Specification for CMU IoT Security and Privacy Label

(CISPL 1.0)

(Last updated on 01/17/2021)

Pardis Emami-Naeini
University of Washington
pardis@cs.washington.edu

Yuvraj Agarwal
Carnegie Mellon University
yuvraj@cs.cmu.edu

Lorrie Faith Cranor
Carnegie Mellon University
lorrie@cmu.edu

Contents

1 Introduction

Consumers are becoming increasingly concerned about the privacy and security practices of their IoT devices [49, 2, 65, 31, 46, 21, 71, 14, 12, 45]. However, information about device privacy and security practices is seldom available for consumers to consider before making a purchase [8, 21, 9]. To fill this gap, we designed an informative and usable privacy and security label for IoT devices.

We conducted an expert study with 22 privacy and security experts from industry, academia, government, and public policy organizations, and asked them what privacy and security information we should include on the label [20]. In addition, we reviewed more than 70 privacy and security standards and guidelines for IoT devices. Our expert study and review of standards and guidelines informed our label design.

To balance the need to convey a large amount of information with a desire for a label that would be accessible to consumers, we designed a layered privacy and security label with two layers. The primary "overview" layer conveys information most likely to be important to consumers in a concise format that could be printed on product packaging or displayed in an online store. In addition, the primary layer includes a QR code and a URL that direct consumers to the secondary "detail" layer, which includes more detailed information.

We conducted a series of semi-structured interviews with consumers and followed a user-centric design process to iteratively improve the label and make it more understandable to consumers. An example of the primary layer and the secondary layer of the label is provided in 1 and 2, respectively.

1.1 Specifications

This document describes the label elements, grouped into three sections: Security Mechanisms, Data Practices, and More Information.

Each element described in this document appears in the primary layer, secondary layer, or both layers of the label. When the label appears in online form, it may have interactive features that allow an additional "Consumer explanation" to be displayed, for example when the user clicks on an information (i) icon. In addition, the secondary layer includes expandable components, denoted with a plus symbol.

For each element, we may provide the following pieces of information:

Layer: Layer of the label on which the element appears.

Mentioned by: Other sources, which talked about the privacy and security practice.

Label example: At least one formatted example of the element.

Consumer explanation: Additional information that may be displayed in an interactive label via hover or other mechanism to explain meaning of element to consumers.

Values: List of possible values along with their consumer explanations, whether more than one value is permitted, and whether the specified values are optional. When only one element is permitted, we indicate: "(one of the following)."

Optional sub-attributes: List of optional sub-attributes.

Linked information: If the value is a URL, a description is provided of the content that should be placed at that URL. This linked information could be optional or required.

Optional additional information: Optional additional details that may be displayed in the label's expanded view.

Best practices: Recommended privacy and security practices associated with an element.

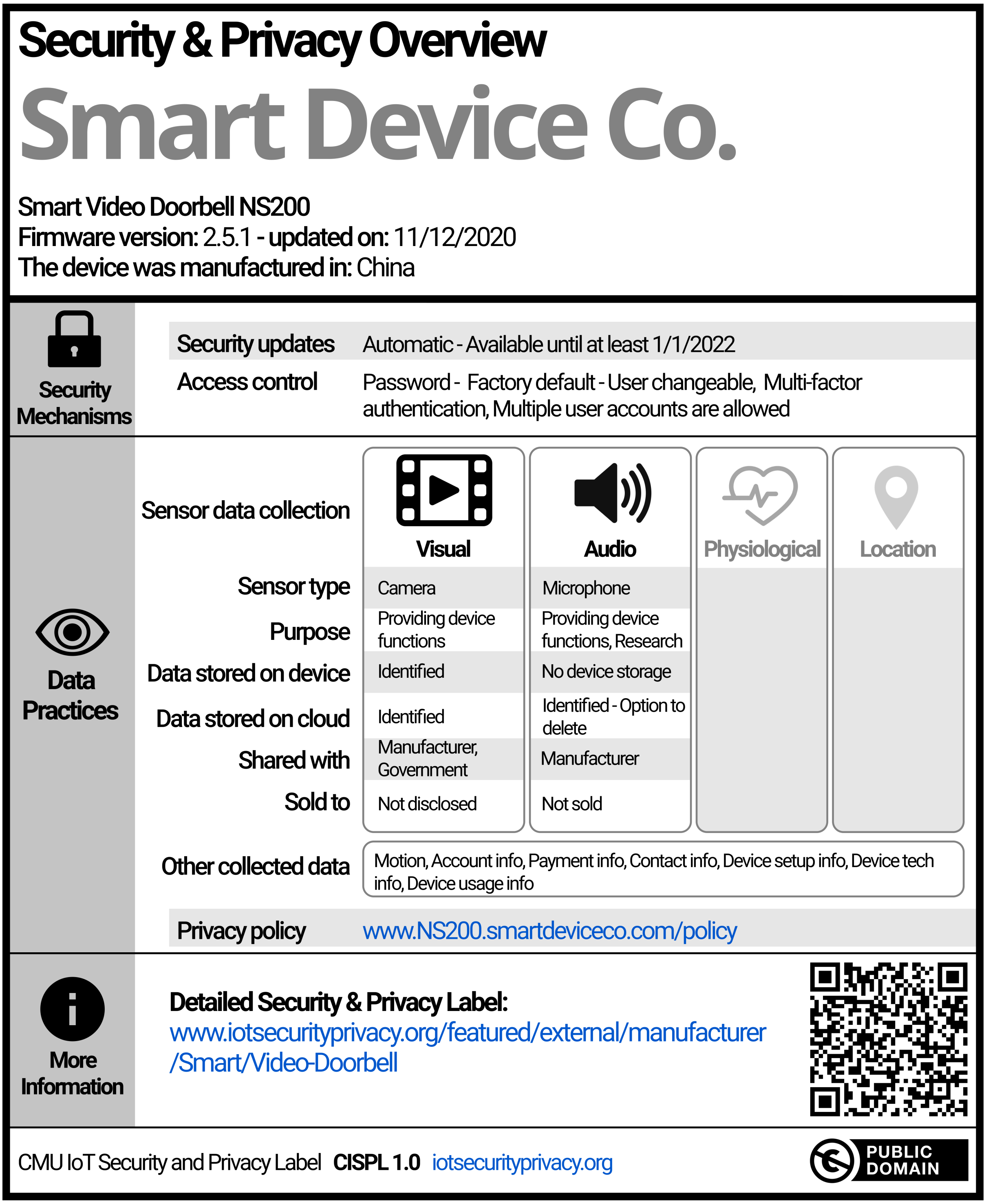
Special note: Additional information that we expect the manufacturer to consider about a value or an attribute.

The following values may be disclosed for any attribute or sub-attribute:

`<not_disclosed>` : Manufacturers can select `<not_disclosed>` option as an attribute value when they prefer not to disclose a particular piece of information. Manufacturers are discouraged from using this option as it limits the utility of the label.

`<other>` : If a value is not listed in this specification that accurately describes a manufacturer's practices, they should use the `<other>` option and provide the relevant information.

1.2 Example of IoT Privacy and Security Label in Use



Security & Privacy Overview

Smart Device Co.

Smart Video Doorbell NS200
Firmware version: 2.5.1 - **updated on:** 11/12/2020
The device was manufactured in: China

Security Mechanisms

Security updates	Automatic - Available until at least 1/1/2022
Access control	Password - Factory default - User changeable, Multi-factor authentication, Multiple user accounts are allowed

Data Practices

Sensor data collection	Visual	Audio	Physiological	Location
Sensor type	Camera	Microphone		
Purpose	Providing device functions	Providing device functions, Research		
Data stored on device	Identified	No device storage		
Data stored on cloud	Identified	Identified - Option to delete		
Shared with	Manufacturer, Government	Manufacturer		
Sold to	Not disclosed	Not sold		

Other collected data	Motion, Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info
Privacy policy	www.NS200.smartdeviceco.com/policy

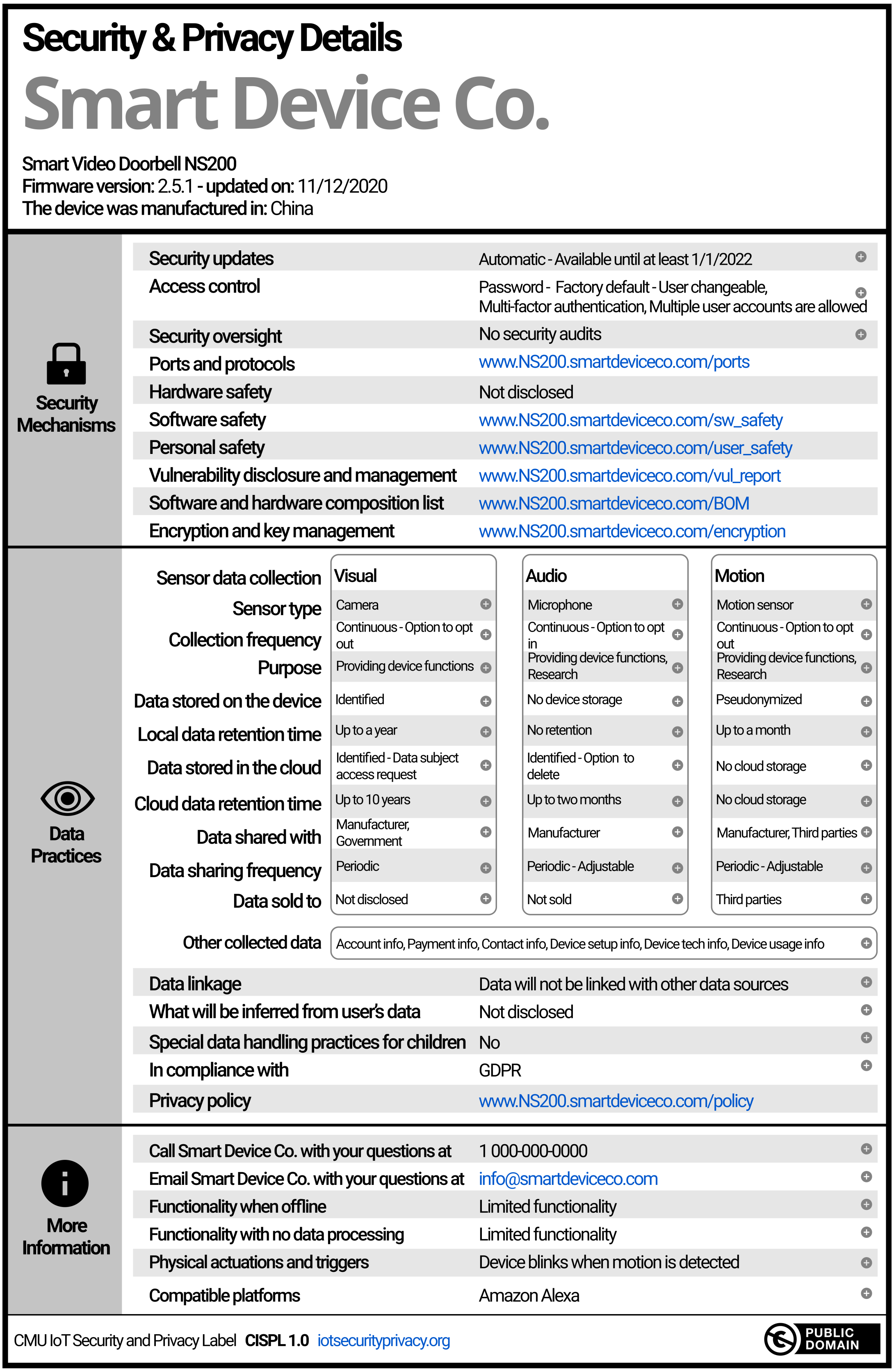
More Information

Detailed Security & Privacy Label:
www.iotsecurityprivacy.org/featured/external/manufacturer/Smart/Video-Doorbell

CMU IoT Security and Privacy Label **CISPL 1.0** iotsecurityprivacy.org

PUBLIC DOMAIN

Figure 1: Primary layer of the label. This layer is designed to be printed on product packaging or to appear on a product website.



Security & Privacy Details

Smart Device Co.

Smart Video Doorbell NS200
Firmware version: 2.5.1 - **updated on:** 11/12/2020
The device was manufactured in: China

Security Mechanisms

Security updates	Automatic - Available until at least 1/1/2022
Access control	Password - Factory default - User changeable, Multi-factor authentication, Multiple user accounts are allowed
Security oversight	No security audits
Ports and protocols	www.NS200.smartdeviceco.com/ports
Hardware safety	Not disclosed
Software safety	www.NS200.smartdeviceco.com/sw_safety
Personal safety	www.NS200.smartdeviceco.com/user_safety
Vulnerability disclosure and management	www.NS200.smartdeviceco.com/vul_report
Software and hardware composition list	www.NS200.smartdeviceco.com/BOM
Encryption and key management	www.NS200.smartdeviceco.com/encryption

Data Practices

Sensor data collection	Visual	Audio	Motion
Sensor type	Camera	Microphone	Motion sensor
Collection frequency	Continuous - Option to opt out	Continuous - Option to opt in	Continuous - Option to opt out
Purpose	Providing device functions	Providing device functions, Research	Providing device functions, Research
Data stored on the device	Identified	No device storage	Pseudonymized
Local data retention time	Up to a year	No retention	Up to a month
Data stored in the cloud	Identified - Data subject access request	Identified - Option to delete	No cloud storage
Cloud data retention time	Up to 10 years	Up to two months	No cloud storage
Data shared with	Manufacturer, Government	Manufacturer	Manufacturer, Third parties
Data sharing frequency	Periodic	Periodic - Adjustable	Periodic - Adjustable
Data sold to	Not disclosed	Not sold	Third parties

Other collected data: Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info

Data linkage	Data will not be linked with other data sources
What will be inferred from user's data	Not disclosed
Special data handling practices for children	No
In compliance with	GDPR
Privacy policy	www.NS200.smartdeviceco.com/policy

More Information

Call Smart Device Co. with your questions at	1 000-000-0000
Email Smart Device Co. with your questions at	info@smartdeviceco.com
Functionality when offline	Limited functionality
Functionality with no data processing	Limited functionality
Physical actuations and triggers	Device blinks when motion is detected
Compatible platforms	Amazon Alexa

CMU IoT Security and Privacy Label **CISPL 1.0** iotsecurityprivacy.org

PUBLIC DOMAIN

Figure 2: Secondary layer of the label. This layer can be accessed from the primary layer by scanning the QR code or typing in the URL.

1.3 Licensing FAQ

How can my organization license the IoT Security & Privacy Label so we can use it?

We are releasing our IoT Security & Privacy label design under a Creative Commons CC0 license because we want organizations to be able to use the label easily and adapt it to meet their needs. To the extent possible under law, we have waived all copyright and related or neighboring rights to our IoT Security and Privacy Label.

Am I allowed to use parts of the label or make changes to the label?

You are welcome to make changes to the label or use components of the label. However, if you do so you may not claim compliance with the CISPL 1.0. We do not endorse any revisions to the label that are not published by us on iotsecurityprivacy.org.

How should I acknowledge the source of the label design?

When using our label design or components of our label design, we would appreciate your acknowledging our efforts by citing one of our research papers or the label specification; by acknowledging Pardis Emami-Naeini, Lorrie Cranor, and Yuvraj Agarwal; or by mentioning iotsecurityprivacy.org. However, this is not a requirement to use the label.

How should I let you know that I am using the label?

We would be interested in hearing about your use of the label, and will link to selected examples of label usage on our website. If you are comfortable with it we can consider adding your label as a featured example on our website. Please email us at contact@iotsecurityprivacy.org.

Will you work with my organization to help us adapt the label for our needs?

Please reach out to us at contact@iotsecurityprivacy.org if you would like us to work with you. We're busy researchers, but as time permits we are happy to help with efforts to further label adoption.

How can I support further research on IoT security and privacy at Carnegie Mellon University?

If you are interested in supporting our research we suggest you become a CyLab partner. This will provide you with early access to our research (and the research of other security and privacy researchers at CMU) and a variety of opportunities such as attending our annual CyLab Partners Conference. You can also support our research through a gift or a sponsored research agreement. Please email us at: yuvraj@cs.cmu.edu and lorrie@cs.cmu.edu if you would like to explore ways to support our research and we would be happy to discuss it further with you.

2 Security Mechanisms

2.1 Security Updates

Layer: Primary and secondary

Mentioned by: [73, 68, 76, 41, 72, 17, 13, 43, 60, 25, 24, 52, 19, 34, 30, 29, 69, 3, 18, 1, 5, 4, 10, 11, 15, 22, 32, 33, 34, 38, 28, 40, 42, 44, 47, 48, 51, 59, 61, 62, 56, 74, 75, 64]

Label example: Automatic - available until at least 1-1-2022

Consumer explanation : How the device receives security updates

Values (one or more of the following)

`<automatic>` Automatic
Consumer explanation: Device will automatically receive security updates

`<manual>` Manual
Consumer explanation: User needs to manually install security updates

`<consent_based>` Consent based
Consumer explanation: User will be asked whether to update the device

`<no_update>` No security updates
Consumer explanation: Device will not receive any security updates

`<not_disclosed>`

`<other>`

Optional sub-attributes for all the values of "Security Updates", except `<not_disclosed>` and `<no_update>` (one of the following)

`<expiration_date>` Available until at least *date*
Consumer explanation: The date until which the device is guaranteed to be updated

Optional additional information

- What controls do users have related to updates (e.g., approve, reject, update notifications)
- Why updates are important to be installed and to what types of risks would users be exposed to if updates are not installed
- Description of how the manufacturer makes updates secure
- How users should install updates
- Justification as to why the device does not get updated
- End-of-life and hardware replacement policy and what users should expect after the update expiration date (e.g., limited functionality, vulnerability management, paying extra fee for updates)
- Justification for update expiration date

Best practices

- Automatic updates should be enabled by default [68, 73, 43, 25, 17, 5, 10, 11, 32, 38, 48, 74], with an option to disable and change the timing of the update if the user is authenticated to do so [25, 38].
- Users should be able to control the timing of updates (e.g., when the device is not in use, at a certain time of day).
- If updates are not automatic by default, users should be notified of available updates and there should be a documented process for users to update their devices [68, 59].
- Update files should be encrypted and be transmitted using encryption [61].
- Updates should be cryptographically signed and get verified for authenticity and integrity before being installed [68, 73, 17, 5, 15, 32, 38, 42, 47, 48, 59, 62].
- Users should be able to approve or reject the updates [59].
- There should be an anti-rollback protection feature to prevent downgrading of the device to an older version of its software and firmware [18, 73, 41, 62].
- Constrained devices that cannot be updated should be isolatable and replaceable [24, 19, 17].
- There should be an easy update installation process for users [68, 41].
- Device should be able to update over-the-air or over-the-wire [73, 25, 17, 74].
- Automatic updates should be phased in over a short time interval to prevent spreading a failure to all instances of a device [38].
- Automatic updates should not change the network protocol interfaces in any way that is incompatible with previous versions [25, 38].
- Devices should be functional when being updated [48] and security updates should not have an impact on the functioning of the device [19]. If new features are introduced by the updates, they should be disabled by default and only be enabled by an authenticated user [38].
- Updates should not change the user-configured preferences and settings [17] without user notification [25, 59].

2.2 Access Control

Layer: Primary and secondary

Mentioned by: [73, 68, 41, 17, 18, 13, 30, 43, 25, 24, 29, 19, 60, 54, 5, 15, 26, 38, 40, 42, 44, 48, 59, 61, 62, 74, 75]

Label example: Password - factory default - user changeable, multiple user accounts

Consumer explanation : How the device can be accessed and who is allowed to access it

Values (one or more of the following)

`<password>` Password
Consumer explanation: Password is required to access the device settings or data

`<biometric>` Biometric
Consumer explanation: User's physical or behavioral characteristics are required to access the device settings or data

`<MFA>` Multi-factor authentication
Consumer explanation: At least two factors are required to access the device settings or data, for example a password and a one-time code sent to a previously registered phone number

`<no_control>` No control over access
Consumer explanation: Anyone can access the device without a password or other authentication method

`<multi_account>` Multiple user accounts
Consumer explanation: To access the device, user needs to create an account; multiple user accounts may be created

`<single_account>` Required user account
Consumer explanation: To access the device, user needs to create an account

`<optional_account>` Optional user account
Consumer explanation: User may create an account, but it is not required

`<no_account>` No user accounts
Consumer explanation: Device does not support the creation of user accounts

`<not_disclosed>`

`<other>`

Optional sub-attributes for `<password>` (one of the following)

`<factory_default>` Factory default
Consumer explanation: The credentials required to access the device have default values that are initially generated by the manufacturer

`<user_generated>` User generated
Consumer explanation: User needs to create their own credentials to access the device

Optional sub-attributes for `<factory_default>` (one of the following)

`<user_changeable>` User changeable
Consumer explanation: User may change the credentials that are required to access the device (for security purposes, make sure to change all default credentials before using the device)

`<not_user_changeable>` Not changeable by user

Consumer explanation: User cannot change the credentials that are required to access the device

Optional additional information

- If one type of access control is password, whether the password is used to protect settings or data
- If one type of access control is password, whether the password is used on the device or for an associated cloud account
- If one type of access control is password, whether the device can be accessed locally without the password
- Tips on how to make strong passwords
- How users can reset their passwords
- What the password expiration policy is
- If the type of access control is multi-factor authentication, what types of factors/-pieces of evidence are required
- If the type of access control is biometric data, what characteristics of the user are required
- Justification as to why no authentication method is being used
- Justification as to why credentials have default values, if any
- Justification as to why users cannot set or change the credentials
- At which stage users can/should set or change the credentials
- Justification as to why users need to have an account to access the mobile application/device
- If it is allowed to create more than one account, what levels of access and privilege each account can have
- If it is allowed to create more than one account, how many accounts can be created to access the device/mobile application
- Justification as to why no user account is needed to access the device/mobile application

Best practices

- If default settings or credentials are used, users should be notified [40].
- Default credentials should be avoided [75]. If default credentials are used, they should be unique to each device [68, 73, 13, 24, 41, 18, 33, 42, 44, 62, 74].
- Credentials should not be re-settable to any factory default values [24, 19].
- If the device can be accessed from a network interface, users should be required to define unique passwords [5, 48].
- Default credentials should be required to be changed by users on the initial setup [73, 13, 25, 17, 18, 38, 44, 48].
- Device should not function until the default credentials are changed by the user [38].
- Systems that allow users to choose passwords should offer users the option to automatically generate a unique password that follows password creation best practices [73].
- A strong password strength policy should be enforced for both default and user-generated passwords [68, 13, 73, 41, 54, 61, 48, 44, 29, 62].
- If a system uses passwords, it should be compatible with the popular password managers [68].
- Rate-limiting techniques should be in place to prevent brute force repeated login attempts [68, 18, 25, 29, 73, 41, 13, 44, 59, 62].
- Services accessible over wireless and IP interfaces should implement session management to limit multiple sessions and users should be logged out after a duration of inactivity [13, 73, 41].
- Secure authentication modification and recovery mechanism(s) should be in place to ensure access can be recovered and users can continue using the system [68, 73, 41].
- Displaying user credentials on login interfaces should be disallowed or obscured by default [25, 41].
- Users should be required to authenticate each time they want to start a new session with the app that controls the device.
- Password recovery and reset protocol should be robust and should not supply an attacker with information indicating a valid account [25].
- Authentication credentials should be salted, hashed and/or encrypted by following industry best practices [25, 73].
- Devices should offer a multi-factor authentication option [68, 17, 13, 18, 25, 59].
- Entered passwords should be masked to prevent exposure on screen [44].
- Users should be notified when the authentication/account security settings have been changed [68].

- The manufacturer should not require users to verify their identity with their government-issued identification or with other forms of identification that could be connected to their offline identity [68].
- Device should have a logging system that records events relating to user authentication, management of account and access rights, modification to security rules, and the functioning of the system [17]. Logs should be stored on durable storage and be retrievable only via an authenticated connection [25, 30, 24].

2.3 Security Oversight

Layer: Secondary

Mentioned by: [68]

Label example: Audits performed by internal and third-party security auditors

Consumer explanation : Manufacturer's use of security audits related to this device

Values (one of the following)

`<internal_audit>` Audits performed by internal security auditors
Consumer explanation: A security team inside the company is commissioned to assess the security practices of the company against a set of documented standards

`<external_audit>` Audits performed by third-party security auditors
Consumer explanation: An independent security team outside of the company is commissioned to assess the security practices of the company against a set of documented standards

`<internal_external_audit>` Audits performed by internal and third-party security auditors
Consumer explanation: Security teams both inside the company and from outside of the company are commissioned to assess the security practices of the company against a set of documented standards

`<no_audit>` No security audits
Consumer explanation: Security practices of the company are not being assessed by anyone

`<not_disclosed>`

Optional additional information

- What criteria are considered to assess the company's security practices
- Who the internal or external auditors are
- How frequent the audits happen
- Findings of the audits
- What the manufacturer will do with the findings of the audits

Best Practices

- If a vulnerability is discovered in the audits, which it could impact users, they should be immediately notified while the manufacturer is working on its patch.
- Audits should happen periodically in the life cycle of the product to ensure continuous security protection.
- The manufacturer should conduct both internal and external security audits on its products and services [68].

2.4 Ports and Protocols

Layer: Secondary

Mentioned by: [73, 41, 30, 43, 60, 24, 19, 17, 13, 25, 29, 18, 5, 10, 57, 15, 33, 34, 40, 44, 47, 59, 60, 61, 62, 56, 74, 63]

Label Example: `www.NS200.example.com/ports`

consumer explanation: List and justification of all the physical interfaces, network ports, and listening services

Values (one of the following)

`<link>` *[Open text field with the following text in grey and not editable]: www.NS200.example.com/ports*

`<not_disclosed>`

Optional linked information

- List of all physical interfaces (e.g., Ethernet, USB) that the device supports
- List of all communication protocols that are being used
- Justification for having each interface and communication protocol
- What access is provided across each of the interfaces
- What safeguards are designed for each interface to prevent it from being misused
- Guidance on how users can securely setup their device
- Manufacturer Usage Description (MUD) file, describing how device normally behaves in the network
- Information on how the device's functions within the network may affect users' privacy

Best practices

- Device should support the latest versions of the industry standard or well-analyzed and peer-reviewed protocols [73, 17, 18, 13, 30, 43, 60, 25, 24, 29, 41].
- If device uses Wi-Fi connections, it should support industry accepted wireless security defaults [73].
- Protocols should not be allowed to downgrade to a less secure option [73].
- Securing or disabling developer-level ports and services prior to the product shipment [18] and limit the functionality of the system "out of the box" and instead providing options for users to enable features where they see a need and disable features they do not want to have [73].
- Unnecessary function, interfaces, and services should be disabled [18, 5, 10].
- Manufacturer should provide a file server that distributes MUD files in accordance with MUD RFC [30].
- Endpoints should only run applications or services whose TCP or UDP ports are described in the MUD profile.
- Users should be notified when the device stops complying with its MUD and manufacturer should inform users about the privacy implications related to how their device functions in the network [41].
- Make the installation and maintenance of device an easy process for users [19].
- Device should support an automated onboarding capability [30].
- Connections to remote services, interfaces, and end-points should be cryptographically authenticated [43, 29, 73].

2.5 Hardware Safety

Layer: Secondary

Mentioned by: [55, 41, 13, 43, 27, 60, 52, 30, 73, 17, 18, 15, 59]

Label example: `www.NS200.example.com/hw_safety`

Consumer explanation: Safeguards the manufacturer has in place to protect the device hardware from tampering

Values (one of the following)

`<link>` *[Open text field with the following text in grey and not editable]: www.NS200.example.com/hw_safety*

`<not_disclosed>`

Optional linked information

- Features that have been implemented to prevent unauthorized tampering with the device
- What user should look for to find out whether the device is tampered with
- How a user is informed if the device is tampered with and the event is detected

Best practices

- Device's process system should have an irrevocable hardware secure boot process [17], which should be enabled by default. If device does not support secure boot, upon a firmware update the user data and credentials should be re-initialised [41].
- Device implements a hardware-based Root of Trust (RoT) for updates and boot authentication [73, 43, 17, 18]
- Use tamper-evident measures to make end users aware if tampering occurs [13, 41].
- Developer-level ports should be secured or disabled [17].
- Unused or insecure local and remote administrative services and ports should be removed [17, 24, 41, 52] and if that can not be avoided and the device is likely to be deployed in public areas, offer a configuration option that logically disables the interfaces [52].
- For products in which local attacks are a concern, internal chip-to-chip interfaces should be secured [43].

2.6 Software Safety

Layer: Secondary

Mentioned by: [68, 73, 17, 52, 30, 24, 19, 41, 18, 1, 10, 25, 29, 34, 39, 41, 47]

Label example: `www.NS200.example.com/sw_safety`

Consumer explanation: Safeguards the manufacturer has in place to secure the software of the device

Values (one of the following)

`<link>` *[Open text field with the following text in grey and not editable]: www.NS200.example.com/sw_safety*

`<not_disclosed>`

Optional linked information

- How sensitive information that is being stored and logged in the software is being protected
- What types of risks are introduced via the libraries the binary links to, either directly or indirectly
- List of software safety features and secure toolchains against vulnerabilities and crashes, their justification, and how they are being implemented
- Security Development Lifecycle (SDL) process that includes the process the manufacturer designed to ensure the security considerations throughout the software life cycle
- The complexity of the code
- Under fuzz testing, what is the code coverage, number of crashes, and type(s) of crashes
- How vulnerable the software is to algorithmic complexity attacks

Best practices

- Critical applications stored in executable fields of memory should be stored read-only [29].
- The software is not overly complex [68].
- The software is not susceptible to crashes [68].
- If the program is forced to unexpectedly terminate, it shuts down in a secure manner [68, 13].
- Secure boot mechanism should be in place [11, 13, 24, 25, 29, 41, 60, 62, 56, 73].
- The device and mobile application store sensitive information and code (e.g., keys, in a secure, software signing root of trust) in secure and tamper-resistant memory. Upon detection of tampering of the databases or files, they are reinitialised [41].
- A software development lifecycle (SDL) should be in place [17].
- The configuration of the device and any related web services is tamper-resistant; i.e., sensitive configuration parameters should only be changeable by authorised people (evidence should list the parameters and who is authorised to change).
- Critical code and features should be separated from non-critical functions, and unwanted or unnecessary code should be removed from the software [73, 13, 24].
- System software should be tested to check for publicly disclosed and undisclosed vulnerabilities [68, 73, 17, 1].
- Error messages should be carefully designed and documented to prevent user information exposure [73].

- Any functions that allow for logging of sensitive data should be disabled by default and only be temporarily (not more than 15 minutes) enabled after authentication [73].
- Functions that allows for direct execution of scripts or commands by the system should be removed [73].
- Any customer-provided code/script, any input from outside, or output from one subsystem to another should be checked and sanitized before execution. Output data should be filtered to be in a form appropriate for its intended usage [73, 17, 60, 25, 24, 19, 41, 18].
- The software should not use unsafe libraries [68].
- Security-focused toolchains should be used to develop, compile, build, and maintain the software [17].
- Software should run with appropriate privileges, taking into account both security and functionality [19, 24, 73, 41].
- Memory/storage location used to store updates after authentication should not be user accessible or externally writable [73].
- Memory location and caches used to store sensitive data are sanitized as soon as possible after they are no longer needed [41].

2.7 Personal Safety

Layer: Secondary

Mentioned by: [68, 41, 66]

Label example: `www.NS200.example.com/user_safety`

Consumer explanation: Safeguards the manufacturer has in place to protect users against safety risks, including abuse and harassment

Values (one of the following)

`<link>` *[Open text field with the following text in grey and not editable]:* *www.NS200.example.com/user_safety*

`<not_disclosed>`

Optional linked information

- List of mechanisms to ensure that any failure of the device, either through malware, lack of power, or software flaws, does not result in safety risks
- List of safety aspects of the product that affect users if the security is compromised
- List of mechanisms that are considered in the product to protect users from abusive behavior

- Guidelines to help users protect themselves against abusive behavior
- Guidelines on how users can report incidents of abusive behavior

Best practices

- Where a product or service includes any safety critical or life-impacting functionality, the services infrastructure should incorporate protection against DDOS attacks [41].
- Where a product or service includes any safety critical or life-impacting functionality, the services infrastructure should incorporate redundancy to ensure service continuity and availability [41].
- By protecting users' identities, any previous incident of device being used for abusive behaviors should be publicly disclosed.

2.8 Vulnerability Disclosure and Management

Layer: Secondary

Mentioned by: [73, 68, 30, 17, 18, 43, 60, 25, 24, 52, 19, 41, 13, 1, 4, 10, 11, 32, 33, 38, 40, 42, 48, 59, 74, 75]

Label example: `www.NS200.example.com/vul_report`

Consumer explanation: How transparent and timely the manufacturer has been in disclosing the discovered vulnerabilities, managing them, and mitigating their potential harms

Values (one of the following)

`<link>` *[Open text field with the following text in grey and not editable]: www.NS200.example.com/vul_report*

`<not_disclosed>`

Optional linked information

- Discovered and reported vulnerabilities
- While a patch is being created, what steps users should take to mitigate the potential risks of the vulnerability
- How severe the vulnerabilities were
- When were the vulnerabilities discovered
- When were the vulnerabilities fixed
- What steps the manufacturer took to fix the vulnerabilities
- What harms did the vulnerabilities lead to

- The steps involved in approving, signing, and distributing the patch/fix
- The amount of time it takes for the manufacturer to review the reports of the vulnerabilities
- The average amount of time it takes for the manufacturer to fix a discovered vulnerability
- The standard industry average time to patch the vulnerabilities related to the specific device type
- Justification on why it will take on average a specific number of months to patch a vulnerability
- How the manufacturer notifies data subject who might be affected by a data breach

Best practices

- Device should provide mitigation operation including device shut-down in the event of a security breach [30].
- Manufacturer should have a publicly disclosed mechanism and point of contact so that researchers and others can report vulnerabilities [68, 25, 24, 52, 19, 4, 10, 11, 48].
- The manufacturer should actively monitor for new vulnerabilities in the product software, cloud, and mobile application, immediately inform users of potential vulnerabilities and report the findings and fixes [73].
- The manufacturer should have a mechanism in place to look into and fix the discovered and reported vulnerabilities in a timely manner.
- Manufacturer should have an active Product Security Incident Response Team (PSIRT) that users can easily locate and contact to report vulnerabilities [30, 41].
- The manufacturer should commit not to pursue legal actions against security researchers [68].
- The manufacturer should notify the relevant authorities without undue delay when a data breach occurs [68].
- Manufacturer should inform users of potential vulnerabilities, harms, and any mitigating steps they need to take whilst a patch is being created [73, 1, 10, 11].
- Vulnerabilities rated as CVSS 7 or higher should be patched within 1 month, vulnerabilities rated between 4 to 7 should be patched within 3 months, and those rated as less than 4 may be left unpatched [73].

2.9 Software and Hardware Composition List

Layer: Secondary

Mentioned by: [73, 60, 17, 70, 51, 15, 59]

Label example: `www.NS200.example.com/BOM`

Consumer explanation: Software and hardware components that are used in the device

Values (one of the following)

`<link>` *[Open text field with the following text in grey and not editable]: www.NS200.example.com/BOM*

`<not_disclosed>`

Optional linked information

- List of all different software and hardware components that are used and their versions
- List of vulnerabilities and patches for the software and hardware components
- For software components, the license of any 3rd part library/components used
- Where each hardware component is manufactured at
- Where each hardware component is sourced from

2.10 Encryption and Key Management

Layer: Secondary

Mentioned by: [73, 17, 13, 30, 43, 60, 25, 68, 37, 24, 52, 19, 6, 41, 18, 1, 10, 11, 15, 29, 34, 42, 44, 47, 59, 60, 62, 64, 57, 33, 35, 36, 38, 28, 39, 48, 61, 56]

Label Example: `www.NS200.example.com/encryption`

Consumer explanation: How user's data will be protected using encryption

Values (one of the following)

`<link>` *[Open text field with the following text in grey and not editable]: www.NS200.example.com/encryption*

`<not_disclosed>`

Optional linked information

- If the data stored on the device is encrypted, what encryption method(s) are used
- If the data stored on the mobile application is encrypted, what encryption method(s) are used
- If the data stored on the cloud is encrypted, what encryption method(s) are used
- If the data in transit between device and cloud is encrypted, what encryption method(s) are used
- If the data in transit between mobile application and cloud is encrypted, what encryption method(s) are used
- If no encryption is being used, an explanation as to why
- How cryptographic keys are generated, stored, and managed
- The crypto libraries that are used and their versions

Best practices

- End point devices should be enabled with cryptographically unique identities [29].
- Open, published, peer-reviewed industry standards and protocols should be used for all cryptographic functions [17, 18].
- Cryptographic authentication should be implemented.
- Keys should be generated by an industry standard random number generator with sufficient entropy [73, 6].
- Unique secret and private keys should be generated per single intended purpose [73].
- Each key should be used for a unique purpose.
- End-to-end encryption is enabled by default.
- Credentials and Crypthographic methods should be updatable to enable using new cryptographic algorithms [17, 18, 10].
- Data in transit and at rest should be encrypted, using unique keys [73, 68, 13, 25, 52, 19, 17, 60, 41, 18].
- End-to-end encryption is enabled by default [68].
- Cryptographic keys should be generated, stored, and managed by following industry best practices [73, 17, 13, 30, 43, 60, 25, 37, 27].
- Hardware Security Module (HSM), Trusted Execution Environment (TEE), or Trusted Platform Module (TPM) should be used for key storage and operation [15, 60].

3 Data Practices

3.1 Sensor Data Collection

Layer: Primary and secondary

Mentioned by: [68, 73, 55, 41, 1, 15, 59, 67]

Label example: Visual

Consumer explanation: Data types that the device sensors can collect

Values (one of the following)

`<visual>` Visual

Consumer explanation: Device can collect visual data (e.g., video, still image)

Representative icon: 🎞

`<audio>` Audio

Consumer explanation: Device can collect audio

Representative icon: 🔊

`<health>` Physiological

Consumer explanation: Device can measure information related to user's body and health status

Representative icon: ♡

`<position>` Position

Consumer explanation: Device can measure the exact location of an object or its relative position

Representative icon: 📍

`<motion>` Motion

Consumer explanation: Device can sense motion

Special note: This information will be presented on the primary layer as a value of *Other Sensor Data Collection*.

`<magnetic_field_change>` Changes to the magnetic field

Consumer explanation: Device can sense the changes to the magnetic field and find the position of an object

Special note: This information will be presented on the primary layer as a value of *Other Sensor Data Collection*.

`<proximity>` Presence

Consumer explanation: Device can detect the presence of nearby people or objects

Special note: This information will be presented on the primary layer as a value of *Other Sensor Data Collection.*

`<pressure>` Pressure
Consumer explanation: Device can sense the pressure
Special note: This information will be presented on the primary layer as a value of *Other Sensor Data Collection.*

`<tampering>` Tampering efforts
Consumer explanation: Device can detect when it is unexpectedly moved or when someone is trying to open the case to access the device's internal components
Special note: This information will be presented on the primary layer as a value of *Other Sensor Data Collection.*

`<distance>` Distance
Consumer explanation: Device can sense ultrasonic sound waves to measure the distance to an object
Special note: This information will be presented on the primary layer as a value of *Other Sensor Data Collection.*

`<level>` Liquid level
Consumer explanation: Device can sense the level of the liquid
Special note: This information will be presented on the primary layer as a value of *Other Sensor Data Collection.*

`<light>` Light
Consumer explanation: Device can detect the amount of light
Special note: This information will be presented on the primary layer as a value of *Other Sensor Data Collection.*

`<carbon_monoxide>` Carbon monoxide
Consumer explanation: Device can detect the amount of Carbon Monoxide in the air
Special note: This information will be presented on the primary layer as a value of *Other Sensor Data Collection.*

`<water>` Humidity
Consumer explanation: Device can detect the humidity to measure the amount of water in the air
Special note: This information will be presented on the primary layer as a value of *Other Sensor Data Collection.*

`<water_quality>` Water quality
Consumer explanation: Device can sense the quality of water
Special note: This information will be presented on the primary layer as a value of *Other Sensor Data Collection.*

`<smoke>` Smoke
Consumer explanation: Device can detect the presence of smoke in the air
Special note: This information will be presented on the primary layer as a value of *Other Sensor Data Collection.*

`<temperature>` Temperature

Consumer explanation: Device can measure temperature

Special note: This information will be presented on the primary layer as a value of *Other Sensor Data Collection*.

`<not_disclosed>` Not disclosed

`<other>` Other *[text box]*

Optional sub-attributes for all the values of "Sensor Data Collection", except `<not_disclosed>` (one of the following)

`<opt_in_collection>` Option to opt in

Consumer explanation: The specified data type will not be collected unless the user opts in

`<opt_out_collection>` Option to opt out

Consumer explanation: The specified data type will be collected unless the user opts out

Optional additional information

- Details of the data that is being collected
- What information users can obtain from the company and how they can request to obtain a copy of the information
- What steps users need to take to correct any false information about them
- How users can enable the controls they have for each data type
- Justification as to why no control is being offered for a sensor or a data type
- What users should expect to happen if they opt in/out
- Information on the range of the device sensors
- Enumerate all the physiological data types that are being collected (e.g. heart rate, blood glucose, activity, etc)

Best practices

- The information that is being collected by the product should be directly relevant and necessary for the service.
- If unnecessary data collection is turned off, the device should still function [68].
- By following an easy procedure, users can obtain a copy of the public-facing and private information that the manufacturer holds about them [68].
- By following an easy procedure, users can obtain their information in a structured data format [68].

- Users should be able to modify and correct the false information that is being collected about them.
- Users should be offered options to control the collection of their data, including third-party data collection, and if this is not possible for some data types, a justification should be offered [68, 15, 25].
- Users should be able to be informed of the decisions that are made because of information about them.
- There should be clear indicators as to when the sensors are active and collecting data [68].
- The manufacturer should have a system in place to monitor and limit employee access to user information [68].
- Device should only records audio/visual data in accordance with the authorization of the user [41].

3.2 Sensor Type

Layer: Primary and secondary

Mentioned by: [68, 73, 55, 41, 1, 15]

Label example: Camera sensors

Consumer explanation: Types of sensors the device has

Values (one or more of the following)

`<camera>` Camera sensors
Consumer explanation: Device is equipped with camera sensors

`<microphone>` Microphone sensors
Consumer explanation: Device is equipped with microphone sensors

`<accelerometer>` Accelerometer sensors
Consumer explanation: Device is equipped with accelerometer sensors

`<motion_sensor>` Motion sensors
Consumer explanation: Device is equipped with motion sensors

`<magnetometer>` Magnetometer sensors
Consumer explanation: Device is equipped with magnetometer sensors

`<occupancy_sensor>` Occupancy sensors
Consumer explanation: Device is equipped with occupancy sensors

`<proximity_sensor>` Proximity sensors
Consumer explanation: Device is equipped with proximity sensors

`<bluetooth>` Bluetooth sensors
Consumer explanation: Device is equipped with bluetooth sensors

`<tamper_switch>` Tamper detection sensors
Consumer explanation: Device is equipped with tamper detection sensors

`<ultrasonic>` Ultrasonic sensors
Consumer explanation: Device is equipped with ultrasonic sensors

`<ambient_light_sensor>` Ambient light sensors
Consumer explanation: Device is equipped with ambient light sensors

`<carbon_monoxide_sensor>` Carbon monoxide sensors
Consumer explanation: Device is equipped with carbon monoxide sensors

`<humidity_sensor>` Humidity sensors
Consumer explanation: Device is equipped with humidity sensors

`<photoelectric_sensor>` Photoelectric sensors
Consumer explanation: Device is equipped with photoelectric sensors

`<split_spectrum_sensor>` Split spectrum sensors
Consumer explanation: Device is equipped with split spectrum sensors

`<temperature_sensor>` Temperature sensors
Consumer explanation: Device is equipped with temperature sensors

`<capacitive_sensor>` Capacitive sensors
Consumer explanation: Device is equipped with capacitive sensors

`<optical_sensor>` Optical sensors
Consumer explanation: Device is equipped with optical sensors

`<GPS_sensor>` GPS sensors
Consumer explanation: Device is equipped with GPS sensors

`<not_disclosed>` Not disclosed

`<other>` Other *[text box]*

Optional additional information

- What types of controls users have for each sensor

3.3 Data Collection Frequency

Layer: Secondary

Mentioned by: [68]

Label example: Periodic - Adjustable

Consumer explanation: How frequently user's data is being collected when the device is turned on

Values (one or more of the following)

`<trigger_based_collection>` When event happens
Consumer explanation: Data is collected when specific events happen

`<third_party_collection_frequency>` When third parties request it
Consumer explanation: The frequency of data collection is imposed by the third parties

`<user_collection_frequency>` When user requests it
Consumer explanation: Data is collected when the user requests it

`<periodic_collection_frequency>` Periodic

`<continuous_collection_frequency>` Continuous

`<law_collection_frequency>` When required by law

`<not_disclosed>` Not disclosed

`<other>` Other *[text box]*

Optional sub-attributes for all the values of "Data Collection Frequency", except `<not_disclosed>` (one of the following)

`<adjustable_collection_frequency>` Adjustable
Consumer explanation: User can modify the frequency of data collection

Optional additional information

- Justification as to why the data is being collected with the specified frequency
- Justification as to why users cannot adjust the frequency of data collection
- Steps users can take to adjust frequency or exercise other options related to collection frequency
- If data is periodically being collected, what the exact frequency is
- How frequent third party collects data
- If data collection is trigger-based, what events activate the data collection and what controls users have about each event (e.g., disabling the data collection on specific events)

Best practices

- Use the lowest data collection frequency needed to provide the service requested by users.

3.4 Purpose

Layer: Primary and secondary

Mentioned by: [55, 68, 41, 1, 4, 15, 22, 24, 59, 67]

Label example: Providing and improving core device functionality - Option to opt in

Consumer explanation: The purpose of data collection

Values (one or more of the following)

<primary_features> Providing and improving core device functionality
Consumer explanation: Data is being collected to provide the main device features, improve services, and help develop new features
Special note: This category of purpose does not include advertisement purposes.

<personalization> Personalization
Consumer explanation: Data is being collected to provide user with personally relevant features and customized content
Special note: This category of purpose does not include advertisement purposes.

<advertising> Tailored advertising and monetization
Consumer explanation: The manufacturer receives income from sending user tailored advertisements or selling user's data to third parties

<contact_user> Contacting and updating users
Consumer explanation: Data is being collected so that manufacturer can contact user and notify user of improvements, changes, new services, security breaches, and updates
Special note: This category of purpose does not include advertisement purposes.

<security> Security and safety
Consumer explanation: Data is being collected to increase and maintain safety and prevent potentially illegal activities and misuse
Special note: This category of purpose does not include advertisement purposes.

<research> Research
Consumer explanation: Data is being collected for research purposes
Special note: This category of purpose does not include advertisement purposes.

<not_specified> Unspecified third-party use
Consumer explanation: The manufacturer is not able to specify the purpose of the collected data that will be shared with third parties
Special note: IoT companies should be able to specify the purpose of all their collected data. However, when data is going to be shared with another manufacturer, the purpose of data collection could be unspecified.

<not_disclosed> Not disclosed

<other> Other *[text box]*

Optional sub-attributes for all the values of "Purpose", except `<not_disclosed>` and `<not_specified>` (one of the following)

`<opt_in_purpose>` Option to opt in
Consumer explanation: The data will not be used for the specified purpose unless the user opts in

`<opt_out_purpose>` Option to opt out
Consumer explanation: The data will be used for the specified purpose unless the user opts out

Optional additional information

- If an option is being offered to control the purpose of data collection, what steps users need to take to enable those options
- Whether the manufacturer itself uses the data for the specified purpose or sends data to a third party to satisfy the specified purpose
- What users should expect to happen if they opt in/out
- Information on how the collected data will be used to satisfy the specified purpose of data collection
- Who should be contacted to get more information on what types of research projects will be conducted with the data

Best practices

- The minimum information elements that are relevant and necessary to accomplish the purpose of collection should be identified and data should not be used for purposes other than the ones specified in the policy [59, 61].
- Users should be offered options to opt-out from the purpose of data collection and if this is not feasible for all the purposes, they should be offered with a justification as to why.
- If a specific purpose for data collection is no longer needed, the data collection should be stopped.
- There should be a clear purpose for all the collected and shared data. If not, the data should not be collected [15].
- Users should have control on whether and how their information is used for targeted advertisement [68].
- Tailored advertising should be disabled by default [68].
- If any purpose other than providing device functionality, users should be provided with an option to opt-in [59, 61].

3.5 Data Stored on the Device

Layer: Primary and secondary

Mentioned by: [73, 41, 25, 42, 48, 61]

Label example: Identifiable - Option to delete

Consumer explanation: Whether user's identity could be revealed by the data stored on the device

Values (one of the following)

`<identifiable_local_storage>` Identifiable
Consumer explanation: User's identity could be revealed from the data stored on the device

`<de_identified_local_storage>` De-identified
Consumer explanation: The data stored on the device does not contain any personal identifiers that reveal a user's identity

`<pseudo_local_storage>` Pseudonymized
Consumer explanation: The identifiers in the data stored on the device are replaced with pseudonyms, which are held separately from the data subject to technical safeguards

`<no_local_storage>` No device storage
Consumer explanation: The collected data will not be stored on the device

`<not_disclosed>` Not disclosed

`<other>` Other *[text box]*

Optional sub-attributes for all the values of "Data Stored on the Device", except `<not_disclosed>` and `<no_local_storage>` (one or more of the following)

`<opt_in_local_storage>` Option to opt in
Consumer explanation: The data will not be stored on the device unless the user opts in to device storage

`<opt_out_local_storage>` Option to opt out
Consumer explanation: The data will be stored on the device unless the user opts out of the device storage

`<delete_local_storage>` Option to delete
Consumer explanation: User can delete the data that is being stored on the device

`<access_local_storage>` Data subject access request
Consumer explanation: User can request to download the data that is being stored on the device

Optional additional information

- Justification as to why this level of detail is needed
- Information related to how the stored information would be identifiable
- List of personal information that could be revealed by the identifiable data
- Information related to how data will be de-anonymized
- Information related to how data will be aggregated
- If users are offered an option to delete their data, what steps they need to take to delete their data
- If users are offered an option to delete their data, how long after the request data will get deleted
- What users should expect to happen if they delete their data or opt in/out from data storage

Best practices

- If the purpose of data collection could be satisfied by less detailed data, the granularity should be changed.
- Users' identifiable data should be de-identified or anonymized [73, 57, 44].
- The product/service should store the minimum amount of personal information from users required for the operation of the device [41].
- Users should be able to review their identifiable data [73].
- Users should be able to opt-in/out for their identifiable data to be stored [73].
- Users should be offered an option to request their identifiable data to be deleted [68, 73].
- The manufacturer should delete the outdated and unnecessary personal information or make sure it is retained in a de-identified format [68].
- User information should be deleted as soon as the user's service is terminated or the service no longer operates [68, 41].
- Data should be deleted as soon as the data required for processing is extracted [25].
- user should be able to delete their stored data that is not essential to the device's operation within a defined period established by the IoT manufacturer [17].
- There should be specific reasons to justify the identifiable data being collected and stored [57].
- Users should be able to track what personal information is being deleted [41].

- The device manufacturer should perform a privacy impact assessment (PIA) to identify Personally Identifiable Information (PII) [41].
- The device manufacturer should make sure that the identifiers used for the device and the communications are independent of the users[41, 58].

3.6 Local Data Retention Time

Layer: Secondary

Mentioned by: [68, 73, 41, 57, 48, 59, 61]

Label example: Up to a month - Adjustable

Consumer explanation: For how long data will be stored on the device

Value (one of the following)

`<five_minutes_local_storage>` Less than five minutes
Consumer explanation: User's data will be retained on the device up to five minutes and after that it will get deleted

`<day_local_storage>` Up to a day
Consumer explanation: User's data will be retained on the device up to one day and after that it will get deleted

`<week_local_storage>` Up to a week
Consumer explanation: User's data will be retained on the device up to one week and after that it will get deleted

`<month_local_storage>` Up to a month
Consumer explanation: User's data will be retained on the device up to one month and after that it will get deleted

`<year_local_storage>` Up to a year
Consumer explanation: User's data will be retained on the device up to one year and after that it will get deleted

`<10_years_local_storage>` Up to 10 years
Consumer explanation:] User's data will be retained on the device up to 10 years and after that it will get deleted

`<forever_local_storage>` Forever
Consumer explanation: User's data may be retained on the device indefinitely

`<no_retention_local_storage>` No retention
Consumer explanation: User's data will not be retained on the device

`<not_disclosed>` Not disclosed

`<other>` Other *[text box]*

Optional sub-attributes for all the values of "Local Data Retention Time", except <not_disclosed> and <no_retention_local_storage> (one of the following)

<adjustable_local_retention> Adjustable
Consumer explanation: User can change the duration for which their data will be retained on the device

Optional additional information

- The exact retention time
- Justification as to why data needs to be retained for the specified duration

Best practices

- Data should not be kept longer that is necessary for a explicitly mentioned purpose [57].

3.7 Data Stored in the Cloud

Layer: Primary and secondary

Mentioned by: [41, 10, 57, 25, 42, 44, 48, 16, 61, 73]

Label example: Identifiable - Option to delete

Consumer explanation: Whether user's identity could be revealed by the data stored in the cloud

Values (one of the following)

<identifiable_cloud_storage> Identifiable
Consumer explanation: User's identity could be revealed from the data stored in the cloud

<de_identified_cloud_storage> De-identified Consumer explanation: The data stored in the cloud does not contain any personal identifiers that reveal a user's identity

<pseudo_cloud_storage> Pseudonymized
Consumer explanation: The identifiers in the data stored in the cloud are replaced with pseudonyms, which are held separately from the data subject to technical safeguards

<no_cloud_storage> No cloud storage
Consumer explanation: The collected data will not be stored in the cloud

<not_disclosed> Not disclosed

<other> Other *[text box]*

Optional sub-attributes for all the values of "Data Stored in the Cloud", except `<not_disclosed>` and `<no_cloud_storage>` (one or more of the following)

`<opt_in_cloud_storage>` Option to opt in
Consumer explanation: The data will not be stored in the cloud unless user opts in to cloud storage

`<opt_out_cloud_storage>` Option to opt out
Consumer explanation: The data will be stored in the cloud unless user opts out of the cloud storage

`<delete_cloud_storage>` Option to delete
Consumer explanation: User can delete the data that is being stored in the cloud

`<access_cloud_storage>` Data subject access request
Consumer explanation: User can request to download the data that is being stored in the cloud

Optional additional information

- Justification as to why this level of detail is needed
- Information related to how the stored information would be identifiable
- List of personal information that could be revealed by the identifiable data
- Information related to how data was de-anonymized
- Information related to how data was aggregated
- If users are offered an option to delete their data, what steps they need to take to delete their data
- If users are offered an option to delete their data, how long after the request data will get deleted
- What users should expect to happen if they delete their data or opt in/out from data storage

Best practices

- If the purpose of data collection could be satisfied by less detailed data, the granularity should be changed.
- The product/service should store the minimum amount of personal information from users required for the operation of the device [41].
- Users should be able to review their identifiable data [73].
- Users should be able to opt in/out for their identifiable data to be stored [73].
- There should be specific reasons to justify the identifiable data being collected and stored [57].

- Users' identifiable data should be de-identified or anonymized [73, 57, 44].
- The cloud service should meet industry standard cloud security principles, such as NIST Cyber Security Framework [53] or UK Government Cloud Security Principles [50].
- Users should be offered an option to request their identifiable data to be deleted [68, 73].
- The manufacturer should delete the outdated and unnecessary personal information or make sure it is retained in a de-identified format [68].
- User information should be deleted as soon as the user's service is terminated or the service no longer operates [68, 41].
- user should be able to delete their stored data that is not essential to the device's operation within a defined period established by the IoT manufacturer [17].
- Data should be deleted as soon as the data required for processing is extracted [25].
- Users should be able to track what personal information is being deleted [41].
- The device manufacturer should perform a privacy impact assessment (PIA) to identify Personally Identifiable Information (PII) [41].
- The device manufacturer should make sure that the identity of the device is independent of the users[41].
- The physical location where the data is being stored and process should be complied with the regulations [16].

3.8 Cloud Data Retention Time

Layer: Secondary

Mentioned by: [41, 57, 48, 59, 61]

Label example: Up to a month

Consumer explanation: For how long data will be stored in the cloud

Value (one of the following)

`<five_minutes_cloud_storage>` Less than five minutes
Consumer explanation: User's data will be retained in the cloud up to five minutes and after that it will get deleted

`<day_cloud_storage>` Up to a day
Consumer explanation: User's data will be retained in the cloud up to one day and after that it will get deleted

`<week_cloud_storage>` Up to a week
Consumer explanation: User's data will be retained in the cloud up to one week and after that it will get deleted

<month_cloud_storage> Up to a month

Consumer explanation: User's data will be retained in the cloud up to one month and after that it will get deleted

<year_cloud_storage> Up to a year

Consumer explanation: User's data will be retained in the cloud up to one year and after that it will get deleted

<10_years_cloud_storage> Up to 10 years

Consumer explanation:] User's data will be retained in the cloud up to 10 years and after that it will get deleted

<forever_cloud_storage> Forever

Consumer explanation: User's data may be retained in the cloud indefinitely

<no_retention_cloud_storage> No retention

Consumer explanation: User's data will not be retained in the cloud

<not_disclosed> Not disclosed

<other> Other *[text box]*

Optional sub-attributes for all the values of "Cloud Data Retention Time", except <not_disclosed> and <no_retention_cloud_storage> (one or more of the following)

<adjustable_cloud_retention> Adjustable

Consumer explanation:] User can change the duration for which their data will be retained in the cloud

Optional additional information

- Who is managing the cloud
- Justification as to why data needs to be retained for the specified duration
- What country the data center is located in

Best practices

- Data should not be kept longer that is necessary for a explicitly mentioned purpose [57].

3.9 Data Shared with

Layer: Primary and secondary

Mentioned by: [68, 41, 1, 15, 22, 24, 25, 29, 23, 28, 48, 59, 67, 73]

Label example: Manufacturer

Consumer explanation: Who user's data will be shared with

Values (one or more of the following)

`<manufacturer_sharing>` Manufacturer

`<third_party_sharing>` Third parties

`<gov_sharing>` Government and legal authorities

`<service_sharing>` Service providers

`<emergency_sharing>` Emergency services

`<public_sharing>` Public

`<not_shared_sharing>` Not shared

`<not_disclosed>` Not disclosed

`<other>` Other *[text box]*

Optional sub-attributes for all the values of "Data Shared with", except `<not_disclosed>` and `<not_shared>` (one of the following)

`<opt_in_sharing>` Option to opt in
Consumer explanation: The data will not be shared unless the user opts in

`<opt_out_sharing>` Option to opt out
Consumer explanation: The data will be shared unless the user opts out

Optional additional information

- The name of the third-parties the data is being shared with
- The privacy policy of the third-parties the data is being shared with
- Number and types of requests manufacturer receives from private third-parties and government authorities to access user data and how many of them manufacturer complies with
- If data is being shared with the manufacturer, who within the company has access to the user's data and why
- In what cases, manufacturer is prohibited by law from disclosing the requests for user information
- What users should expect to happen if they opt in/out
- If data is being shared with service providers, who those service providers and their privacy policies are
- If data is being shared with emergency services, who those emergency services and their privacy policies are

Best practices

- If the data is being shared with a third party for processing, the manufacturer should ensure that the third party implements the required technical and organizational measure to protect user data [68, 59].
- Manufacturer should notify users when third-party or government entities request their user information [68].
- If data is being shared with the manufacturer, only authorized personnel should have access to user's data [41].
- Users should be able to specify what information is being shared to which parties [29].

3.10 Data Sharing Frequency

Layer: Secondary

Mentioned by: [68, 25]

Label example: Continuous - Adjustable

Consumer explanation: How frequent user's data is being shared

Values (one or more of the following)

`<trigger_based_sharing>` When an event happens
Consumer explanation: Data is shared when specific events happen

`<third_party_sharing_frequency>` When third parties request it
Consumer explanation: The frequency of data sharing is imposed by the third parties

`<user_sharing_frequency>` When user requests it
Consumer explanation: Data is shared when the user requests it

`<periodic_sharing_frequency>` Periodic

`<continuous_sharing_frequency>` Continuous

`<law_sharing_frequency>` When required by law

`<not_shared_sharing_frequency>` Not shared

`<not_disclosed>` Not disclosed

`<other>` Other *[text box]*

Optional sub-attributes for all the values of "Data Sharing Frequency", except `<not_disclosed>` and `<not_shared_sharing_frequency>` (one of the following)

`<adjustable_sharing_frequency>` Adjustable
Consumer explanation: User can modify the frequency of data sharing

Optional additional information

- If user activation is required for data sharing to happen, how users can activate/deactivate their device
- Justification as to why the data is being shared with the specified frequency
- If data is periodically being shared, what the exact frequency is
- What steps users need to take to adjust the frequency of the shared data
- Justification as to why users cannot adjust the frequency of data sharing
- Explanation on the manufacturer's process for sharing or not sharing user information
- If data sharing is trigger-based, what events activate the data sharing and what controls users have about each event (e.g., disabling the data sharing on specific events)

Best practices

- Users should be offered with options to control the frequency of data sharing [25].
- Lower the data sharing frequency if the service could be provided by sharing information with lower frequency.
- The manufacturer complies only with legal and ethical third-party requests for user information.

3.11 Data Sold to

Layer: Primary and secondary

Mentioned by: [59]

Label example: Third parties - Option to opt out

Consumer explanation: Who user's data will be sold to

Values (one of the following)

`<third_party_selling>` Third parties

`<not_sold>` Not sold

`<not_disclosed>` Not disclosed

Optional sub-attributes for all the values of "Data Sold to", except `<not_disclosed>` and `<not_sold>` (one of the following)

`<opt_in_selling>` Option to opt in
Consumer explanation: The data will not be sold unless user opts in

`<opt_out_selling>` Option to opt out
Consumer explanation: The data will be sold unless user opts out

Optional additional information

- The name of the third-parties the data is being sold to
- The privacy policy of the third-parties the data is being sold to
- What users should expect to happen if they opt in/out

Best practices

- Users should be able to opt in whether they would like their identifiable data to be sold to third parties.

3.12 Other Collected Data

Layer: Primary and secondary

Label example: Device usage info

Consumer explanation: Data being collected through means other than device sensors

Values (one or more of the following)

<contact_info> Contact info
Consumer explanation: User's contact information is collected

<account_info> Account info
Consumer explanation: User's account information is collected

<payment_info> Payment info
Consumer explanation: User's payment information is collected

<device_info> Device setup info
Consumer explanation: Device's setup information is collected

<tech_info> Device tech info
Consumer explanation: Technical information related to the device is collected

<usage_info> Device usage info
Consumer explanation: Device's usage information is collected

<unique_id> Device unique identifiers
Consumer explanation: Device's unique identifiers (e.g., MAC address) are collected

<not_disclosed> Not disclosed

<other> Other *[text box]*

Optional additional information

- The purpose of each collected data type
- What choices users have for each collected data type
- Who each collected data type is shared with
- Who each collected data type is sold to
- For how long each collected data type will be retained on the device
- For how long each collected data type will be retained on the cloud
- With what level of detail (granularity) each collected data type will be stored on the device
- With what level of detail (granularity) each collected data type will be stored on the cloud
- With what frequency each collected data type is being collected
- With what frequency each collected data type is being shared

3.13 Special Data Handling Practices for Children

Layer: Secondary

Mentioned by: [59]

Label example: Yes

Consumer explanation: Whether the manufacturer has specific safeguards to handle data from children

Values (one of the following)

`<special_handling>` Yes
Consumer explanation: The manufacturer has specific safeguards to handle data from children

`<no_special_handling>` No
Consumer explanation: The manufacturer has no unique safeguard to handle data from children

`<not_disclosed>` Not disclosed

Optional additional information

- What types of safeguards are in place to protect children's data
- Justification as to why safeguards are needed or not needed to protect children's data
- Information on the exact age threshold the safeguards apply to

Best practices

- If children under the age of 16 can interact with the device, manufacturer should have safeguards in place to protect their data.

3.14 Data Linkage

Layer: Secondary

Mentioned by: [28]

Label example: Data may be linked with internal and external data sources

Consumer explanation: Other sources of information the collected data will be linked with

Values (One of the following)

`<internal_linkage>` Data may be linked with internal data sources
Consumer explanation: Data may be linked with information collected from the manufacturer

`<external_linkage>` Data may be linked with external data sources
Consumer explanation: Data may be linked with sources of information external to the manufacturer

`<internal_external_linkage>` Data may be linked with internal and external data sources
Consumer explanation: Data may be linked sources of information from the manufacturer as well as sources of information external to the manufacturer

`<no_linkage>` Data is not being linked with any sources of information

`<not_disclosed>` Not disclosed

Optional sub-attributes for all the values of "Data Linkage", except `<not_disclosed>` and `<no_linkage>` (one of the following)

`<opt_in_linkage>` Option to opt in
Consumer explanation: The data will not be linked with the specified data sources unless the user opts in

`<opt_out_linkage>` Option to opt out
Consumer explanation: The data will be linked with the specified data sources unless the user opts out

Optional additional information

- If data is being linked with data sources, internal or external, what those sources are, where they are, and who is protecting those data sources

- Privacy policy of the providers of external sources

- Justification as to why data is being linked with other data sources
- What personal information would potentially get revealed by data linkage
- Whether the manufacturer has safeguards against linkage attacks and what those safeguards are
- What users should expect to happen if they opt in/out

Best practices

- User's permission is required to link their personal information with other data sources.

3.15 In Compliance with

Layer: Secondary

Mentioned by: [41, 59]

Label example: GDPR, ISO27001

Consumer explanation: Privacy and security laws and standards the manufacturer is complying with

Values (one of the following)

`<compliance>` *[Open text field with the following text in grey and not editable]:* *GDPR*

`<not_disclosed>` Not disclosed

Optional additional information

- Link to the specified laws and standards
- Justification as to in what way(s) the manufacturer is complying with each specific law or standard

Best practices

- The product/service should be made compliant with the local and/or regional personal information protection legislation where the product is to be sold [41].

3.16 What Will be Inferred from User's Data

Layer: Secondary

Mentioned by: [7]

Label example: Preferences, Characteristics, Psychological trends

Consumer explanation: In addition to the information that is directly being collected by the device and/or the mobile application, what additional information about user will be inferred

Values (one or more of the following)

`<preferences>` Attitudes and preferences

`<characteristics>` Characteristics and psychological traits

`<aptitudes>` Aptitudes and abilities

`<behaviors>` Behaviors

`<no_inference>` No data inference
Consumer explanation: No additional information about user will be inferred from the collected data

`<not_disclosed>` Not disclosed

`<other>` Other *[text box]*

Optional additional information

- What inferences will be made with the data
- What underlying sensors are used for those inferences

3.17 Privacy Policy

Layer: Secondary

Mentioned by: [68, 73, 41, 19, 17, 10, 13, 29, 48]

Label example: www.NS200.example.com/policy

Consumer explanation: Detailed privacy and security practices

Values (one of the following)

`<link>` *[Open text field with the following text in grey and not editable]:*
www.NS200.example.com/policy

`<not_disclosed>` Not disclosed

Optional linked information

Details for privacy practices and security mechanisms that were not included on the label

Explanation on what types of user activities are not allowed

Explanation on in what circumstances user accounts could be restricted or closed

Explanation on the mechanism to identify the users violating the rules

Explanation on what rules the manufacturer has and how the manufacturer enforces its rules

Number of user accounts manufacturer has closed or restricted on its own initiative and reasons as to why

Number of user accounts manufacturer has closed or restricted as a result of a government request and reasons as to why

Number of user accounts manufacturer has closed or restricted as a result of a request from private third-parties and reasons as to why

Manufacturer's policy toward human rights, including freedom of expression and privacy

How users will be notified of any changes in the privacy policy and terms of service

How long it will take from the notification of any changes to when the changes come into effect

History of the changes to the privacy policy

How users can decommission the device in different scenarios, including sale, abandonment, or recycling

What steps users should take to maintain the privacy and security of the device/service

Best practices

- The manufacturer should not prohibit use of the product with other, complementary, products [68].
- The manufacturer should not retain any control or ownership over the operation, use, inputs, or outputs of the product after it has been purchased by the consumer [68].
- The manufacturer should not restrict the transfer of ownership when the consumer sells the product on the privacy market [68].
- The manufacturer should notify users when it restricts or closes user accounts [68].
- The manufacturer should publicly commit to respect users' human rights, freedom of expression and privacy [68].
- The manufacturer should have a whistleblower program in place that employees, staff, and volunteers can report their concerns related to how manufacturer treats its users' freedom of expression and privacy [68].
- The manufacturer should have a process to review complaints, including complaints related to freedom of expression and privacy [68].
- The manufacturer's board of directors should oversight over how manufacturer's practices affect freedom of expression and privacy [68].
- The manufacturer should have a mechanism in place to implement its commitments to freedom of expression and privacy and continuously assess free expression and privacy risks associate with new product features and services [68].

- The manufacturer should engage with a range of stakeholders on freedom of expression and privacy issues [68]

- The privacy policies are presented in an understandable manner and written in the language(s) most commonly spoken by the manufacturer's users [68].

- The manufacturer should notify when it changes its privacy policies and terms of service [68, 73].

- A cryptographic protected ownership proof should be transferred along the supply chain and extended if a new owner is added in the chain [41].

- When a device's ownership is transferred to a different owner, all the previous owner's personal information should be removed from the device and registered service(s) [41].

- In case of ownership change, the device should have an irrevocable method of decommissioning and recommissioning [41].

- The manufacturer should ensure that the identity of the device is independent of the end user, in order to ensure anonymity [41].

- The summary of policy changes and their impact should be available for a minimum of two years [59].

4 More Information [1]

4.1 Call *Manufacturer* with Your Questions at

Layer: Secondary

Label example: 412-313-2793

Consumer explanation: Manufacturer's phone number

Values (one of the following)

`<phone>` *[Open text field with the following text in grey and not editable]:*
Number to contact

`<not_disclosed>` Not disclosed

Optional additional information

- Other ways to contact the manufacturer

- List of frequently asked questions

- Items users can contact the manufacturer to get help for

- The availability of the manufacturer to answer users' questions (e.g., 24/7 support)

[1] On the primary layer, the link and the QR code to the secondary layer is provided as "More Information"

4.2 Email *Manufacturer* with Your Questions at

Layer: Secondary

Label example: info@casa.com

Consumer explanation: Manufacturer's email address

Values (one of the following)

`<email>` *[Open text field with the following text in grey and not editable]:*
Email to contact

`<not_disclosed>` Not disclosed

Optional additional information

- Other ways to contact the manufacturer
- List of frequently asked questions
- Items users can contact the manufacturer to get help for
- The availability of the manufacturer to answer users' questions (e.g., 24/7 support)

4.3 Functionality when Offline

Layer: Secondary

Mentioned by: [73, 24, 19, 17, 41]

Label example: Limited functionality

Consumer explanation : How the device is expected to function when no internet is available

Values (one of the following)

`<full_offline>` Full functionality
Consumer explanation: Device will remain functional when no internet is available

`<limited_offline>` Limited functionality
Consumer explanation: Device will remain partially functional when no internet is available

`<none_functional_offline>` No functionality
Consumer explanation: Device will not remain functional when no internet is available

`<not_disclosed>` Not disclosed

Optional additional information

- What functionalities should user expect the device to have when no internet is available
- What safety-related consequences users should be aware of when no internet is available

Best practices

- Manual backup/override should be provided for safety-related services in case of power and internet outage [73, 24, 19, 17].
- Device should remain operating and locally functional in the case of a lost network connection [41, 73, 24, 19, 17].

4.4 Functionality with No Data Processing

Layer: Secondary

Label example: Limited functionality

Consumer explanation: How the device is expected to function when data is not being processed

Values (one of the following)

`<full_data_processing>` Full functionality
Consumer explanation: Device will remain functional when data is not being processed

`<limited_data_processing>` Limited functionality
Consumer explanation: Device will remain partially functional when data is not being processed

`<none_functional_data_processing>` No functionality
Consumer explanation: Device will not remain functional when data is not being processed

`<not_applicable_data_processing>` Not applicable
Consumer explanation: Device will not process any data

`<not_disclosed>` Not disclosed

Optional additional information

- What types of data processing is expected to happen and reasons as to why data needs to be processed
- If data is not being processed, reasons as to why
- What functionalities should user expect the device to have when data is not being processed

- What safety-related consequences users should be aware of when data is not being processed
- Whether and how user can activate the no data processing mode
- Reasons as to why the no data processing mode should be or should not be activated

4.5 Physical Actuations and Triggers

Layer: Secondary

Label example: Device blinks when motion is detected

Consumer explanation: How the device is expected to behave in response to triggers

Values (one of the following)

`<triggers>` *[Open text field with the following text in grey and not editable]:*
Device blinks when motion is detected

`<not_disclosed>` Not disclosed

Optional additional information

- Safety concerns users should be aware of related to how device responses to various triggers

4.6 Compatible Platforms

Layer: Secondary

Label example: Amazon Alexa

Consumer explanation: List of platforms the device can work with

Values (one of the following)

`<compatibility>` *[Open text field with the following text in grey and not editable]:*
Amazon Alexa

`<not_disclosed>` Not disclosed

Optional additional information

- Link to the privacy policy of the compatible platforms
- Safety concerns users should be aware of related to devices being connected to each other

5 Summary of Changes

Changes applied to 5/27/2020 version of the document

- Revising the specification document to be consistent with the taxonomy of the label

Changes applied to 1/17/2021 version of the document

- Adding the licensing information to the specification and the example labels.

References

[1] Alliance for Internet of Things Innovation. Report on workshop on security and privacy in the hyper-connected world. https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf.

[2] Orlando Arias, Jacob Wurm, Khoa Hoang, and Yier Jin. Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems*, 1(2):99–109, 2015.

[3] Aspen Institute. Aspen cybersecurity group internet of things (iot) security first principles. https://assets.aspeninstitute.org/content/uploads/2018/11/Aspen-Cybersecurity-Group-IoT-Security-First-Principles.pdf?_ga=2.43245153.559795698.1578954276-1312256215.1578954276.

[4] Atlantic Council Scowcroft Center for Strategy and Security. Smart homes and the internet of things. https://www.atlanticcouncil.org/wp-content/uploads/2016/03/Smart_Homes_0317_web.pdf.

[5] AT&T. The ceo's guide to securing the internet of things. https://www.business.att.com/content/dam/attbusiness/reports/exploringiotsecurity.pdf.

[6] Elaine Barker and John Kelsey. Recommendation for random number generation using deterministic random bit generators. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf.

[7] Xavier Becerra. AB-375 privacy: personal information: businesses. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[8] J. M. Blythe and S. D. Johnson. The consumer security index for iot: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in iot devices. In *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, pages 1–7, 2018.

[9] John M Blythe, Nissy Sombatruang, and Shane D Johnson. What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? *Journal of Cybersecurity*, 5(1), 06 2019. tyz005.

[10] Broadband Internet Technical Advisory Group. Interne of things (iot) security and privacy recommendations. http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf.

[11] CableLabs. A vision for secure iot. https://www.cablelabs.com/insights/vision-secure-iot.

[12] Jen Caltrider. 10 fascinating things we learned when we asked the world "how connected are you?". https://goo.gl/92JDfq, November 2017.

[13] Cellular Telecommunications Industry Association. CTIA cybersecurity certification test plan for IoT devices. https://theinternetofthings.report/Resources/Whitepapers/853a8ac3-06c6-4975-9287-cb2403fa7617_CTIA-IoT-Test-Plan-V1_0.pdf.

[14] Centre for International Governance Innovation & IPSOS. 2016 CIGI-IPSOS global survey on internet security and trust. https://www.cigionline.org/internet-survey-2016, 2016.

[15] Cloud Security Alliance. Security guidance for early adopters of the internet of things (iot). https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf.

[16] Cloud Standards Customer Council. Cloud customer architecture for iot. https://www.omg.org/cloud/deliverables/CSCC-Cloud-Customer-Architecture-for-IoT.pdf.

[17] Council to Secure the Digital Economy. The C2 consensus on IoT device security baseline capabilities. https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf.

[18] Council to Secure the Digital Economy. International anti-botnet guide. https://securingdigitaleconomy.org/wp-content/uploads/2018/11/CSDE-Anti-Botnet-Report-final.pdf.

[19] Department for Digital, Culture, Media and Sport. Code of practice for consumer IoT security. https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security.

[20] P. Emami-Naeini, Y. Agarwal, L. Cranor, and H. Hibshi. Ask the experts: What should be on an iot privacy and security label? In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 771–788, Los Alamitos, CA, USA, may 2020. IEEE Computer Society.

[21] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, page 534. ACM, 2019.

[22] European Commission. Report on workshop on security & privacy in iot. https://ec.europa.eu/information_society/newsroom/image/document/2017-15/final_report_20170113_v0_1_clean_778231E0-BC8E-B21F-18089F746A650D4D_44113.pdf.

[23] European Research Cluster on the Internet of Things. Internet of things. http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf.

[24] European Telecommunications Standards Institute. Cyber security for consumer internet of things. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.00.00_20/en_303645v020000a.pdf.

[25] European Union Agency for Cybersecurity. Baseline security recommendations for IoT. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

[26] European Union Agency for Network and Information Security. Security and resilience of smart home environments. https://www.enisa.europa.eu/publications/security-resilience-good-practices.

[27] Federal Information Processing Standards. Security requirements for cryptographic modules. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.

[28] Oscar Garcia-Morchon, Sandeep Kumar, and Mohit Sethi. Internet of things (iot) security: State of the art and challenges. https://www.rfc-editor.org/rfc/pdfrfc/rfc8576.txt.pdf.

[29] Global System for Mobile Communications Association. GSMA IoT security guidelines for endpoint ecosystems. https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.13-v1.0.pdf.

[30] GlobalPlatform. Security Evaluation Standard for IoT Platforms. https://globalplatform.org/wp-content/uploads/2019/11/SESIP_GP-0_0_0_5a.pdf.

[31] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva. Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, 17(3):1294–1312, 2015.

[32] I Am The Cavalry Hippocratic Oath for Connected Medical Devices. I am the cavalry. https://www.iamthecavalry.org/wp-content/uploads/2016/01/I-Am-The-Cavalry-Hippocratic-Oath-for-Connected-Medical-Devices.pdf.

[33] IEEE Internet Technology Policy Community. Internet of things (iot) security best practices. https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf.

[34] Industrial Internet Consortium. Industrial internet of things volume G4: Security framework. https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf.

[35] Intel. Policy framework for the internet of things (iot). https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/policy-iot-framework.pdf.

[36] International Electrotechnical Commission. Iot 2020: Smart and secure iot platform. http://www.iec.ch/whitepaper/pdf/iecWP-loT2020-LR.pdf.

[37] International Organization for Standardization. Banking — key management (retail) — part 1: Principles. https://www.iso.org/standard/34937.html.

[38] Internet Engineering Task Force. Best current practices for securing internet of things (iot) devices. https://tools.ietf.org/html/draft-moore-iot-security-bcp-01.

[39] Internet Society. The internet of things an internet society public policy briefing. https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-IoT.pdf.

[40] IoT Acceleration Consortium. Iot security guidelines ver. 1.0. http://www.iotac.jp/wp-content/uploads/2016/01/IoT-Security-Guidelines_ver.1.0.pdf.

[41] IoT Security Foundation. IoT security compliance framework. https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf.

[42] IoT Security Initiative. Security design best practices. https://www.iotsi.org/security-best-practices.

[43] ioXt. The ioXt security pledge. https://static1.squarespace.com/static/5c6dbac1f8135a29c7fbb621/t/5ca695ffee6eb0769f5608d1/1554421249364/ioXt-SecurityPledge-booklet-final.pdf.

[44] Korea Internet & Security Agency. We will be a your partner in the internet & security field. https://www.kisa.or.kr/eng/main.jsp.

[45] Veronica Lara. What the Internet of Things means for consumer privacy. https://perspectives.eiu.com/technology-innovation/what-internet-things-means-consumer-privacy-0/white-paper/what-internet-things-means-consumer-privacy, March 2018.

[46] Hosub Lee and Alfred Kobsa. Privacy preference modeling and prediction in a simulated campuswide IoT environment. In *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 276–285. IEEE, 2017.

[47] Microsoft. Security best practices for internet of things (iot). https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices.

[48] Mozilla. Minimum standards for tackling iot security. https://medium.com/read-write-participate/minimum-standards-for-tackling-iot-security-70f90b37f2d5.

[49] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an IoT world. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 399–412, 2017.

[50] National Cybersecurity Institute. Cloud security guidance. https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles.

[51] National Institute of Standards and Technology. Considerations for a core iot cybersecurity capabilities baseline. https://www.nist.gov/system/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf.

[52] National Institute of Standards and Technology. Core cybersecurity feature baseline for securable IoT devices: A starting point for iot device manufacturers. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8259-draft.pdf.

[53] National Institute of Standards and Technology. NIST cybersecurity framework. https://www.nist.gov/cyberframework.

[54] National Institute of Standards and Technology. NIST special publication 800-63b digital identity guidelines authentication and lifecycle management. https://pages.nist.gov/800-63-3/sp800-63b.html.

[55] National Institute of Standards and Technology. Security and privacy controls for federal information systems and organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[56] NortonLifeLock. An internet of things reference architecture. https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices.

[57] NYC Department of Information Technology & Telecommunications. Security. https://iot.cityofnewyork.us/security/.

[58] oneM2M. onem2m technical report. http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf.

[59] Online Trust Alliance. Ota iot trust framework. https://www.internetsociety.org/iot/trust-framework/.

[60] Open Connectivity Foundation. OCF security specification. https://openconnectivity.org/specs/OCF_Security_Specification_v2.0.1.pdf.

[61] Open Web Application Security Project. Iot security guidance. https://www.owasp.org/index.php/IoT_Security_Guidance.

[62] PSA Certified. Psa certified level 1 questionnaire. https://www.psacertified.org/app/uploads/2019/02/JSADEN001-PSA_Certified_Level_1-1.0Web.pdf.

[63] Elena Reshetova and Michael McCool. The internet of things an internet society public policy briefing. https://www.w3.org/TR/wot-security/#recommended-security-practices.

[64] Elena Reshetova and Michael McCool. Web of things (wot) security best practices. https://w3c.github.io/wot-security-best-practices/.

[65] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. Security, privacy and trust in internet of things: The road ahead. *Computer networks*, 76:146–164, 2015.

[66] Leonie Tanczer, Isabel Lopez Neira, Simon Parkin, Trupti Patel, and George Danezis. Gender and IoT research report. https://www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.pdf.

[67] Telecommunications Industry Association. Realizing the potential of the internet of things: Recommendations to policy makers. https://www.tiaonline.org/wp-content/uploads/2018/05/Realizing_the_Potential_of_the_Internet_of_Things_-_Recommendations_to_Policymakers.pdf.

[68] The Digital Standard. The standard. https://www.thedigitalstandard.org/the-standard.

[69] The National Telecommunications and Information Administration. Communicating iot device security update capability to improve transparency for consumers. https://www.ntia.doc.gov/files/ntia/publications/communicating_iot_security_update_capability_for_consumers_-_jul_2017.pdf.

[70] The National Telecommunications and Information Administration. Framing software component transparency: Establishing a common software bill of material (SBOM). https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf.

[71] Christian Thorun, Max Vetter, Lucia Reisch, and Anne Karina Zimmer. Indicators of consumer protection and empowerment in the digital world. https://www.vzbv.de/sites/default/files/downloads/2017/03/13/conpolicy_executive_summary.pdf, March 2017.

[72] Tietoturva. Prerequisites for obtaining the security badge. https://tietoturvamerkki.fi/fi/vaatimukset/.

[73] Underwriters Laboratories. Identity management & security. https://ims.ul.com/IoT-security-rating.

[74] U.S. Department of Homeland Security. Strategic principles for securing the internet of things (iot). https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

[75] Mark R Warner. S.1691 - internet of things (iot) cybersecurity improvement act of 2017. https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt.

[76] YourThings. YourThings scorecard. https://yourthings.info/.