companion Apps

R11

The government should endorse adopting and recognizing Universal Opt-Out Signals for Internet of Things (IoT) devices and any associated applications.

Justification

- The recommendation aims to strengthen user privacy and data protection, which are growing concerns in an increasingly interconnected world.
- Universal Opt-Out Signals would streamline the user experience, making it easier for consumers to manage their privacy settings across multiple IoT devices and companion apps.

Implementation

- The technical feasibility of implementing Universal Opt-Out Signals across a wide range of IoT devices and companion apps.
- Costs associated with setting up the infrastructure to recognize and enforce these Opt-Out Signals.
- Developing standardized guidelines or legislation to mandate the adoption of Universal Opt-Out Signals.

Barriers

- Resistance from IoT manufacturers and app developers who may not want to incur the cost or complexity of implementing Universal Opt-Out Signals.
- Technological constraints in harmonizing Opt-Out Signals across diverse platforms and devices.
- Potential legislative hurdles if this conflicts with existing data protection or privacy laws.

Agencies

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

Federal considerations

- Use National Cybersecurity Strategy Implementation Plan July 2013 Initiative Number: 3.2.2 - Initiative Title: Initiate a U.S. Government IoT security labeling program (Cyber Trustmark)
- UOO - The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA) - Law Passed: January 1, 2023 - Provision Enforcement starts: June 2024
- UOO - Colorado Privacy Act (CPA) - Law Passed: July 1, 2023 - Provision Enforcement starts: July 1, 2024
- UOO - Connecticut Data Privacy Act (CTDPA) - Law Passed: July 1, 2023 - Provision Enforcement starts: July 1, 2024

R12 - Add "Location Tracking Enabled" notice to U.S. Cyber Trust Mark IoT devices

R12

Include as part of the proposed privacy transparency system for IoT devices, using the “U.S. Cyber Trust Mark”, the following statement regarding the privacy of location data, if applicable: Proposed Statement for Inclusion: "Notice: Precise location tracking is enabled by default on this device."

Justification

- Transparency: Consumers have a right to know if their location data is being collected and shared. This statement provides immediate and clear information regarding this aspect.
- Informed Consent: For ethical data collection and use, consumers should be aware of what data is being collected without needing to delve into complex privacy policies.
- Regulatory Alignment: This recommendation aligns with various data protection regulations advocating transparency and informed consent.

Implementation

- Standardization: The statement's wording, visibility, and placement should be standardized across all IoT devices that receive the U.S. Cyber Trust Mark.
- Technical Feasibility: How will the notice be displayed? Will it be part of the physical label, on a website, or listed in an app for user awareness?
- Audits and Compliance: Systems need to be in place to verify that the companies adhere to the notification requirement.

Barriers

- Industry Resistance: Manufacturers may resist the implementation due to perceived negative impacts on sales or added complexity.
- Consumer Education: There is the risk that consumers may fail to understand the importance of the notice.
- Legal Challenges: Companies may argue that this constitutes an unfair labeling or notice burden.

Agencies

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

Federal considerations

- Use National Cybersecurity Strategy Implementation Plan July 2013 - Initiative Number: 4.6.1 Initiative Title: Publish a National Cyber Workforce and Education Strategy

Universal Opt-Out Laws in the US

as of September 2023

- The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA) - Law Passed: January 1, 2023 - Provision Enforcement starts: June 2024
- Colorado Privacy Act (CPA) - Law Passed: July 1, 2023 - Provision Enforcement starts: July 1, 2024
- Connecticut Data Privacy Act (CTDPA) - Law Passed: July 1, 2023 - Provision Enforcement starts: July 1, 2024
- The California Delete Act - To be signed by Governor Before October 14, 2023