NEW AMERICA

September 2020

The Digital Standard Testing Handbook

How to Assess the Security of the Internet of Things

Nat Meysenburg, Ross Schulman, & Andi Wilson Thompson

Acknowledgments

In addition to Ranking Digital Rights and Consumer Reports, we would like to thank the many product designers, developers, and manufacturers that provided feedback on the Digital Standard. We would also like to thank Craig Newmark Philanthropies for its generous support of our work in this area.

About the Author(s)

Nat Meysenburg is a technologist at the Open Technology Institute who works on building and maintaining systems with privacy, security and freedom in mind.

Ross Schulman is a senior counsel and senior policy technologist at New America's Open Technology Institute.

Andi Wilson Thompson is a senior policy analyst at New America's Open Technology Institute where she focuses on issues including digital security, vulnerabilities equities, encryption, and internet freedom.

About New America

We are dedicated to renewing the promise of America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Open Technology Institute

OTI works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

Contents

Contents Cont'd

Contents Cont'd

Definitions

Note: Definitions will be adapted and added throughout this project.

Legal Documents

Legal documents, when used in our methodology, refers to all of the legally binding documents that a company presents to a person purchasing or using a product. These may include the privacy policy, terms of service, end user license agreement (EULA), and warranty, as well as any other documents that represent a public statement of fact or commitment about the product by the company.

Privacy Policy

A privacy policy is a statement that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data. Be aware that some products might be subject to more than one privacy policy. For example, website privacy policies may or may not apply to data collected from devices sold by the company. They often only cover information related to the website itself. In order to find a product's privacy policy, look in the packaging the device came in for any relevant paperwork. Look at documentation associated with any mobile apps required for use along with the product. Privacy policies may also be located on the company's website, sometimes under a tab titled "Policies" or "Legal."

Terms of Service

Terms of Service (ToS) are a set of regulations that are attached to a product or service. These regulations may also be called Terms and Conditions (ToC) or Terms of Use (ToU). Be aware that some products might be subject to more than one ToS policy. For example, products that work jointly between two companies or two services within the same company may be subject to separate ToS documents. Products may also contain different components like software or hardware that may each be governed by different ToS policies. In order to find a product's ToS, look in the packaging the device came in for any relevant paperwork. Look at documentation associated with any mobile apps required for use along with the product. ToS may also be located on the company's website, sometimes under a tab titled "Policies" or "Legal."

Introduction

The Internet of Things (IoT) is rapidly expanding, and more and more manufacturers of consumer products like kitchen appliances, televisions, and security systems are connecting those devices to the internet. Last year, New America's Open Technology Institute (OTI) undertook a project to **educate people** about the **Digital Standard**, a new framework for evaluating the privacy and security of internet-connected consumer products and software. The Standard was developed by a group of organizations, including **Ranking Digital Rights**, in collaboration with **Consumer Reports**, **Aspiration**, **the Cyber Independent Testing Lab**, **Disconnect**, and other partners. For companies, the Digital Standard is a useful tool to help drive privacy and security-focused development, and as a checklist to add to quality assurance processes. For the press, the Digital Standard is a benchmark by which to measure products while reporting on information security and data privacy. Civil society organizations can use the Digital Standard in policy research, or as an example as they advocate for companies to implement best practices for privacy and security.

The most common complaint we heard while discussing the Standard with product designers, developers, and manufacturers was that it didn't provide enough guidance about how to perform the tests that it describes. The Standard contains dozens of "indicators" (individual items detailing the elements of behavior that make up a test) that need to be evaluated when testing a given device. They take the form of a broad statement to be evaluated, such as "users can control how their information is used to target advertising" or "the software does not make use of unsafe functions or libraries." They describe what the designated outcome should be, but by and large the indicators do not spell out how to arrive at an answer. A more in-depth step-by-step instruction manual is usually called a "methodology," however there is not yet a Digital Standard methodology available to the public.

OTI is setting out to fill that gap by selecting a few representative products and apps and putting them through the Digital Standard wringer. Throughout the process, we'll be taking detailed notes on how exactly we judged each indicator, including what information we needed to collect in order to measure whether the indicator is met, where we looked for it and where we found it, and how we interpreted the inevitable vagueness and edge cases. We will publish our notes openly as a resource as we go along, and we'll update the methodology in real time to keep up with our findings. We hope this enables more people to use the Digital Standard.

Terms of Service and Privacy Policy Documents

Criteria: I can easily find, read, and understand the terms of service and privacy policy.

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

Note: This test applies the same indicators to a company's terms of service and privacy policy. We have separated the process and results into a section for each document for clarity.

Terms of Service

→ **INDICATORS**

1. The company clearly discloses which terms of service apply to the product/service in question.
2. The terms of service are easy to find.
3. The terms of service are available in the language(s) most commonly spoken by the company's users.
4. The terms of service are presented in an understandable manner.

Methodology for Assessing Each Indicator

1) The company clearly discloses which terms of service apply to the product/service in question.

- Obtain and review a copy of the product's terms of service.

- If you can find the terms of service and it is clear that they apply to the product you are testing, mark **PASS**.

- If you can find the terms of service but it is not clear that they apply to the product you are testing, mark **PARTIAL PASS**.

- If you cannot find the terms of service, mark **FAIL**.

2) The terms of service are easy to find.

- If you can easily find the terms of service, mark **PASS**.

- If you cannot easily find the terms of service, mark **FAIL**.

3) The terms of service are available in the language(s) most commonly spoken by the company's users.

- To assess whether the terms of service are available in the necessary language(s) requires us to know more about the product's distribution and global sales. This may be, but is not always available, on the product's website.

- If the product's website provides a list of all countries in which the product is sold and you can find the terms of service in languages that apply to all countries in which the product is for sale, mark **PASS**.

- If you can find the terms of service in one language or more, but it is not clear whether those languages apply to the majority of the product's users, mark **PARTIAL PASS**.

- If you cannot find the terms of service, mark **FAIL**.

4) The terms of service are presented in an understandable manner.

- To assess whether the terms of service are "understandable" is challenging and requires information that is not provided in the current indicators for the Digital Standard. An "understandable manner" is an ambiguous term, and different testers may interpret it in different ways.

- For example, there is debate about best practices in length of terms of service. There is an argument that a shorter, more plain-language set of terms of service is preferable because non-experts are more likely to read it. There is also an argument that a long, comprehensive terms of service gives users complete information about the product that they are using without leaving facts out or ambiguity of terms.

- In order to establish what an "understandable manner" is for the purpose of evaluation, the tester must generate an opinion as to what the best practices for understandable terms of service development are, and apply those to the product's terms of service.

- For the purposes of this process, we suggest that "understandable" be applied as using plain language to describe policies, a clear structure that allows users to easily review by using headings or other structural signposts, and defining ambiguous terms like "Content," "Third Party," etc. to clarify for users.

- If the terms of service are written in plain language, the important terms are defined, and the document is easy to follow, mark **PASS**.

- If some, but not all of the above are true, mark **PARTIAL PASS**.

- If none of the above are true, mark **FAIL**.

Privacy Policy

→ INDICATORS

1. The company clearly discloses which privacy policy applies to the product/service in question.

2. The privacy policy is easy to find.

3. The privacy policy is available in the language(s) most commonly spoken by the company's users.

4. The privacy policy is presented in an understandable manner.

1) The company clearly discloses which privacy policy applies to the product/service in question.

- Obtain and review a copy of the product's privacy policy.

- If you can find the privacy policy and it is clear that it applies to the product you are testing, mark **PASS**.

- If you can find the privacy policy but it is not clear that it applies to the product you are testing, mark **PARTIAL PASS**.

- If you cannot find the privacy policy, mark **FAIL**.

2) The privacy policy is easy to find.

- If you can easily find the privacy policy, mark **PASS**.

- If you cannot easily find the privacy policy, mark **FAIL**.

3) The privacy policy is available in the language(s) most commonly spoken by the company's users.

- To assess whether the privacy policy is available in the necessary language(s) requires us to know more about the product's distribution and global sales. This may be, but is not always available, on the product's website.

- If the product's website provides a list of all countries in which the product is sold and you can find the privacy policy in languages that apply to all countries that the product is for sale in, mark **PASS**.

- If you can find the privacy policy in one language or more, but it is not clear whether those languages apply to the majority of the product's users, mark **PARTIAL PASS**.

- If you cannot find the privacy policy, or conclude that the privacy policy is not available in all of the commonly spoken languages of users, mark **FAIL**.

4) The privacy policy is presented in an understandable manner.

- This indicator is a challenge to evaluate. An "understandable manner" is an ambiguous term, and different testers may interpret it in different ways.

- In order to establish what an "understandable manner" is for the purpose of evaluation, the tester must generate an opinion as to what the best practices for understandable privacy policy development is, and apply those to the product's terms of service.

- For the purposes of this process, we suggest that "understandable" be applied as using plain language to describe policies, a clear structure that allows users to easily review by using headings or other structural signposts, and defining ambiguous terms like "Content," "Third Party," etc. to clarify for users.

- If the privacy policy is written in plain language, the important terms are defined, and the document is easy to follow, mark **PASS**.

- If some, but not all, of the above are true, mark **PARTIAL PASS**.

- If none of the above are true, mark **FAIL**.

Terms of Service and Privacy Policy Change Notification

Criteria: The company provides clear notification when it changes its terms of service and privacy policy.

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

Note: This test applies the same indicators to a company's terms of service and privacy policy. We have separated the process and results into a section for each document for clarity.

Terms of Service

→ INDICATORS

1. Commitment to notify users about changes to the terms of service.
2. Disclosure of how users will be directly notified of changes to the terms of service.
3. Disclosure of timeframe for notification prior to changes to the terms of service coming into effect.
4. Maintains a public archive or change log of the terms of service.

Methodology for Assessing Each Indicator

1) Commitment to notify users about changes to the terms of service.

- Obtain and review a copy of the product's terms of service.

- Review the terms of service to determine whether they include any content commiting to notify users about any policy changes.

- If the terms of service does not indicate that the company will notify users, mark **FAIL**.

- If the terms of service indicates that the company will notify users, mark **PASS**.

2) Disclosure of how users will be directly notified of changes to the terms of service.

- Review any relevant terms of service to identify any language describing *how* users will be notified of changes to the terms of service.

- If the terms of service indicates how the company will notify users, mark **PASS**.

- If the terms of service does not indicate how the company will notify users, mark **FAIL**.

3) Disclosure of timeframe for notification prior to changes to the terms of service coming into effect.

- Review any relevant terms of service to identify any language describing a timeline for notifying users of changes to the terms of service.

- If the terms of service indicates when the changes will take effect, mark **PASS**.

- If the terms of service does not indicate when the changes will take effect, mark **FAIL**.

4) Maintains a public archive or change log of the terms of service.

- Review any relevant terms of service for language describing or identifying past terms of service or commitments to document terms of service policy changes.

- If the terms of service indicates that they have a policy of retaining previous policies for reference, mark **PASS**.

- If the terms of service contains or links to documentation of past policies, but does not provide clear language regarding whether this is a consistent practice, mark **PARTIAL PASS**.

- If the terms of service does not provide any language or examples that indicate public documentation of policy changes, mark **FAIL**.

Privacy Policy

→ **INDICATORS**

1. Commitment to notify users about changes to the privacy policy.

2. Disclosure of how users will be directly notified of changes to the privacy policy.

3. Disclosure of timeframe for notification prior to changes to the privacy policy coming into effect.

4. Maintains a public archive or change log of the privacy policy.

Methodology for Assessing Each Indicator

1) Commitment to notify users about changes to the privacy policy.

- Obtain and review a copy of the product's privacy policy.

- If the privacy policy indicates that the company will notify users, mark **PASS**.

- If the privacy policy does not indicate that the company will notify users, mark **FAIL**.

2) Disclosure of how users will be directly notified of changes to the privacy policy.

- Review any relevant privacy policies for language on change notification processes.

- If the privacy policy indicates how the company will notify users, mark **PASS**.

- If the privacy policy does not indicate how the company will notify users, mark **FAIL**.

3) Disclosure of timeframe for notification prior to changes to the privacy policy coming into effect.

- Review any relevant privacy policies for language on change notification timeline.

- If the privacy policy indicates when the changes will take effect, mark **PASS**.

- If the privacy policy does not indicate when the changes will take effect, mark **FAIL**.

4) Maintains a public archive or change log of the privacy policy.

- Review any relevant privacy policies to identify any language describing past policies or commitments to document policy changes.

- If the privacy policy indicates that they have a policy of retaining previous policies for reference, mark **PASS**.

- If the privacy policy contains or links to documentation of past policies, but does not provide clear language regarding whether this is a consistent practice, mark **PARTIAL PASS**.

- If the privacy policy does not provide any language or examples that indicate public documentation of policy changes, mark **FAIL**.

Process for Terms of Service Enforcement

Criteria: I know how, when, and why the company or organization unilaterally closes user accounts and/or restricts access to services.

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ INDICATORS

1. The company or organization clearly explains what types of activities it does not permit.
2. The company or organization clearly explains why it may restrict a user's account.
3. The company or organization clearly discloses the mechanisms it uses to identify accounts that violate the rules.
4. The company or organization clearly discloses whether any non-government and non-judicial entities receive priority consideration when identifying accounts to be restricted for violating the company's rules, and if so, how that priority status is conferred.
5. The company or organization clearly explains its process for enforcing its rules.
6. The company or organization provides clear examples to help the user understand what the rules are and how they are enforced.

Methodology for Assessing Each Indicator

1) The company or organization clearly explains what types of activities it does not permit.

- Obtain and review the product's terms of service.
- Review the product's terms of service for language listing specific activities that are not permitted.
- If a list of types of activities the company does not permit is included in the terms of service, mark **PASS**.
- If a list of types of activities the company does not permit is not included in the terms of service, mark **FAIL**.

2) The company or organization clearly explains why it may restrict a user's account.

- These restrictions may be different than those listed in the types of activities that the terms of service will and won't permit. For example, some activities that violate the terms of service could result in a content takedown, others may result in closing a user's account.
- If there is a list of reasons available in the terms of service, mark **PASS**.
- If there is not a list of reasons available in the terms of service, mark **FAIL**.

3) The company or organization clearly discloses the mechanisms it uses to identify accounts that violate the rules.

- If information about these mechanisms is available in the terms of service, mark **PASS**.
- If information about these mechanisms is not available in the terms of service, mark **FAIL**.

4) The company or organization clearly discloses whether any non-government and non-judicial entities receive priority consideration when identifying accounts to be restricted for violating the company's rules, and if so, how that priority status is conferred.

- This indicator does not ascribe value to whether actors receiving, or not receiving, priority consideration is a positive or negative for consumer privacy and security. Therefore, if we are using pass as a signal of adhering to best practices, it is unclear what our ideal situation is.

- If the company does not provide information about any sort of priority status, whether they provide that status or not, then they would fail the test. For privacy and security purposes it would be preferable that companies *not* provide any sort of priority consideration, but as this indicator is written, they would not receive any credit for treating all requests equally should they fail to include that stipulation in their terms of service.

- If this information is available in the terms of service, mark **PASS**.

- If this information is not available in the terms of service, mark **FAIL**.

5) The company or organization clearly explains its process for enforcing its rules.

- If information about these mechanisms is available in the terms of service, mark **PASS**.

- If information about these mechanisms is not available in the terms of service, mark **FAIL**.

6) The company or organization provides clear examples to help the user understand what the rules are and how they are enforced.

- If examples are available in the terms of service, mark **PASS**.

- If examples are not available in the terms of service, mark **FAIL**.

Transparency About Terms of Service Enforcement

Criteria: I know how often the company or organization unilaterally closes user accounts.

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ **INDICATORS**

1. The company or organization publishes data about the number of accounts it restricts or closes on its own initiative.
2. The company or organization publishes data about the number of accounts it restricts or closes as a result of a government request.
3. The company or organization publishes data about the number of accounts it restricts or closes as a result of a request from private third-parties.
4. The company or organization clearly discloses that it notifies users when it restricts or closes user accounts.

Methodology for Assessing Each Indicator

1) The company or organization publishes data about the number of accounts it restricts or closes on its own initiative.

- Obtain and review a copy of the product's terms of service.
- Review the terms of service to locate any information describing data reporting requirements and processes regarding the number of accounts the company restricts or closes.

- Look for a transparency report published in relation to the product. This should be listed on the website, likely under a “Legal” tab.

- If the company does publish a transparency report, check if it contains information about account restrictions or closures. Note: indicators 1, 2, and 3 under this test discuss information that may be available in a transparency report. The difference between each indicator is based on what actor makes the request to restrict or close an account: the company, a government actor, or a private third-party organization.

- The Digital Standard contains tests specific to criteria for transparency reporting. Refer to those tests for more information on the role these reports play in evaluating privacy and security.

- If the company publishes information about the number of accounts it restricts or closes on its own initiative, mark **PASS**.

- If the company does not publish information about account restrictions or closures on its own initiative, mark **FAIL**.

2) The company or organization publishes data about the number of accounts it restricts or closes as a result of a government request.

- Review the terms of service for information on data reporting requirements and processes.

- Look for a transparency report published in relation to the product. This should be listed on the website, likely under a “Legal” tab.

- If the company does publish a transparency report, check if it contains information about account restrictions or closures as a result of a government request.

- The Digital Standard contains tests specific to criteria for transparency reporting. Refer to those tests for more information on the role these reports play in evaluating privacy and security.

- If the company publishes information about the number of accounts it restricts or closes as a result of a government request, mark **PASS**.

- If the company does not publish information about account restrictions or closures as a result of a government request, mark **FAIL**.

3) The company or organization publishes data about the number of accounts it restricts or closes as a result of a request from private third-parties.

- Review the terms of service for information on data reporting requirements and processes.
- Look for a transparency report published in relation to the product. This should be listed on the website, likely under a “Legal” tab.
- If the company does publish a transparency report, check if it contains information about account restrictions or closures as a result of a request from private third-parties.
- The Digital Standard contains tests specific to criteria for transparency reporting. Refer to those tests for more information on the role these reports play in evaluating privacy and security.
- If the company publishes information about the number of accounts it restricts or closes as a result of a request from private third-parties, mark **PASS**.
- If the company does not publish information about account restrictions or closures as a result of a request from private third-parties, mark **FAIL**.

4) The company or organization clearly discloses that it notifies users when it restricts or closes user accounts.

- Review the terms of service for information on requirements and processes for notifying users regarding account restrictions or closures.
- Look for a transparency report published in relation to the product. This should be listed on the website, likely under a “Legal” tab.
- If the company does publish a transparency report, check if it contains information about user notification requirements or processes for account restrictions or closures.
- The Digital Standard contains tests specific to criteria for transparency reporting. Refer to those tests for more information on the role these reports play in evaluating privacy and security.
- If the company clearly discloses that it notifies users when it restricts or closes user accounts, mark **PASS**.

- If the company does not clearly disclose that it notifies users when it restricts or closes user accounts, mark **FAIL**.

Identity Policy

Criteria: I can register using any name and identifying characteristics I wish, or keep my identity completely anonymous.

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ **INDICATORS**

1. The company does 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.

Methodology for Assessing Each Indicator

1) The company does 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.

- Obtain and review a copy of the product's terms of service and privacy policy.
- Look for language regarding information that the company collects.
- Look for information regarding any sort of requirement that the user must use a legal name, or provide any copies of identification like a drivers' license in order to use the product.
- Try to set up an account using the device or application. See what information is collected and whether that information is verified in any way.

- If identity verification is not required, mark **PASS**.

- If information is required that could be linked to an offline identity, but does not require government-issued documents, mark **PARTIAL PASS**.

- If users are required to verify identity using government-issued documents, mark **FAIL**.

Security Oversight

Criteria: The company is a responsible caretaker of my data.

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ INDICATORS

1. The company has systems in place to limit and monitor employee access to user information.
2. The company has an internal security team that conducts security audits on the company's products and services.
3. The company commissions third-party security audits on its products and services.
4. The company ensures that third-parties who process data on behalf of the company implement the required technical and organizational measures to protect user data.

Methodology for Assessing Each Indicator

1) The company has systems in place to limit and monitor employee access to user information.

- Obtain and review a copy of the product's privacy policy, review any other online documentation available
- Look for language describing access limitations or data privacy policies that prevent employees from viewing user information.

- Review the website more generally, likely sections marked “Legal” or “Policies,” for information about user privacy and access to information.

- If the privacy policy indicates that the company has limitations or processes regulating employee access to user information, mark **PASS**.

- If the privacy policy does not indicate whether or not the company has limitations or processes regulating employee access to user information, mark **FAIL**.

2) The company has an internal security team that conducts security audits on the company's products and services.

- Obtain and review a copy of the product’s privacy policy.

- Look for language describing internal review processes or audits.

- Look for language describing staff or experts who are engaged in security audits.

- Review the website more generally, likely sections marked “Legal” or “Policies” for information about security audits.

- If the privacy policy indicates that the company has an internal security team that conducts security audits on the company's products and services, mark **PASS**.

- If the privacy policy does not indicate whether or not the company has limitations or processes regulating employee access to user information, mark **FAIL**.

3) The company commissions third-party security audits on its products and services.

- Obtain and review a copy of the product’s privacy policy.

- Look for language describing whether the company commissions third-parties to conduct review processes or audits of its services.

- Look for language describing which third-parties are engaged to conduct these audits.

- Review the website more generally, likely sections marked “Legal” or “Policies,” for information about third-party security audits.

- If the privacy policy or another part of the website indicates that the company commissions third-party security audits on its products and services, mark **PASS**.

- If the privacy policy does not indicate whether or not the company commissions third-party security audits on its products and services, mark **FAIL**.

4) The company ensures that third-parties who process data on behalf of the company implement the required technical and organizational measures to protect user data.

- Obtain and review a copy of the product’s privacy policy.

- Look for language describing security measures required of third-party data processors.

- If the privacy policy describes requirements for data protection policies by third-party data processors, mark **PASS**.

- If the privacy policy does not describe requirements for data protection policies by third-party data processors, mark **FAIL**.

Third-Party Requests for User Data

Criteria: The company complies only with legal and ethical third-party requests for user information.

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ **INDICATORS**

1. The company explains its process for responding to non-judicial government requests.
2. The company explains its process for responding to court orders.
3. The company explains its process for responding to requests from foreign jurisdictions.
4. The company explains its process for responding to requests made by private parties.
5. The company's explanations include the legal basis under which it may comply.
6. The company commits to carry out due diligence on requests before deciding how to respond and to push back on unlawful requests.
7. The company provides guidance or examples of implementation of its process.

1) The company explains its process for responding to non-judicial government requests.

- Obtain and review a copy of the product's privacy policy. Obtain and review any transparency reports that the company has published.

- Look for any information about third-party requests for user information. These are often divided into judicial/law enforcement requests (warrants, court orders, and other legal tools), non-judicial government requests, and third-party requests that do not come from governments.

- Some policies identify each of these types of requests and provide separate information, but many also combine them into a broader information sharing policy.

- For this indicator you want to find specific information about non-judicial government requests, for example, what information they require from governments as part of these requests, who reviews these requests, and how they provide user information to governments.

- If the privacy policy describes a process for responding to non-judicial government requests, mark **PASS**.

- If the privacy policy does not describe a process for responding to non-judicial government requests, mark **FAIL**.

2) The company explains its process for responding to court orders.

- Obtain and review a copy of the product's privacy policy. Obtain and review any transparency reports that the company has published.

- Look for any information about third-party requests. These are often divided into judicial/law enforcement requests (warrants, court orders, and other legal tools), non-judicial government requests, and third-party requests that do not come from governments.

- Some policies identify each of these types of requests and provide separate information, but many also combine them into a broader information sharing policy.

- For this indicator, you want to find specific information about the process the company follows in responding to court orders. Different types of court orders may be listed, for example warrants or any court orders or legal tools used in the country where the company operates.

- If the privacy policy describes a process for responding to court orders, mark **PASS**.

- If the privacy policy does not describe a process for responding to court orders, mark **FAIL**.

3) The company explains its process for responding to requests from foreign jurisdictions.

- Obtain and review a copy of the product's privacy policy. Obtain and review any transparency reports that the company has published.

- Look for any information about third-party requests for user information.

- For this indicator, you want to see a clear indication that any policies about information sharing distinguish based upon where the request is coming from. For example, a company may use a different process for responding to requests from the country where it operates versus a third-party country with a different legal system or processes.

- This indicator does not specify whether "requests from foreign jurisdictions" means solely government requests, or whether it includes third-parties located in a different country.

- If the privacy policy describes a process for responding to foreign jurisdiction requests, mark **PASS**.

- If the privacy policy does not describe a process for responding to foreign jurisdiction requests, mark **FAIL.**

4) The company explains its process for responding to requests made by private parties.

- Obtain and review a copy of the product's privacy policy.

- Look for any information about third-party requests for user information.

- For this indicator, the privacy policy should distinguish between government requests and non-government third-party requests.

- If the privacy policy describes a process for responding to private party requests, mark **PASS**.

- If the privacy policy does not describe a process for responding to private party requests, mark **FAIL**.

5) The company's explanations include the legal basis under which it may comply.

- Obtain and review a copy of the product's privacy policy.

- Look for any information about compliance with third-party requests.

- For this indicator, the privacy policy includes legal language describing the grounds under which it may comply.

- If the privacy policy describes the legal basis under which it may comply with third-party requests, mark **PASS**.

- If the privacy policy does not describe the legal basis under which it may comply with third-party requests, mark **FAIL**.

6) The company commits to carry out due diligence on requests before deciding how to respond and to push back on unlawful requests.

- Obtain and review a copy of the product's privacy policy. Obtain and review any transparency reports that the company has published.

- Look for any information about compliance with third-party requests.

- Look for any information regarding a legal review process for requests to assess whether they are lawful.

- Look for any information regarding ways that a company may respond to requests that they deem unlawful.

- If the privacy policy describes a commitment to carry out due diligence, mark **PASS**.

- If the privacy policy does not describe a commitment to carry out due diligence, mark **FAIL**.

7) The company provides guidance or examples of implementation of its process.

- Obtain and review a copy of the product's privacy policy. Obtain and review any transparency reports that the company has published.

- Look for examples of how third-party requests for user data would be handled under that privacy policy.

- If the privacy policy provides examples of implementation, mark **PASS**.

- If the privacy policy does not provide examples of implementation, mark **FAIL**.

Data Control

Criteria: I can see and control everything the company knows about me.

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

Notes:

- *Some devices may capture a category of information but not transmit that data to the service provider, instead using the data only locally on the device, or presenting it for the information of the owner.*
- *In such cases, that data capture may not be reported in the legal documents as being collected by the service provider.*
- *While we encourage companies to develop products that only store collected data locally on the device instead of transmitting data to the cloud, it is still a best practice for companies to inform users of all data collected, even if a piece of information does not leave the device.*

→ INDICATORS

1. The definition of "user information" includes information collected from third-parties.
2. Users can control the collection of their information.
3. Users can delete their information.
4. Users can control how their information is used to target advertising.
5. Clear explanation of how users can control whether their information is used for targeted advertising.
6. Users can obtain a copy of their information.

7. Disclosure of what user information users can obtain.

8. Users can obtain their information in a structured data format.

9. Users can obtain all public-facing and private user information the company holds about them.

Methodology for Assessing Each Indicator

1) The definition of "user information" includes information collected from third-parties.

- Find the definition of "user information" (or equivalent phrase) in the legal documents.
    - This definition may also take the form of a list labeled "Information We Collect" or a similar phrase.
- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.
- If there is a definition of user information or a description of information the service provider collects and it includes information collected from third parties, mark **PASS**.
- If policies do not have a definitions section or do not define user information, mark **FAIL**.
- If the definition does not include information collected from third parties, look for any sections defining what data is collected.
    - If there is a section describing information that is collected, but no information from third parties is reported, mark **PASS**.
    - If legal documents indicate that information is collected from third parties (even though they failed to include that in the definition), mark **FAIL**.

2) Users can control the collection of their information.

- Obtain and review a copy of the product's legal documents, comparing what information is collected and what information the owner is able to restrict from sharing.

- There are likely going to be some pieces of information that the owner cannot withhold without making the service inoperable, such as billing information. For the purposes of evaluating this indicator, reviewers can disregard data that is integral to the operation of the service or product.

- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.

- Note that products that are already designed to collect the minimal amount of data from the user may fail this indicator when in reality the product is very privacy-protective. Testers may consider giving a **PASS** in such an instance.

- If the legal documents give users control over what data is collected (or indicate how to enact such control via the product), with some allowances for basic pieces of information without which the service could not operate, mark **PASS**.

- If legal documents give users control over the collection of some, but not all types of data, mark **PARTIAL PASS**.

- If the legal documents do not address user control of collection, mark **FAIL**.

- If the legal documents explicitly deny users the ability to control collection of any data, mark **FAIL**.

3) Users can delete their information.

- Review the legal documents, comparing what information is collected and what information the owner is able to delete.

- There are likely going to be some pieces of information that the owner cannot delete without making the service inoperable, such as billing information. For the purposes of evaluating this indicator, reviewers can disregard data that is integral to the operation of the service or product.

- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.

- Note that products that are already designed to collect the minimal amount of data from the owner may fail this indicator when in reality the product is very privacy-protective. Testers may consider giving a **PASS** in such an instance.

- If the legal documents give users the ability to delete data (or indicate how to enact such control via the product), with some allowances for basic pieces of information without which the service could not operate, mark **PASS**.

- If the legal documents do not address users' ability to delete data, mark **FAIL**.

- If the legal documents explicitly deny users the ability to delete data, mark **FAIL**.

4) Users can control how their information is used to target advertising.

- Review the legal documents, looking for any mention of targeted advertising.

- Search for sections describing a user's ability to constrain how the company uses information about them for purposes of targeted advertising (sometimes referred to as behavioral advertising).

- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.

- If the legal documents indicate that the company does not use or share customer information for targeted advertising, mark **PASS**.

- If the legal documents indicate that the company does use or share customer information for targeted advertising, and that users can control how their information is shared, mark **PASS**.

- If the legal documents state that customer information is used for targeted advertising and that users cannot control the use of their information for that purpose, mark **FAIL**.

5) Clear explanation of how users can control whether their information is used for targeted advertising.

- Review the legal documents, looking for any mention of targeted advertising.

- Look at any sections detailing with whom and under what circumstances the company will share customer information.

- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.

- If the legal documents provide a list of how users' information will be shared and that list does not include sharing of information for purposes of advertising, mark **PASS**.

- If the legal documents do indicate that user information will be shared for purposes of advertising.

    - Search for language describing how users can control the sharing of information for advertising purposes.

    - If the documents describe in enough detail for the average person to follow how a user can control the sharing of their information for advertising, mark **PASS**.

    - If the legal documents reviewed do not describe, or do not describe clearly enough to be followed, how a user can control the sharing of their information for targeted advertising, mark **FAIL**.

6) Users can obtain a copy of their information.

- Review the legal documents, looking for discussion of users' ability to obtain copies of their data. Commonly used terms that describe this kind of ability include "access" and "portability."

- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.

- If the legal documents give users the right to access their own information in some form without restriction, mark **PASS**.

- If the legal documents give users the right to access only some of their information, or if it is not clear how much information users can obtain or how users can obtain their information, mark **PARTIAL PASS**.

- If the legal documents do not mention or expressly forbid users from accessing their own information, mark **FAIL**.

7) **Disclosure of what user information users can obtain.**

- Review the legal documents, looking for discussion of users' ability to obtain copies of their data. Commonly used terms that describe this kind of ability include "access" and "portability."

- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.

- If the legal documents list in detail what information is available to obtain, mark **PASS**.

- If the legal documents list obtainable information generically or by category, mark **PARTIAL PASS**.

- If the legal documents do not list in detail what information is available to obtain, mark **FAIL**.

8) Users can obtain their information in a structured data format.

- Review the legal documents, looking for discussion of users' ability to obtain copies of their data. Commonly used terms that describe this kind of ability include "access" and "portability."

- Look for descriptions of the ability to download user data for statements about a "structured" or "machine-readable" format.

    - OR, attempt to make use of the service's data download feature and inspect the files returned by the service, looking for files in common formats, such as JSON, XML, or other structured file types.

- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.

- If the legal documents state that data downloads are available in a structured format, or the download itself is provided in such a format, mark **PASS**.
- If the download is not provided in a structured format or no download is available at all, mark **FAIL**.

9) Users can obtain all public-facing and private user information the company holds about them.

- Review the legal documents, looking for discussion of users' ability to obtain copies of their data. Commonly used terms that describe this kind of ability include "access" and "portability."
- Look for a statement establishing the ability of users to obtain all public-facing and private information the service provides has about the user.
- Note that it is not enough that the list of information that users can obtain is the same as the list of information that the service states that it collects, as the service provider may gain access to information about users from other services such as data brokers.
- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.
- If the legal documents state that users may obtain all public-facing and private information (or just "all information") about the user, mark **PASS**.
- If the legal documents do not state that users may obtain all public-facing and private information about the user or if users cannot access their information at all, mark **FAIL**.

Data Collection

Criteria: I know what user information this company is collecting and when.

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

Notes:

- *Some devices may capture a category of information but not transmit that data to the service provider, instead using the data only locally on the device, or presenting it for the information of the owner.*
- *In such cases, that data capture may not be reported in the legal documents as being collected by the service provider.*
- *While we encourage companies to develop products that only store collected data locally on the device instead of transmitting data to the cloud, it is still a best practice for companies to inform users of all data that is collected, even if a piece of information does not leave the device.*
- *It is important to note that these indicators (like many of the others in the Digital Standard) measure only what the service provider says that they do in their own documents. They do not measure what data the product actually collects.*

→ INDICATORS

1. Disclosure of the type of user information collected.
2. Disclosure of how user information is collected.
3. Test the product's sensors to determine whether they give clear indication when they become activated.

Methodology for Assessing Each Indicator

1) Disclosure of the type of user information collected.

- Obtain and review a copy of the service provider's legal documents.

- Find the portion of the legal documents that describe what information the service provider collects in the course of operation of the product.

- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.

- If the legal documents provide a description of precisely what user information the service provider collects, or describes the data in more generalized categories or types of information, mark **PASS**.

- If the legal documents do not describe data collected, or describe that data at such a high level as to be unhelpful for the consumer, mark **FAIL**.

2) Disclosure of how user information is collected.

- Obtain and review a copy of the service provider's legal documents.

- Find the portions of the legal documents addressing information collection. This information may be specified on its own, but may also be mixed in with the descriptions of the types of data collected, so gathering the information from a few locations may be necessary.

- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.

- Determine whether the documents describe the method for collecting each type of data listed in the disclosures. Note that there are some types of information for which the means of collection are self-evident, e.g. billing and contact information that is collected when a user creates an account with a service are obviously collected directly from the user. If the legal documents do not include such obvious methods of collection in such self-evident instances, but describe other methods of collection, mark **PASS**.

- If the legal documents describe how the information is collected for each type of data the service provider collects from the user, mark **PASS**.

- If the legal documents describe how the information is collected for some, but not all of the types of data the service provider collects from the user, mark **PARTIAL PASS**.

- If the legal documents do not describe how information is collected at all, mark **FAIL**.

3) Test the product's sensors to determine whether they give clear indication when they become activated.

- Examine product description, legal documents, and/or product advertising to collect a list of probable sensors included in the product.

- For each sensor that could collect personal information, take whatever steps are necessary to activate the sensor and look for indication of activation.

- If every sensor that could collect personal information displays some indication when it is activated, mark **PASS**.

- If the test can show that the device's sensors activate but there is no clear indication for users, mark **FAIL**.

Minimal Data Collection

Criteria: The only information the company collects about me is what's needed to make the product or service work correctly.

See the test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

Notes:

- *Some devices may capture a category of information but not transmit that data to the service provider, instead using the data only locally on the device, or presenting it for the information of the owner.*
- *In such cases, that data capture may not be reported in the legal documents as being collected by the service provider.*
- *While we encourage companies to develop products that only store collected data locally on the device instead of transmitting data to the cloud, it is still a best practice for companies to inform users of all data collected, even if a piece of information does not leave the device.*

→ INDICATORS

1. The user information collected is only that which is directly relevant and necessary for the service.
2. Product still works when all permissions not relevant to product's functionality are declined.

1) The user information collected is only that which is directly relevant and necessary for the service.

- Obtain and review a copy of the product's legal documents.
- Find the section of the legal documents that lists the user information collected by the product or service and compare the types of information collected to the features offered by the product.
- If the legal documents provide reasons for the collection of each type of data, look for reasons that are not tied to, or go beyond what would be needed for, the operation of the service.
- Try to think through whether certain types of data collected are truly needed based upon the stated purpose of the product or service.
    - Note that this reasoning will be necessarily subjective.
    - Keep in mind that data may have multiple uses, e.g. an address could be necessary for billing purposes, but may also be used for marketing or customer research.
    - Note that such additional potential uses may well cause a product to fail other indicators.
- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.
- If the legal documents provide clear and convincing descriptions of the need for each type of data collected for the operation of the product, and as long as one use of the data out of many potential uses fits the actual necessary functions of the product or service, mark **PASS**.
- If most of the types of data have adequate reasons for collection provided, but a small number (particularly for difficult to define categories) do not, mark **PARTIAL PASS**.
- If most or all of the types of data collected have no rationale for their collection that is directly related to and necessary for the operation of the service, mark **FAIL**.

2) Product still works when all permissions not relevant to product's functionality are declined.

- Check for methods to decline permission for the product to collect information.

    - If the product has a user interface of any kind, look for a “settings” or “options” menu or screen. Search any such screens for data collection restrictions.

    - If the product has an accompanying mobile app or web interface, look for any feature that allows the user to deny collection of unneeded data.

- If the product does present methods to revoke permission to collect data.

    - Revoke or decline all collection not deemed to be directly related to the functionality of the product.

    - Test all known functionality of the product and record whether the product still operates as before/as advertised.

    - If the product operates the same after permissions not relevant to the product’s functionality are declined, mark **PASS**.

- If the product is collecting information that is not needed for it to operate, and if the product does not present any method by which to decline permission for collection of data determined to be unnecessary for functionality (such as the user’s date of birth or street address in a smart thermostat), mark **FAIL**.

- If there are no visible settings that would enable the user to control data collection or use that may affect the user’s privacy, mark **FAIL**.

Data Use

Criteria: Data usage is consistent with the context of the relationship with the user and is transparent.

See the test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

Notes:

- *Some devices may capture a category of information but not transmit that data to the service provider, instead using the data only locally on the device, or presenting it for the information of the owner.*
- *In such cases, that data capture may not be reported in the legal documents as being collected by the service provider.*
- *While we encourage companies to develop products that only store collected data locally on the device instead of transmitting data to the cloud, it is still a best practice for companies to inform users of all data collected, even if a piece of information does not leave the device.*

→ INDICATORS

1. The company puts limits on the use of my data that are consistent with the purpose for which the data is collected.
2. The company explicitly discloses every way in which it uses my data.

Methodology for Assessing Each Indicator

1) The company puts limits on the use of my data that are consistent with the purpose for which the data is collected.

- Obtain and review a copy of the service provider’s legal documents.

- Find the portion of the legal documents that addresses data use and compare the reasons the company provides for using data with the reasons it provides for collecting data. In particular, consider whether the company provides reasons why it needs each type of data collected in order to operate the product or provide offered services.

- Look in particular for data uses that fall outside of the stated purposes for data collection.

- If the legal documents are not clear about whether they apply to the “smart device” being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.

- If the use limitations stated in the legal documents are related to and proportional with the stated purposes for collecting the data, mark **PASS**.

- If the legal documents refer to uses of personal information that are outside the scope of the stated reasons listed for data collection, or if the documents do not explain whether or how certain collected data is used, mark **FAIL**.

2) The company explicitly discloses every way in which it uses my data.

- Make use of the product, both as an everyday user would and making sure to explore all the features of the product.

- Make note of all instances where personal data is likely to be used.

    - Look for personalization, advertisements, and “automatic” features.

    - If the product has a phone app, look at the permissions requested by the app as well as any information on data collection that the phone operating system offers (e.g. the app using the phone’s location services).

- Review the language in legal documents discussing how data is used.

    - Consider whether the language states that it is a comprehensive list of all the ways in which collected data is used.

    - Compare the list of uses to the observations from the prior step.

- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.

- If all of the uses of personal data observed during the testing of the product are included in the legal documents, mark **PASS**.

- If use of the product produces evidence of uses of data not disclosed in the legal documents, mark **FAIL**.

Data Retention and Deletion

See the test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

Notes:

- *This test features three separate criteria by which to assess the test's success. Each criteria features a unique set of indicators and a related methodology.*
- *Some devices may capture a category of information but not transmit that data to the service provider, instead using the data only locally on the device, or presenting it for the information of the owner.*
- *In such cases, that data capture may not be reported in the legal documents as being collected by the service provider.*
- *While we encourage companies to develop products that only store collected data locally on the device instead of transmitting data to the cloud, it is still a best practice for companies to inform users of all data collected, even if a piece of information does not leave the device.*

Criteria: The company retains data only as long as relevant and reasonably necessary to provide service to me.

→ INDICATORS

1. The company on its own deletes outdated and unnecessary personal information, or renders that data to be reasonably de-identified.
2. The company provides specific retention periods for different types of information that are reasonably scoped to get rid of outdated and unnecessary personal information.

Methodology for Assessing Each Indicator

1) The company on its own deletes outdated and unnecessary personal information, or renders that data to be reasonably de-identified.

- Obtain and review a copy of the service provider’s legal documents.
- Look for sections of the legal documents dealing with data deletion or retention.
    - This information may be in its own section with titles incorporating words such as “deletion” or “retention.”
    - This information may also be included elsewhere in the legal documents, such as alongside the list of types of data collected.
    - Do not confuse commitments about the user’s ability to delete personal information with this indicator, which focuses on the service’s obligation to delete personal information when it is no longer needed to perform the service.
- If the legal documents are not clear about whether they apply to the “smart device” being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.
- If legal documents state that personal information is deleted or anonymized “only as long as needed for providing the service” (or other similar language), mark **PASS**.
    - Many services will include a blanket clause that data may be retained in order to comply with legal obligations; such language should not cause the service to fail this indicator.
- If there is a strong commitment to deleting data, but only after an excessive or vague retention period, or if there are strong deletion commitments for most types of personal information, but less strong (or no) commitments for some other types, mark **PARTIAL PASS**.
- If the service’s legal documents are silent about the circumstances in which the service will delete personal information, or specifies that data will be retained longer than would be necessary to operate the service, mark **FAIL**.

2) The company provides specific retention periods for different types of information that are reasonably scoped to get rid of outdated and unnecessary personal information.

- Look for sections of the legal documents dealing with data retention.
  - If the service collects many different types of data, look to see if specific retention periods are given that are scoped to how personal the information in question is.
  - If the service does not collect many types of data, fewer different retention periods may still be appropriate, particularly if those periods are very short.
- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.
- If the legal documents give specific and limited retention periods for particular types of data, mark **PASS**.
- If there are specific retention periods for a few types of data, but not all of them, or not types that are particularly sensitive, mark **PARTIAL PASS**.
- If the service does not indicate that it has specific retention periods with reasonable scoping, mark **FAIL**.

Criteria: I can delete the data the company has about me that is not needed to provide the service.

→ INDICATORS

1. The company offers easy-to-find and -use controls that allow users to delete data not necessary to render service.

Methodology for Assessing Each Indicator

1) The company offers easy-to-find and -use controls that allow users to delete data not necessary to render service.

- Look in any user interfaces, such as web pages or mobile applications, related to the operation of the product or maintenance of user accounts related to the product.

- Look for controls related to the deletion of user data, which may exist in a "Profile" menu or window.

- If the app or web interface offers the ability to delete user data and is easy to find and use, mark **PASS**.

- If there is no feature in the app or web interface that offers the ability to delete user data, or such a feature exists but is unduly hard to find or use, mark **FAIL**.

Criteria: My account and information are deleted when I leave the service.

→ INDICATORS

1. All user information is deleted when the user's service is terminated, or the service no longer operates.

Methodology for Assessing Each Indicator

1) All user information is deleted when the user's service is terminated, or the service no longer operates.

- Look for sections of the legal documents dealing with data deletion or retention.

- Note whether the legal documents address the question of what happens to personal data when the user terminates their use of the service or the service ceases operations.

- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.

- If the legal documents indicate that users' personal information is deleted within a reasonable time frame (keeping in mind that the rotation of backups can add some delay to full deletion of information) of the termination of a user's account with the service, mark **PASS**.

- If the legal documents indicate that personal information is deleted within a reasonable time frame of the service ceasing operations, mark **PASS**.

- If only one of the above two situations pertains, mark **PARTIAL PASS**.

- If the legal documents do not mention what happens in either of those circumstances, mark **FAIL**.

Threat Notification

Criteria: The company notifies appropriate authorities and those affected when a data breach occurs.

See the test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ **INDICATORS**

1. The company will notify the relevant authorities without undue delay when a data breach occurs.
2. The company clearly discloses its process for notifying data subjects who might be affected by a data breach.
3. The company clearly discloses what kinds of steps it will take to address the impact of a data breach on its users.

Methodology for Assessing Each Indicator

1) The company will notify the relevant authorities without undue delay when a data breach occurs.

- Obtain and review the company's legal documents, particularly their privacy policy, usually available on the company's website.
- Look for information about how the company will respond to a data breach.
    - Note that the term "breach" is unique enough that doing a web search for it, confined to the website of the manufacturer, can be useful.

- Most states require notification of a data breach to affected residents "as expediently as possible" while others require notification within a certain time frame, such as 45 or 60 days. In most cases, delay is permitted if it is in the service of ascertaining the scope of the breach and restoring the integrity of the affected systems.

- If the legal documents indicate that the company will notify the relevant authorities within a timeframe that allows for investigation into and remediation of the breach, mark **PASS**.

- If the legal documents indicate that the company will notify the relevant authorities but does not commit to any time frame for doing so, mark **PARTIAL PASS**.

- If the legal documents contain no commitment to inform relevant authorities in the event of a data breach, mark **FAIL**.

2) The company clearly discloses its process for notifying data subjects who might be affected by a data breach.

- Obtain and review the company's legal documents, particularly their privacy policy, usually available on the company's website.

- Look for descriptions of the company's data breach practices, particularly for notification of individuals affected by the breach (as opposed to notification of government authorities).

    - Note that the term "breach" is unique enough that doing a web search for it, confined to the website of the manufacturer, can be useful.

- If the legal documents disclose how the company plans to act in the case of a data breach, including details about when and how individual data subjects will be informed of the breach, mark **PASS**.

- If the legal documents do not clearly disclose the company's process for responding to a data breach, mark **FAIL**.

    - Note that it is not enough for a company to simply state that affected data subjects will be informed. Some greater level of detail is required to pass this indicator.

3) The company clearly discloses what kinds of steps it will take to address the impact of a data breach on its users.

- Obtain and review the company’s legal documents, particularly their privacy policy, usually available on the company’s website.

- Look for descriptions of the company’s data breach practices, particularly regarding what the company will do in the event of a data breach to address the impact of a breach on its users.

    - Note that the term “breach” is unique enough that doing a web search for it, confined to the website of the manufacturer, can be useful.

    - Some examples of steps a company might take include paying for credit monitoring and restitution for any monetary losses due to the breach.

- If the company’s legal documents describe what steps the company would take to address the impact of a data breach on users, mark **PASS**.

- If the company does not mention any steps the company would take to address the impact of a data breach, mark **FAIL**.

User Notification About Third-Party Requests for User Information

Criteria: The company tells me if the government or other third parties ask for my information.

See the test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ INDICATORS

1. The company notifies users when government entities (including courts or other judicial bodies) request their user information.
2. The company notifies users when private parties request their user information.
3. The company clearly discloses situations when it might not notify users, including a description of the types of government requests it is prohibited by law from disclosing to users.

Methodology for Assessing Each Indicator

1) The company notifies users when government entities (including courts or other judicial bodies) request their user information.

- Obtain and review the company's legal documents, particularly their privacy policy, usually available on the company's website.
- Look for a commitment within the legal documents to inform users when a government entity requests their personal information or information associated with their user account.

- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.

- If the legal documents commit to notifying the user when government entities request their personal information or information associated with their user account, mark **PASS**.

- If the legal documents carry no commitment to notifying the user when governmental entities request their personal information or information associated with their user account, mark **FAIL**.

2) The company notifies users when private parties request their user information.

- Obtain and review the company's legal documents, particularly their privacy policy, usually available on the company's website.

- Look for a commitment within the legal documents to inform users when a private party requests their personal information or information associated with their user account.

- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.

- If the legal documents commit to notifying the user when private parties request their personal information or information associated with their user account, mark **PASS**.

- If the legal documents carry no commitment to notifying the user when private parties request their personal information of information associated with their user account, mark **FAIL**.

3) The company clearly discloses situations when it might not notify users, including a description of the types of government requests it is prohibited by law from disclosing to users.

- Obtain and review the company's legal documents, particularly their privacy policy, usually available on the company's website.

- Look for information about when the company may not notify users of requests to access their information.

- If the legal documents are not clear about whether they apply to the "smart device" being evaluated, or only to the websites and other services of the service provider, limit grade to **PARTIAL PASS**.

- If the legal documents include a list of situations in which the company will not notify users of requests to access their information, including the types of government requests from which it is prohibited from notifying users, mark **PASS**.

- If the legal documents include a list of situations in which the company will not notify users of requests to access their information, but does not include further details, mark **PARTIAL PASS**.

- If the legal documents do not mention that the company may be prohibited from notifying users of requests to access their information, mark **FAIL**.

Transparency Reporting

Criteria: The company is transparent about its practices for sharing user data with the government and other third parties.

Note: All of the indicators in this test are predicated on the idea that the relevant company publishes a transparency report of some kind. If the company does not publish a transparency report, it will fail all of these indicators. Knowing this ahead of time may save testers the time and effort of reading through each indicator.

See the test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ **INDICATORS**

1. The company lists the number of requests it receives by country.

2. The company lists the number of requests it receives for stored user information and for real-time communications access.

3. The company lists the number of accounts affected.

4. The company lists whether a demand sought communications content or non-content or both.

5. The company identifies the specific legal authority or type of legal process through which law enforcement and national security demands are made.

6. The company includes requests that come from court orders.

7. The company lists the number of requests it receives from private parties.

8. The company lists the number of requests it complied with, broken down by category of demand.

9. The company lists what types of government requests it is prohibited by law from disclosing.

10. The company reports this data at least once per year.

11. The data reported by the company can be exported as a structured data file.

Methodology for Assessing Each Indicator

1) The company lists the number of requests it receives by country.

- Locate the company's transparency report, if it produces one.
    - The transparency report will likely be located in the same section of the website as the other legal documents such as the privacy policy and terms of service, however some companies place them in their own section.
    - A web search can also help find the transparency report if it is not in an obvious location on the company's website.
- If there is a transparency report, see if it includes statistical information regarding requests for user data.
- In the transparency report, see if the tabulations of government requests are broken out by requesting country or grouped together.
- If the numbers of requests are not broken out by country, see if the transparency report states elsewhere that the company has received no requests or only received requests from one government.
- If the company received no requests, only received requests from one named country, or breaks out requests by requesting government, mark **PASS**.
- If the company does not break out requests by requesting government, or make clear that all requests were from one particular government, mark **FAIL**.

2) The company lists the number of requests it receives for stored user information and for real-time communications access.

- Locate the company’s transparency report, if it produces one.
    - The transparency report will likely be located in the same section of the website as the other legal documents such as the privacy policy and terms of service, however some companies place them in their own section.
    - A web search can also help find the transparency report if it is not in an obvious location on the company’s website.
- If there is a transparency report, see if it includes statistical information regarding requests for user data.
- In the transparency report, look for how the company distinguishes the requests it receives for user information.
- If the transparency report counts requests for stored user information (which may also be referred to as past data) separately from user information collected in real time, mark **PASS**.
- If the transparency report does not distinguish between stored and real-time user information, mark **FAIL**.

3) The company lists the number of accounts affected.

- Locate the company’s transparency report, if it produces one.
    - The transparency report will likely be located in the same section of the website as the other legal documents such as the privacy policy and terms of service, however some companies place them in their own section.
    - A web search can also help find the transparency report if it is not in an obvious location on the company’s website.
- If there is a transparency report, see if it includes statistical information regarding requests for user data.
- In the transparency report, look for a column of numbers detailing how many accounts were implicated in requests for user information, as distinguished from the sheer number of requests received.

- If the transparency report lists the number of accounts involved in requests for user data separately from the number of requests received, mark **PASS**.

- If the transparency report does not list the number of accounts affected by requests for user data, mark **FAIL**.

4) The company lists whether a demand sought communications content or non-content or both.

- Locate the company's transparency report, if it produces one.

    ◦ The transparency report will likely be located in the same section of the website as the other legal documents such as the privacy policy and terms of service, however some companies place them in their own section.

    ◦ A web search can also help find the transparency report if it is not in an obvious location on the company's website.

- If there is a transparency report, see if it includes statistical information regarding requests for user data.

- Look in the transparency report for a distinction between requests for content and requests for non-content data.

    ◦ Non-content information may be referred to as "metadata" and is information about a communication such as time and date, length, or the parties to the communication.

    ◦ In some cases, the distinction between content and non-content may not be relevant to a given product. For example, some products and services will not generate communications content information. In that case, the company should specify that any requests received for user information were for, e.g., non-content information.

- If the transparency report lists the number of requests for both content and non-content types of data, or if it lists only numbers for one type along with a note that the company does not collect the other type, mark **PASS**.

- If the transparency report does not distinguish between requests for non-content and content, mark **FAIL**.

5) The company identifies the specific legal authority or type of legal process through which law enforcement and national security demands are made.

- Locate the company's transparency report, if it produces one.
    - The transparency report will likely be located in the same section of the website as the other legal documents such as the privacy policy and terms of service, however some companies place them in their own section.
    - A web search can also help find the transparency report if it is not in an obvious location on the company's website.
- If there is a transparency report, see if it includes statistical information regarding requests for user data.
- Look for whether the transparency report separates numbers of requests by what legal authority the request was made under.
    - Commonly this will take the form of the header of a column or row (depending on how the table is formatted) listing a type of authority such as "subpoena" or "National Security Letter."
    - Note that this information may be in a different table than the primary transparency report table, which may only list high-level aggregations.
- If the company groups requests by the specific legal authority under which they were made, mark **PASS**.
- If the company does not group requests by specific legal authority, mark **FAIL**.

6) The company includes requests that come from court orders.

- Locate the company's transparency report, if it produces one.
    - The transparency report will likely be located in the same section of the website as the other legal documents such as the privacy policy and terms of service, however some companies place them in their own section.

    - A web search can also help find the transparency report if it is not in an obvious location on the company's website.

- If there is a transparency report, see if it includes statistical information regarding requests for user data.

- Read the transparency report looking for indications that the company has included requests for user information that were made under the authority of an established court.

    - Some terms to look for include "subpoena," "warrant," and "discovery."

- If the transparency report includes requests that were made pursuant to a court order, mark **PASS**.

- If the transparency report does not include such requests, mark **FAIL**.

7) The company lists the number of requests it receives from private parties.

- Locate the company's transparency report, if it produces one.

    - The transparency report will likely be located in the same section of the website as the other legal documents such as the privacy policy and terms of service, however some companies place them in their own section.

    - A web search can also help find the transparency report if it is not in an obvious location on the company's website.

- Look for indications in the transparency report of requests from parties that are NOT courts or other government entities.

- If the transparency report includes statistics regarding requests made by private parties, mark **PASS**.

- If the transparency report does not include requests made by private parties, mark **FAIL**.

8) The company lists the number of requests it complied with, broken down by category of demand.

- Locate the company's transparency report, if it produces one.

    - The transparency report will likely be located in the same section of the website as the other legal documents such as the privacy policy and terms of service, however some companies place them in their own section.

    - A web search can also help find the transparency report if it is not in an obvious location on the company's website.

- If there is a transparency report, see if it includes statistical information regarding requests for user data.

- Look in the transparency report for the number of requests that it received in each category with which it complied (as opposed to those it refused to comply with for any reason).

- If the company lists the number of requests it complied with in addition to listing simply those it received, mark **PASS**.

- If the company does not list how many requests it complied with in addition to how many it received, mark **FAIL**.

9) The company lists what types of government requests it is prohibited by law from disclosing.

- Locate the company's transparency report, if it produces one.

    - The transparency report will likely be located in the same section of the website as the other legal documents such as the privacy policy and terms of service, however some companies place them in their own section.

    - A web search can also help find the transparency report if it is not in an obvious location on the company's website.

- Look in the transparency report for a description of the types of government requests the company is prohibited by law from disclosing.

    - Some laws prohibit the recipients of demands for customer data from even revealing the existence of the demand itself (sometimes called a ”nondisclosure order" or "gag order"). This indicator is testing whether the company informs the public about the fact of such a gag order.

    - This information will likely not be in table format along with the rest of the numbers in a transparency report, so look for it in the written language surrounding the report.

- If the transparency report includes information on what types of government requests it is prohibited from listing, mark **PASS**.

- If the transparency report does not include information about requests it is prohibited from including in its numbers, mark **FAIL**.

10) The company reports this data at least once per year.

- Locate the company's transparency report, if it produces one.

    - The transparency report will likely be located in the same section of the website as the other legal documents such as the privacy policy and terms of service, however some companies place them in their own section.

    - A web search can also help find the transparency report if it is not in an obvious location on the company's website.

- Look in the transparency report for indications of how often the company releases a report.

    - Ideally, look for links to older reports and determine if they have been released annually or more frequently.

    - Also look for a commitment from the company to release transparency reports on a given timetable

- If the transparency report has been released in the past on at least an annual basis, or if the company has only released one transparency report, but commits to doing so annually, mark **PASS**.

- If the company has released a transparency report on a regular time table in the past, but has not always done so precisely on an annual basis, mark **PARTIAL PASS**.

- If the company has released transparency reports in the past but not on an annual basis, mark **FAIL**.

11) The data reported by the company can be exported as a structured data file.

- Locate the company's transparency report, if it produces one.
    - The transparency report will likely be located in the same section of the website as the other legal documents such as the privacy policy and terms of service, however some companies place them in their own section.
    - A web search can also help find the transparency report if it is not in an obvious location on the company's website.
- Look in the transparency report page for a means to download the data that makes up the transparency report as structured data.
    - Structured data is data that is formatted to be read and analyzed easily by a computer.
    - Most commonly, these files will be in a comma-separated values (csv) file, but they may also be in "json" format or even as Microsoft Excel files.
- If the transparency report is available to download in a structured data format, mark **PASS**.
- If the transparency report is not available for download in a structured data format, mark **FAIL**.

Governance

Criteria:

1. The company or organization publicly commits to respect users' human rights to freedom of expression and privacy.

2. The company or organization's senior leadership exercises oversight over how its policies and practices affect freedom of expression and privacy.

3. The company or organization should have mechanisms in place to implement its commitments to freedom of expression and privacy internally.

4. The company or organization implements due diligence processes, such as human rights impact assessments, to identify how all aspects of its activities affect freedom of expression and privacy and to mitigate any risks posed by those impacts.

5. The company or organization engages with a range of stakeholders on freedom of expression and privacy issues.

6. The company or organization should have grievance and remedy mechanisms to address user's freedom of expression and privacy concerns.

See this test in action:

- **Smart lock**

- **Smart pressure cooker**

- **Smart baby monitor**

→ INDICATORS

1. Explicit and clearly articulated policy commitment to human rights, including freedom of expression and privacy.

2. The board of directors exercises formal oversight over how company practices affect freedom of expression and privacy.

3. An executive-level committee, team, program, or officer, oversees how company practices affect freedom of expression and privacy.

4. A management-level committee, team, program, or officer, oversees how company practices affect freedom of expression and privacy.

5. Provides employee, volunteers, or other staff, training on freedom of expression and privacy issues.

6. Maintains a whistleblower program through which employees, volunteers or other staff can report concerns related to how the company treats its users' freedom of expression and privacy rights.

7. As part of its decision-making, considers how laws affect freedom of expression and privacy in jurisdictions where it operates.

8. Regularly assesses free expression and privacy risks associated with existing products and services.

9. Assesses free expression and privacy risks associated with a new activity, including the launch and/or acquisition of new products or services or entry into new markets.

10. Assesses free expression and privacy risks associated with the processes and mechanisms used to enforce its Terms of Service.

11. Conducts in-depth due diligence wherever the company's risk assessments identify concerns.

12. Senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in decision-making for the company.

13. Conducts assessments on a regular schedule.

14. The company initiates or participates in meetings with stakeholders that represent, advocate on behalf of, or are people directly and adversely impacted by the company's business.

15. Clear disclosure of processes for receiving complaints.

16. Clear disclosure of process for responding to complaints.

17. The company reports on the number of complaints received.

18. The company provides evidence that it is responding to complaints.

Methodology for Assessing Each Indicator

1) Explicit and clearly articulated policy commitment to human rights, including freedom of expression and privacy.

- Obtain and review any documentation that the company has available that may discuss human rights. This could be found on the company's website, or in documentation included with a physical device.

- This information, if it exists, may be found in the:

    - Company human rights policy

    - Privacy policy

    - Company statements, reports, or other communications that reflect official company policy

    - Regulatory documents (e.g. U.S. Federal Trade Commission)

    - Reports from third-party assessors or accreditors

    - Global Network Initiative commitments or assessment reports

    - Company annual report or sustainability report that refers to official policy documents

- Look for language discussing human rights, freedom of expression, and/or privacy.

- If the company discloses this human rights policy commitment in formal policy documents or in other communications that reflect official company policy, mark **PASS**.

- If the company does not disclose this policy commitment in formal policy documents or in other communications that reflect official company policy, mark **FAIL**.

2) The board of directors exercises formal oversight over how company practices affect freedom of expression and privacy.

- Obtain and review any documentation that the company has available that may discuss human rights as well as any documentation explaining the roles and responsibilities of the board of directors. This could be found on the company's website, or in documentation included with a physical device.

- This information, if it exists, may be found in the:

    - Corporate and board governance documents

    - Company human rights policy

    - Company statements, reports, or other communications that reflect official company policy

    - Regulatory documents (e.g. U.S. Federal Trade Commission)

    - Reports from third-party assessors or accreditors

    - Global Network Initiative commitments or assessment reports

    - Company annual report or sustainability report that refers to official policy documents

- Look for text regarding oversight processes, specifically by a board of directors, if the company has one.

- If the company discloses information about board of director oversight processes in formal policy documents or in other communications that reflect official company policy on free expression and privacy, mark **PASS**.

- If the company does not disclose information about board of director oversight processes in formal policy documents or in other communications that reflect such official company policy, mark **FAIL**.

3) An executive-level committee, team, program or officer oversees how company practices affect freedom of expression and privacy.

- Obtain and review any documentation that the company has available regarding the responsibilities of the board of directors or other company officials and any documentation that may discuss human rights. This could be found on the company’s website, or in documentation included with a physical device.

- This information, if it exists, may be found in the:
    - Corporate and board governance documents
    - Company human rights policy
    - Company statements, reports, or other communications that reflect official company policy
    - Regulatory documents (e.g. U.S. Federal Trade Commission)
    - Reports from third-party assessors or accreditors
    - Global Network Initiative commitments or assessment reports
    - Company annual report or sustainability report that refers to official policy documents
- Look for text regarding oversight processes, specifically by an executive-level committee, team, program, or officer.
- If the company discloses information about oversight processes regarding free expression and privacy by the above group of individuals in formal policy documents or in other communications that reflect official company policy, mark **PASS**.
- If the company does not disclose information about such oversight processes by the above group of individuals in formal policy documents or in other communications that reflect official company policy, mark **FAIL**.

4) A management-level committee, team, program or officer oversees how company practices affect freedom of expression and privacy.

- Obtain and review any documentation that the company has available regarding the responsibilities of company leadership and officials and any documentation that may discuss human rights. This could be found on the company’s website, or in documentation included with a physical device.
- This information, if it exists, may be found in the:
    - Company governance documents

    - Company human rights policy
    - Company statements, reports, or other communications that reflect official company policy
    - Regulatory documents (e.g. U.S. Federal Trade Commission)
    - Reports from third-party assessors or accreditors
    - Global Network Initiative commitments or assessment reports
    - Company annual report or sustainability report that refers to official policy documents

- Look for text regarding oversight processes, specifically by a management-level committee, team, program, or officer.

- If the company discloses information about oversight processes on free expression and privacy by the above group of individuals in formal policy documents or in other communications that reflect official company policy, mark **PASS**.

- If the company does not disclose information about such oversight processes by the above group of individuals in formal policy documents or in other communications that reflect official company policy, mark **FAIL**.

5) Provides employee, volunteers or other staff training on freedom of expression and privacy issues.

- Obtain and review any documentation that the company has available that may discuss freedom of expression or privacy training for employees. This could be found on the company's website including in sections providing information for new or potential employees, or in documents elsewhere about company policies.

- This information, if it exists, may be found in the:

    - Company code of conduct
    - Employee handbook
    - Company organizational chart
    - Company CSR/sustainability report

    - Company human rights policy
    - Company statements, reports, or other communications that reflect official company policy
    - Regulatory documents (e.g. U.S. Federal Trade Commission)
    - Reports from third-party assessors or accreditors
    - Global Network Initiative commitments or assessment reports
    - Company annual report or sustainability report that refers to official policy documents

- If the company discloses that they provide such trainings in formal policy documents or in other communications that reflect official company policy, mark **PASS**.

- If the company does not disclose that they provide such trainings in formal policy documents or in other communications that reflect official company policy, mark **FAIL**.

6) Maintains a whistleblower program through which employees, volunteers or other staff can report concerns related to how the company treats its users' freedom of expression and privacy rights.

- Obtain and review any documentation that the company has available that may discuss whistleblower programs. This could be found on the company's website, including in sections providing information for employees, or in documents elsewhere about company policies.

- This information, if it exists, may be found in the:
    - Company code of conduct
    - Employee handbook
    - Company organizational chart
    - Company CSR/sustainability report
    - Company human rights policy

    - Company statements, reports, or other communications that reflect official company policy
    - Regulatory documents (e.g. U.S. Federal Trade Commission)
    - Reports from third-party assessors or accreditors
    - Global Network Initiative commitments or assessment reports

- If the company discloses that they maintain a whistleblower program in formal policy documents or in other communications that reflect official company policy, mark **PASS**.

- If the company does not disclose that they maintain a whistleblower program in formal policy documents or in other communications that reflect official company policy, mark **FAIL**.

7) As part of its decision-making, considers how laws affect freedom of expression and privacy in jurisdictions where it operates.

- Obtain and review any documentation that the company has available that may discuss human rights impact assessments, or other human rights practices or evaluations. This could be found on the company's website:
    - Company human rights policy
    - Company statements, reports, or other communications that reflect official company policy
    - Regulatory documents (e.g. U.S. Federal Trade Commission)
    - Reports from third-party assessors or accreditors
    - Global Network Initiative commitments or assessment reports
    - Company annual report or sustainability report that refers to official policy documents

- If there is such documentation, review company documents to see if there is any information about how it conducts and uses those human rights assessments, whether it considers the impact of laws in jurisdictions where the company operates, and whether they affect decision-making processes.

- If the company discloses that it considers how laws in local jurisdictions affect freedom of expression and privacy as part of its decision-making process in formal policy documents or in other communications that reflect official company policy, mark **PASS**.

- If the company does not disclose that it considers how laws affect freedom of expression and privacy as part of its decision-making process in formal policy documents or in other communications that reflect official company policy, mark **FAIL**.

8) Regularly assesses free expression and privacy risks associated with existing products and services.

- Obtain and review any documentation that the company has available that may discuss human rights impact assessments, or other human rights practices or evaluations. This could be found on the company's website:

    - Company human rights policy

    - Company statements, reports, or other communications that reflect official company policy

    - Regulatory documents (e.g. U.S. Federal Trade Commission)

    - Reports from third-party assessors or accreditors

    - Global Network Initiative commitments or assessment reports

    - Company annual report or sustainability report that refers to official policy documents

- If there is such documentation, review company documents to see if there is any information about when it conducts and how it uses human rights assessments, and if they are conducted regularly on existing products and services.

- If the company discloses that it regularly conducts assessments measuring risks to freedom of expression and privacy from existing products and services in formal policy documents or in other communications that reflect official company policy, mark **PASS**.

- If the company does not disclose that it regularly conducts freedom of expression and privacy evaluations on existing products and services in formal policy documents or in other communications that reflect official company policy, mark **FAIL**.

9) Assesses free expression and privacy risks associated with a new activity, including the launch and/or acquisition of new products or services or entry into new markets.

- Obtain and review any documentation that the company has available that may discuss human rights impact assessments, or other human rights practices or evaluations. This could be found on the company's website:
    - Company human rights policy
    - Company statements, reports, or other communications that reflect official company policy
    - Regulatory documents (e.g. U.S. Federal Trade Commission)
    - Reports from third-party assessors or accreditors
    - Global Network Initiative commitments or assessment reports
    - Company annual report or sustainability report that refers to official policy documents
- If there is such documentation, review company documents to see if there is any information about when it conducts assessments of risks to free expression and privacy, and if they are conducted before engaging in a new activity, including the launch and/or acquisition of new products or services or entry into new markets.
- If the company discloses that it conducts freedom of expression and privacy evaluations before engaging in a new activity, including the launch and/or acquisition of new products or services or entry into new markets in formal policy documents or in other communications that reflect official company policy, mark **PASS**.
- If the company does not disclose that it conducts freedom of expression and privacy evaluations before engaging in a new activity, including the launch and/or acquisition of new products or services or entry into new markets in formal policy documents or in other communications that reflect official company policy, mark **FAIL**.

10) Assesses free expression and privacy risks associated with the processes and mechanisms used to enforce its Terms of Service.

- Obtain and review any documentation that the company has available that may discuss human rights impact assessments, or other human rights practices or evaluations related to the company's Terms of Service. This could be found on the company's website:
    - The Terms of Service themselves
    - Company human rights policy
    - Company statements, reports, or other communications that reflect official company policy
    - Regulatory documents (e.g. U.S. Federal Trade Commission)
    - Reports from third-party assessors or accreditors
    - Global Network Initiative commitments or assessment reports
    - Company annual report or sustainability report that refers to official policy documents
- If there is such documentation, review company documents to see if there is any information about when it conducts free expression and privacy assessments, specifically whether they are used to assess risks associated with the processes and mechanisms used to enforce its terms of service.
- If the company discloses that it assesses free expression and privacy risks associated with the processes and mechanisms used to enforce its terms of service in formal policy documents or in other communications that reflect official company policy, mark **PASS**.
- If the company does not disclose that it assesses free expression and privacy risks associated with the processes and mechanisms used to enforce its terms of service in formal policy documents or in other communications that reflect official company policy, mark **FAIL**.

11) Conducts in-depth due diligence wherever the company's risk assessments identify concerns.

- Obtain and review any documentation that the company has available that may discuss human rights impact assessments, or other human rights practices or evaluations. This could be found on the company's website:
    - Company human rights policy
    - Company statements, reports, or other communications that reflect official company policy
    - Regulatory documents (e.g. U.S. Federal Trade Commission)
    - Reports from third-party assessors or accreditors
    - Global Network Initiative commitments or assessment reports
    - Company annual report or sustainability report that refers to official policy documents
- If there is such documentation, review company documents to see if there is any information about when it conducts human rights risk assessments, and how any concerns raised by those assessments would be addressed.
- If the company discloses that it conducts due diligence regarding concerns raised in any risk assessments in formal policy documents or in other communications that reflect official company policy, mark **PASS**.
- If the company does not disclose that it conducts due diligence regarding concerns raised in any risk assessments in formal policy documents or in other communications that reflect official company policy, mark **FAIL**.

12) Senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in decision-making for the company.

- Obtain and review any documentation regarding the responsibilities of the board of directors or other company officials and any documentation that the company has available that may discuss human rights impact assessments, or other human rights practices or evaluations. This could be found on the company's website:
    - Corporate and board governance documents
    - Company human rights policy

    - Company statements, reports, or other communications that reflect official company policy

    - Regulatory documents (e.g. U.S. Federal Trade Commission)

    - Reports from third-party assessors or accreditors

    - Global Network Initiative commitments or assessment reports

    - Company annual report or sustainability report that refers to official policy documents

- If there is such documentation, review company documents to see if there is any information about how it uses human rights risk assessments, and about whether they affect decision-making processes.

- Review documents to see who may review these assessments and would conduct due diligence.

- If the company discloses that senior executives and/or members of the company's board of directors review and consider the results of human rights impact/other assessments and due diligence in decision-making for the company, mark **PASS**.

- If the company does not disclose that senior executives and/or members of the company's board of directors review and consider the results of human rights impact/other assessments and due diligence in decision-making for the company, mark **FAIL**.

13) Conducts assessments on a regular schedule.

- Obtain and review any documentation that the company has available that may discuss human rights impact assessments, or other human rights practices or evaluations. This could be found on the company's website:

    - Company human rights policy

    - Company statements, reports, or other communications that reflect official company policy

    - Regulatory documents (e.g. U.S. Federal Trade Commission)

    - Reports from third-party assessors or accreditors

    - Global Network Initiative commitments or assessment reports
    - Company annual report or sustainability report that refers to official policy documents

- If there is such documentation, review company documents to see if there is any information about when these assessments are conducted, and if it adheres to a regular schedule.

- If the company discloses a regular timeline on which they conduct human rights impact assessments, mark **PASS**.

- If the company does not disclose a regular timeline on which they conduct human rights impact assessments, mark **FAIL**.

14) The company initiates or participates in meetings with stakeholders that represent, advocate on behalf of, or are people directly and adversely impacted by the company's business.

- Obtain and review any documentation that the company has available that may discuss human rights impact assessments, or other human rights practices or evaluations, or any other efforts to engage with stakeholders interested in the human rights impacts of the company's products and services. This could be found on the company's website:
    - Annual or other reports describing the company's activities
    - Company human rights policy
    - Company statements, reports, or other communications that reflect official company policy
    - Regulatory documents (e.g. U.S. Federal Trade Commission)
    - Reports from third-party assessors or accreditors
    - Global Network Initiative commitments or assessment reports
    - Company annual report or sustainability report that refers to official policy documents

- Look for language regarding stakeholder engagement or consultation.

- If the company discloses that they regularly consult stakeholders that represent, advocate on behalf of, or are people directly and adversely affected by the company's business, mark **PASS**.

- If the company does not disclose that they regularly consult stakeholders that represent, advocate on behalf of, or are people directly and adversely affected by the company's business, mark **FAIL**.

15) Clear disclosure of processes for receiving complaints.

- Obtain and review any documentation that the company has available that may discuss any process through which customers or others may submit complaints to the company, as well as those concerning human rights impact assessments, or other human rights practices or evaluations. This could be found on the company's website:

    - Help page

    - Company human rights policy

    - Company statements, reports, or other communications that reflect official company policy

    - Regulatory documents (e.g. U.S. Federal Trade Commission)

    - Reports from third-party assessors or accreditors

    - Global Network Initiative commitments or assessment reports

    - Company annual report or sustainability report that refers to official policy documents

- If there is such documentation, review company documents to see if there is any information about a process for receiving complaints. Note that this process might be for complaints of all kinds.

- If there is a complaints process, review whether the procedure specifically identifies it as the mechanism for complaints regarding free expression and privacy concerns.

- If the company discloses that they have a process for receiving complaints,specifically related to issues of free expression and privacy, mark **PASS**.

- If the company discloses that they have a process for receiving all types of complaints, mark **PARTIAL PASS**.

- If the company does not disclose that they have a process for receiving complaints, mark **FAIL**.

16) Clear disclosure of process for responding to complaints.

- Obtain and review any documentation that the company has available that may discuss any process through which customers or others may submit complaints to the company, as well as those concerning human rights impact assessments, or other human rights practices or evaluations. This could be found on the company's website:

    - Help page

    - Company human rights policy

    - Company statements, reports, or other communications that reflect official company policy

    - Regulatory documents (e.g. U.S. Federal Trade Commission)

    - Reports from third-party assessors or accreditors

    - Global Network Initiative commitments or assessment reports

    - Company annual report or sustainability report that refers to official policy documents

- If there is such documentation, review company documents to see if there is any information about a process for responding to complaints it receives.

- If there is a process, review whether the process would include complaints regarding free expression and privacy concerns.

- If the company discloses that they have a process for responding to free expression and privacy complaints it receives, **PASS**.

- If the company discloses that they have a process for responding to general complaints it receives, mark **PARTIAL PASS**.

- If the company does not disclose that they have a process for responding to complaints it receives, mark **FAIL**.

17) The company reports on the number of complaints received.

- Obtain and review any documentation that the company has available that may discuss human rights impact assessments, or other human rights practices or evaluations. This could be found on the company's website:
    - Transparency reports
    - Company human rights policy
    - Company statements, reports, or other communications that reflect official company policy
    - Regulatory documents (e.g. U.S. Federal Trade Commission)
    - Reports from third-party assessors or accreditors
    - Global Network Initiative commitments or assessment reports
    - Company annual report or sustainability report that refers to official policy documents
- Review company documents for information and statistics describing the number of complaints received.
- If the company reports on the number of complaints received, mark **PASS**.
- If the company does not report the number of complaints received, mark **FAIL**.

18) The company provides evidence that it is responding to complaints.

- Obtain and review any documentation that the company has available that may discuss human rights impact assessments, or other human rights practices or evaluations. This could be found on the company's website:
    - Transparency
    - Company human rights policy

    - Company statements, reports, or other communications that reflect official company policy
    - Regulatory documents (e.g. U.S. Federal Trade Commission)
    - Reports from third-party assessors or accreditors
    - Global Network Initiative commitments or assessment reports
    - Company annual report or sustainability report that refers to official policy documents

- If yes, review company documents to see if there is any information about a process for responding to complaints it receives.

- Review company documents to see if there are examples or evidence of cases where it has responded to complaints it receives.

- If the company discloses examples or evidence of cases where it has responded to complaints it receives, mark **PASS**.

- If the company does not disclose examples or evidence of cases where it has responded to complaints it receives, mark **FAIL**.

Open Source

Criteria: The product's software is publicly available.

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ INDICATORS

1. Software is open source, meaning published under a license approved and listed by the Open Source Initiative. (**https://opensource.org/licenses/alphabetical**)

Methodology for Assessing Each Indicator

1) Software is open source, meaning published under a license approved and listed by the Open Source Initiative. (https://opensource.org/licenses/alphabetical)

- Obtain and review any documentation that the company has available on its website or packaged with a physical product. This could be listed somewhere like "policies" or elsewhere in blog posts or company statements.
- Look for language describing open source software or any kind of license.
- If the company discloses that they use open source software and lists the relevant license, mark **PASS**.
- If the company does not disclose that they use open source software or does not list the relevant license, mark **FAIL**.

Interoperability

Criteria: The company does not prohibit use of the product with other, complementary products.

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ **INDICATORS**

1. The manufacturer does not use software, copyright, or other devices to restrict the use of products and services that would otherwise be possible to use with your existing products (e.g., set-top boxes, third party applications, etc.).

Methodology for Assessing Each Indicator

1) The manufacturer does not use software, copyright, or other devices to restrict the use of products and services that would otherwise be possible to use with your existing products (e.g., set-top boxes, third party applications, etc.).

- Gather information from online sources, searching for indications as to whether the manufacturer exerts control over the ability for products or services developed by third parties to interact or interoperate with the product. These can be either indications that the manufacturer seeks to prohibit or to promote such as:
    - Prohibitions in the product's warranty or terms of service on using another device or service to connect to, interact with, "scrape," or otherwise interoperate with the product.

    - News articles about the manufacturer attempting to stop people from interoperating their product with other products either through legal action or changes to the hardware or software of the product.

    - News articles about anyone “cracking” or “getting root” on the product, which may indicate that the manufacturer chose to make use of software designed to prohibit interoperability, causing customers to break or remove that software in order to achieve interoperability.

    - Indications on the manufacturer’s website that they promote interoperability, such as a “developer’s” page or a description of the product’s Application Programming Interface (API).

    - Online advertisements for other products that describe themselves as working with the product being reviewed.

- If the manufacturer promotes interoperability with the product, either through affirmative statements or through the existence of APIs or other developer documentation, mark **PASS**.

- If there is evidence of other products being designed and marketed to interoperate with the product, mark **PASS**.

- If there is some evidence to give the product a PASS for this indicator, but there are not enough details publicly available to implement that interoperability in another product, mark **PARTIAL PASS**.

- If there is no evidence of the manufacturer’s stance toward interoperability in its products, either for or against, but the device can be connected to other devices such as a smart speaker or home assistant, mark **PARTIAL PASS**.

- If there is evidence of the manufacturer prohibiting interoperability either in legal documents or through legal or technical action, mark **FAIL**.

- If there is evidence of third parties hacking the product to remove software controls, attempt to ascertain through further research what purpose those controls served and if the purpose is squarely aimed at preventing interoperability, mark **FAIL**.

Ownership

Criteria: When I buy a product, I own every part of it.

See this test in action

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

Notes:

- *This test and accompanying indicator suffer from significant vagueness in their language. It is not clear what degree of control by the manufacturer (if any) over the product would be acceptable in order to pass this indicator. Many (if not most) consumer IoT devices are connected to cloud services run by the manufacturer in order to operate as desired by the purchaser, and that connection will give the manufacturer de facto control of the product. Even if a manufacturer has no desire or intent to withhold control or ownership, this indicator explicitly measures the retaining of control and not the intent to exercise it.*

→ INDICATORS

1. The company does not retain any control or ownership over the operation, use, inputs, or outputs of the product after it has been purchased by the consumer.

Methodology for Assessing Each Indicator

1) The company does not retain any control or ownership over the operation, use, inputs, or outputs of the product after it has been purchased by the consumer.

- Examine operation of product to determine whether control of its functions are routed through or otherwise dependent on connection to the manufacturer.
    - E.g. If the product has a connected mobile phone app, use network analysis tools to determine whether the mobile device and the product communicate directly or through a third server on the internet.
    - *Note: A great number of the "smart" products sold today require a connection to a server managed by the manufacturer, meaning that most of them will fail this indicator.*
- Review the product's legal documents looking for any claims either explicit or implicit by the manufacturer of the ability to unilaterally terminate or modify the functionality of the product in any way.
- If there is no evidence of the manufacturer's ability to deny the owner the full control over the device, mark **PASS**.
- If evidence of the ability to deny the owner of full control over the device is found, mark **FAIL**.

Resale

Criteria: I can resell the product to someone and it will still work.

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ INDICATORS

1. If a consumer sells the product on the private market, the new owner has access to the full functionality of the original product.
2. The company does not restrict the transfer of ownership.

Methodology for Assessing Each Indicator

1) If a consumer sells the product on the private market, the new owner has access to the full functionality of the original product.

- Read the product's legal documents, particularly the terms of service.
- Search the manufacturer's website for terms such as "sale" or "transfer."
- Search the manufacturer's help documentation or "frequently asked questions" for instructions on how to "wipe" or "factory reset" the product.
- Look for language describing the purchaser's ability to reassign or sell the product, the software that runs on the product, or software which is required in order to use the product.
- Look for information about how to activate the product and set up a new account after a second-hand purchase.

- If there is any indication that second-hand purchasers can take the same or similar steps to activate the product as a new purchaser would, mark **PASS**.

- If the legal documents or other language indicates that resale is prohibited, or if there is no indication that second-hand purchasers can take the same or similar steps to activate the product as a new purchaser would, mark **FAIL**.

2) The company does not restrict the transfer of ownership.

- Read the product's legal documents, particularly the terms of service.

- Search the manufacturer's website for terms such as "sale" or "transfer."

- Search the manufacturer's help documentation or "frequently asked questions" for instructions on how to "wipe" or "factory reset" the product.

- Look for language describing the purchaser's ability to reassign or sell the product, the software that runs on the product, or software which is required in order to use the product.

- Look for information about what happens to a purchaser's associated account if they sell the product, or how a second-hand purchaser can reset or "wipe" the product after buying it.

- If there is an affirmative statement of the purchaser's right to sell the product, or if the documents describe what happens in the case of sale of the product, mark **PASS**.

- If there is no such affirmative statement but there are also no limitations on the sale of the product, mark **PARTIAL PASS**.

- If the legal documents explicitly prohibit the sale or transfer of the product, mark **FAIL**.

Functionality Over Time

Criteria: The company commits to maintain the intended functionality of the product for a clearly defined and communicated period of time (i.e., the product life cycle).

See the test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ **INDICATORS**

1. The product life cycle is communicated to the potential owner before purchase.
2. Every feature of the product will continue to work the stated product life cycle; that is, the manufacturer will not 'brick' certain parts of the product during that time frame.
3. The manufacturer will not cease to support the functionality I come to expect during the product life cycle.
4. Replacement services will exist if the manufacturer ceases to support the functionality during the product life cycle.
5. The company commits that, in the event the company is sold or acquired, the new owner will maintain the intended functionality for the full product life cycle.

Methodology for Assessing Each Indicator

1) The product life cycle is communicated to the potential owner before purchase.

- Look at the places that a potential purchaser would have access to before deciding to buy the product, such as the company's product page and purchase page, terms of service, end user license, and warranty pages as well as the external packaging and labeling of the product.

- If the product is produced by, a composite of, or maintained by two or more companies, search for life cycle information on all companies' websites.

- Search for indications of the expected life cycle of the product.

    - Warranties, while a similar concept, are not what this indicator is evaluating

    - This indicator is assessing continued functionality, not just avoidance of breakage.

- If the company indicates in such a way that a prospective purchaser could view that the product and associated services will continue to work for a certain amount of time, particularly if the product relies upon a continuing service operated by the company, mark **PASS**.

- If the company does not indicate that the product and associated services will continue to work for a certain amount of time, mark **FAIL**.

2) Every feature of the product will continue to work the stated product life cycle; that is, the manufacturer will not 'brick' certain parts of the product during that time frame.

- Look in the product's legal documentation including the terms of service, warranty, or other product information or description sources, both on the product's website and in any labeling provided in the product's packaging.

- Look for any descriptions of the manufacturer's ability to discontinue a user's service or to end the functionality of any part or aspect of the product.

- If the manufacturer affirmatively asserts that it will take no action to disable customer products throughout a defined life cycle (with possible exceptions for legal reasons or for violations of the terms of service), or if it is obvious that the manufacturer does not have the ability to render the product useless, mark **PASS**.

- If such an ability is claimed by the manufacturer, or the product can obviously be made useless through unilateral action by the manufacturer, and no exception is given for the time frame of the product's life cycle, mark **FAIL**.

3) The manufacturer will not cease to support the functionality I come to expect during the product life cycle.

- Look in the product's legal documentation including the terms of service, warranty, or other product information or description sources.

- Look for any commitments by the manufacturer to support the product for a certain amount of time, including with firmware updates, new features, or security updates, or that the service the product relies upon will continue to be operated during such a time.

- If the manufacturer provides assurance of continued operation of both the physical device and the underlying service (insofar as either exist), mark **PASS**.

- If the manufacturer does not provide assurances of continued operation of both the physical device and the underlying service, mark **FAIL**.

4) Replacement services will exist if the manufacturer ceases to support the functionality during the product life cycle.

- Look in the product's legal documentation including the terms of service, warranty, or other product information or description sources.

- Attempt to locate any information about the availability of replacement services.

    - Bear in mind that manufacturers that expect to support their products throughout the lifecycle (as tested by the prior indicator), may not provide information about post-support functionality.

- If the manufacturer commits to supporting the product throughout the life cycle, mark **PASS**.

- If the manufacturer indicates that some form of replacement service will exist if the manufacturer ceases support, mark **PASS**.

- If the manufacturer does not provide any indication that some form of replacement service will exist if the manufacturer ceases support, mark **FAIL**.

5) The company commits that, in the event the company is sold or acquired, the new owner will maintain the intended functionality for the full product life cycle.

- *Note: This indicator is likely to be one that companies are unable to pass in at least some cases. If a company is acquired its management may not have any means by which to bind the new owners to continue to maintain functionality.*

- Look in the product's legal documentation including the terms of service, warranty, or other product information or description sources.

- Look in particular for any sections detailing the potential sale or acquisition of the manufacturer.

- If the manufacturer commits that any future owner of the business will maintain the product's functionality for the full product life cycle, mark **PASS**.

- If the manufacturer does not promise that any future owner of the business will maintain the product's functionality, mark **FAIL**.

Privacy by Default

Criteria: The default settings in this product prioritize my privacy; to give up privacy, I actually need to change the settings.

See the test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ **INDICATORS**

1. Targeted advertising is off by default.
2. User interface settings which are optimal for privacy are set by default.

Methodology for Assessing Each Indicator

1) Targeted advertising is off by default.

- Determine whether the product or service hosts advertising or sends ads to users.
- If the product or service hosts or sends ads, look for places where a user might be able to control privacy settings.
    - If a product has multiple interfaces, such as a mobile app, a web app, or an in-device interface, make sure to investigate all of them.
    - Privacy settings may be in a "profile" section of an app, or under the app's "settings."
    - If the manufacturer has a website that users may visit, look at the website's privacy policy for information about targeted advertising.

- If there is a privacy setting for "targeted advertising" (which may also be called "interest-based" or "behavioral" advertising), note whether the setting is on or off for a new user.

- Look in the manufacturer's legal documents for a list of how it uses user data.

    - Note whether "targeted advertising" or a similar term is listed as a possible use of user data.

- If the manufacturer does not host or display ads or if it only hosts or displays ads that are not targeted (e.g. contextual), mark **PASS**.

- If the manufacturer lists targeted advertising as a way it uses user data in its legal documents, and there is a user setting for controlling it that is set to "off" for a new user, mark **PASS**.

- If the manufacturer lists targeted advertising as a way it uses user data in its legal documents, and there is no setting for controlling it, or if there is a user setting for controlling it but it is set to "on" for a new user, mark **FAIL**.

2) User interface settings which are optimal for privacy are set by default.

- Look for places where a user might be able to control their privacy settings.

    - If a product has multiple interfaces, such as a mobile app, a web app, or an in-device interface, make sure to investigate all of them.

    - Privacy settings may be in a "profile" section of an app, or under the app's "settings."

- Identify all of the settings that could have an effect on the privacy of a user's personal information, (e.g., collection of location, sharing with third parties, or usage analytics) and note how those settings are configured for a brand new user.

- If all privacy settings identified are set by default to the choice that limits the amount of personal information shared and maximizes the user's privacy, mark **PASS**.

- If some or all of the settings identified are set by default to choices that do not maximize the user's privacy, mark **FAIL**.

- If there are no visible settings that would enable the user to control data collection or use that may affect the user's privacy, mark **FAIL**.

Best Build Practices

Criteria: The software was built and developed according to the industry's best practices for security.

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

Notes:

- *This test is only considering the Android app that is used to interact with the product. We made this choice due to the open nature of Android, and the wide availability of free tools for inspecting Android app code.*
- *These indicators speak to quality and craftsmanship that goes into the software's coding. Namely, in making sure that the code follows known best practices around secure coding. The procedural overview for these indicators however suggest looking for things that are not an exact fit for analyzing mobile app code. Mainly, since Android apps are written in Java, which handles memory descriptions limits and cleaning up memory allocation (garbage collection), looking for things like how the code handles memory is less of concern than other aspects of good coding. However, if you are evaluating a program or app written in a memory unsafe language (one in which you must do your own memory management) such as C or C++, you absolutely should check the memory handling of that code.*
- *Many Internet of Things devices have software that runs on the device itself, often this is the code that controls the actual non-internet facing part of the "thing" (i.e. the code that actually interacts with a physical lock, or turns off a water faucet). These embedded devices use low-level processors where the device's operating code is written directly to a part of the chip. You should endeavor to get a copy of this code. In testing the initial IoT device for this project, we made several different attempts to obtain it, but were ultimately unable to gain access. In many cases these types of difficulties indicate code quality (it is more secure against tampering). That said, there are more complex ways in which we could have attempted to extract the embedded codebase from a running chip; because these methods would have required specialized, expensive equipment, we have not pursued the issue for this methodology. We will update this description if we have greater success when we test additional products.*

- *For testing Android apps, you will need a copy of the app's package file (APK). For downloading APK files, we use gplaycli, which is a Python tool for searching, downloading, and updating APK files from the official Google Playstore. Information on downloading and using gplaycli can be found on the project's GitHub page:* ***https://github.com/matlink/gplaycli***.

- *In Android, apps must request permission to access data, or use hardware features of a device. Common examples of "permissions" include an app requesting access to a user's contacts, call status, or use of the camera. In addition to requesting permission to access data and features from other parts of the system, an app may set its own permissions that define how other apps can access the data it keeps and the features it provides.*

→ INDICATORS

1. The product was built with effectively implemented safety features.
2. The software does not make use of unsafe functions or libraries.
3. The software is not overly complex.

Methodology for Assessing Each Indicator

1) The product was built with effectively implemented safety features.

- *Note: If possible to obtain firmware, or other SoC code, it should be analyzed as part of this indicator. This methodology currently only focuses on Android app analysis.*

- *Note: This indicator requires three separate elements that capture various aspects of good build practice, and therefore there are three opportunities for pass/fail.*

Best build practice 1

- Obtain a copy of the Android app for the product using gplaycli.

- Obtain and install the Android Studio IDE from the Android project.

- In Android Studio, select "profile or debug APK" and select the downloaded APK file.

- In Android Studio Select the APK in the project tree window, and then select the "analyze" menu (either at the top, or with a right click), and select “inspect code.”

- The code inspection tool runs many tests against the entire project (APK), but we are primarily interested in the security warnings. To find those in the result of the scan go to "Menu -> Android -> Lint -> Security."

- If the app passes all standard security checks, mark **PASS**.

- If the app fails security linting mark **FAIL**.

Best build practice 2

- Inspect the “AndroidManifest.xml” file to see if signature-based permissions are enabled (e.g. android:protectionLevel="signature" is used in permission stanzas).

- If the app uses signature-based permissions, or does not require any special permissions, mark **PASS**.

- If the app requires special permissions, but does not use signature-based permissions mark **FAIL**.

Best build practice 3

- Inspect the “AndroidManifest.xml” file to see if data from the app can be sent to different apps. This will likely be flagged by the linter, but can also be checked by seeing if provider definitions set android:exported="false". It is also important to note whether or not the app may need to share data with another provider in order to function as intended.

- If the app protects data from being exported to other apps, mark **PASS**.

- If the app requires some data to be shared, but protects other data, mark **PASS**.

- If the app does not block data from being shared, and it is not necessary to function, mark **FAIL**.

2) The software does not make use of unsafe functions or libraries.

- *Note*: *If possible to obtain firmware, or other SoC code, it should be analyzed as part of this indicator. This methodology currently only focuses on Android app analysis.*

- Obtain a copy of the Android app for the product using gplaycli.

- Obtain and install the Android Studio IDE from the Android project.

- In Android Studio, select "Profile or debug APK" and select the downloaded APK file.

- Pull out data from the binary that speaks to coding hygiene.

    - Run the Android Studio code Linter, and note the number of errors and warnings in the "Corrections" section ("Menu -> Android -> Lint -> Corrections).

    - Also examine the results in the "General" section, and note the number of syntax errors, and other warnings.

    - If linting the app generates no errors or warnings for correctness, mark **PASS**.

    - If linting the app generates warnings, but no errors, mark **PARTIAL PASS**.

    - If linting the app generates errors for correctness and/or syntax errors, mark **FAIL**.

3) The software is not overly complex.

- *Note*: *If possible to obtain firmware, or other SoC code, it should be analyzed as part of this indicator. This methodology currently only focuses on Android app analysis. While this indicator is geared toward keeping code lean, and thus easier to review, it may be the case that an is designed for a family of products, rather than the specific product being tested. In these cases the codebase may contain libraries and functionality that are not at all needed for basic functioning of the product, but are needed for other products in the family, for example a smart lock may have a companion smart doorbell, and the same app is used to interact with both devices. It is our evaluation that this approach makes sense, and it is likely better to have developers' attention being spent on maintaining a single app well, rather than several similar apps tailored toward limited run products.*

- Pull out data from the binary that speaks to code complexity.
    - Obtain a copy of the Android for the product using gplaycli.
    - Obtain and install the Android Studio IDE from the Android project.
    - In Android Studio, select "Profile or debug APK” and select the downloaded file.
    - In Android Studio a Java class tree can be found on the left side of the window (of a default configuration). Examine the class tree and look for how many there are, including those from third-party libraries, and whether those classes are needed for the functionality of the device being tested.
    - If there are not extraneous classes in the code, mark **PASS**.
    - If there is some extraneous code to support a sibling/variant product, mark **PASS**.
    - If there are unneeded libraries or classes, mark **FAIL**.

Authentication

See the test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

Notes:

- *This test features two separate criteria by which to assess the test's success. Each criteria features a unique set of indicators and a related methodology.*
- *Thus far our development of methodologies to assess these criteria is based on analysis of Android applications. This decision is mainly based on prior experience with Android development and workflows, as well as a wider range of available research, documentation, and tooling for the Android ecosystem.*

Criteria: A product has an authentication system that corresponds to the sensitivity of the user data it manages.

→ INDICATORS

1. If a product supports user accounts, it has an authentication system for accessing those accounts.
2. If a product is packaged with an account with default credentials, those credentials are unique to the instance of the product.
3. If a product has an authentication system, the user must authenticate each time they want to use the product.
4. If a product has an authentication system, it requires at least two pieces of information to authenticate users.
5. For products that handle sufficiently sensitive data, users can choose to use multi-factor authentication.

6. For products that handle sufficiently sensitive data, users can choose to use multi-factor authentication whenever the product is activated, or when a device is unrecognized.

7. If the product uses a password/passphrase for authentication, it requires that passwords are at least 8 characters long.

8. If the product uses a password/passphrase for authentication, the password/passphrase may be at least 20 characters long.

9. If the product uses a password/passphrase for authentication, it requires that passwords are reasonably complex.

10. If the product uses a password/passphrase for authentication, it allows all reasonable characters as input.

11. If the product uses a password/passphrase for authentication, it is compatible with popular password managers.

---

1) If a product supports user accounts, it has an authentication system for accessing those accounts.

- Obtain a copy of the manufacturer's application for testing, and install it on a testing device. For these tests, it is sufficient to simply install the app directly from the relevant official app Store.

- Look for all options available to you when the app starts.

- Note if you are allowed to perform any setup, registration, configuration, preference setting, without first being required to create (or login) with an account.

- Look to see whether any information about user accounts or device settings are revealed before being required to authenticate.

- If the product does not support user accounts, mark **NA.**

- If the product supports user accounts, and requires authentication to perform any actions before it reveals information about the device, mark **PASS.**

- If the product supports user accounts but lacks a user authentication system, mark **FAIL**.

- If the product allows you to perform any actions before authentication, mark **FAIL**.

2) If a product is packaged with an account with default credentials, those credentials are unique to the instance of the product.

- Obtain a copy of the manufacturer's application for testing, and install it on a testing device. For these tests, it is sufficient to simply install the app directly from the relevant official app Store.

- Look at the instructions that came with the product, and look for a section about logging in for the first time. Note if any credentials are supplied with the documentation. If not printed in the documentation, some products' default credentials can be found on the box.

- As you examine the credentials, try to assess whether they are unique. For example, if the product's credentials use common words or phrases such as, "default," "admin," or "12345678" you can conclude they are not unique.

- If the product does not support user accounts and password-based authentication, mark **NA.**

- If the product supports accounts and passwords, but does not use default credentials at all, and the user must select and enter their own unique set of characters, mark **PASS**.

- If the product uses default credentials, but they are unique to the device, mark **PASS.**

- If the product uses common default credentials, mark **FAIL.**

3) If a product has an authentication system, the user must authenticate each time they want to use the product.

- Obtain a copy of the manufacturer's application for testing, and install it on a testing device. For these tests, it is sufficient to simply install the app directly from the relevant official app Store.

- Close out of and stop the app and then restart it several times, and note if you are required to re-enter your password and/or otherwise reauthenticate.

- If the product does not support user accounts and password-based authentication, mark **NA.**

- If you are required to reauthenticate upon restarting, mark **PASS**.

- If you are not required to reauthenticate upon restarting, mark **FAIL**.

4) If a product has an authentication system, it requires at least two pieces of information to authenticate users.

- Obtain a copy of the manufacturer's application for testing, and install it on a testing device. For these tests, it is sufficient to simply install the app directly from the relevant official app Store.
- Create a new user and note if user authentication requires at least two pieces of information (e.g. "username" + "password"). Note all required pieces of information.
- If the product does not support user accounts or any authentication system, mark **NA.**
- If the authentication system requires at least two pieces of information, mark **PASS**.
- If the authentication system does not require at least two pieces of information, mark **FAIL**.

5) For products that handle sufficiently sensitive data, users can choose to use multi-factor authentication.

- Obtain a copy of the manufacturer's application for testing, and install it on a testing device. For these tests, it is sufficient to simply install the app directly from the relevant official app store.
- Determine whether the product handles sensitive data. Examples include health information, location, live or recorded audio or video as well as personal messages.
- If the product does not handle sensitive data, mark **NA.**
- If the product supports accounts, create an account and determine whether there are settings to enable multi-factor authentication, so that in addition to a password, a user can require authentication through a text message, token, or other method.
- If the product handles sensitive data, and multi-factor authentication is available, mark **PASS.**
- If the product handles sensitive data, but there is no authentication mechanism at all, mark **FAIL.**
- If the product handles sensitive data, and multi-factor authentication is not available, mark **FAIL.**

6) For products that handle sufficiently sensitive data, users can choose to use multi-factor authentication whenever the product is activated, or when a device is unrecognized.

- Obtain a copy of the manufacturer's application for testing, and install it on a testing device. For these tests, it is sufficient to simply install the app directly from the relevant official app Store.

- Create an account and if there are settings to enable it, set up multi-factor authentication.

- Examine the settings option for multi-factor authentication, and see whether there is an option to require multi-factor authentication every time the product is re-started or when a device is unrecognized. If yes, select that setting.

- Completely close the app and restart it multiple times on one device, and note if multi-factor authentication is required for authentication each time.

  Completely close and restart the app multiple times on multiple devices, and note if multi-factor authentication is required for authentication on each device each time.

- Determine whether the product handles sensitive data. Examples include health information, location, live or recorded audio or video, as well as personal messages.

- If the product does not handle sensitive data, mark **NA.**

- If the product handles sensitive data and requires you to use multi-factor authentication on each login from all devices, mark **PASS.**

- If the product requires you to use multi-factor authentication on new devices, but does not require multi-factor authentication for subsequent authentication requests on the same device, mark **PARTIAL PASS.**

- If the product does not offer multi-factor authentication, or does not permit users to select a setting under which it is required for each login and when authenticating from new devices, mark **FAIL.**

7) If the product uses a password/passphrase for authentication, it requires that passwords are at least 8 characters long.

- Obtain a copy of the manufacturer's application for testing, and install it on a testing device. For these tests, it is sufficient to simply install the app directly from the relevant official app Store.

- Create or edit an existing account.

- Try passwords such as "a" and "a1b2c3."

- Note minimum password lengths required by the app.

- If the product does not support user accounts and password-based authentication, mark **NA.**

- If the product requires passwords to be at least eight characters long, mark **PASS.**

- If the product does not require passwords to be at least eight characters long, mark **FAIL.**

8) If the product uses a password/passphrase for authentication, the password/passphrase may be at least 20 characters long.

- Obtain a copy of the manufacturer's application for testing, and install it on a testing device. For these tests, it is sufficient to simply install the app directly from the relevant official app Store.

- Create or edit an existing account.

- Try passphrases of 20 characters such as "i love long passphrases."

- Note whether any maximum password length is enforced.

- If the product does not support user accounts and password-based authentication, mark **NA.**

- If the product allows passwords of lengths of at least 20 characters or more, mark **PASS.**

- If the product limits password lengths to below 20 characters, mark **FAIL.**

9) If the product uses a password/passphrase for authentication, it requires that passwords are reasonably complex.

- Obtain a copy of the manufacturer's application for testing, and install it on a testing device. For these tests, it is sufficient to simply install the app directly from the relevant official app Store.

- Create or edit an existing account, attempting to update the password.

- Try passwords such as "aaaaaaaa" and "12345678."

- Note if the app requires complexity in the password (e.g. special characters, capital letters, mixing numbers and letters, etc.).

- If the product does not support user accounts and password-based authentication, mark **NA.**

- If the product requires some password complexity (e.g. requiring mixing numbers and letters, but not requiring special characters), mark **PARTIAL PASS.**

- If the product requires several forms of password complexity, mark **PASS.**

- If the product enforces no forms of password complexity, mark **FAIL.**

10) If the product uses a password/passphrase for authentication, it allows all reasonable characters as input.

- Obtain a copy of the manufacturer's application for testing, and install it on a testing device. For these tests, it is sufficient to simply install the app directly from the relevant official app Store.

- Create or edit an existing account.

- Try passwords such as ")a!aaaaa$a%" and "p 4 5 5 w 0 R d !" Try using a variety of the standard special characters that appear on keyboards.

- Note if the app limits the use of any special characters.

- If the product does not support user accounts and password-based authentication, mark **NA.**

- If the product allows all special characters on a standard keyboard, mark **PASS.**

- If the product allows some special characters, but places limits, mark **PARTIAL PASS.**

- If the product does not allow any special characters from the standard set on a keyboard in the password, mark **FAIL.**

11) If the product uses a password/passphrase for authentication, it is compatible with popular password managers.

- Obtain a copy of the manufacturer's application for testing, and install it on a testing device. For these tests, it is sufficient to simply install the app directly from the relevant official app Store.

- Create and then sign out of an account in the app.

- Add the credential for the app to a password manager.

- Try to log in using the functionality of the password manager.

- Note what, if any, issues you have.

- If the product does not support user accounts and password-based authentication, mark **NA.**

- If the product allows the use of a password manager, mark **PASS.**

- If the product does not allow the use of a password manager, mark **FAIL.**

Criteria: A product that has an authentication system resists attempts to break it.

→ **INDICATORS**

1. The product allows users to be notified via an out-of-band medium when account security settings are changed.
2. To change a password/passphrase/pin, a user must enter the previous password/passphrase/pin, or have access to a secondary system that is used to reset it.
3. The product notifies users when account security settings have changed.
4. If the product has an authentication system, it also has a system to prevent brute-force/dictionary attacks.

Methodology for Assessing Each Indicator

1) The product allows users to be notified via an out-of-band medium when account security settings are changed.

- Obtain a copy of the manufacturer's application for testing, and install it on a testing device. For these tests, it is sufficient to simply install the app directly from the relevant official app Store.
- Create an account and set up authentication.
- Look at the documentation that came with the product, and attempt to locate any instructions for enabling notifications out-of-band.
- If this is not documented, look through the app settings for security or notifications.

- Note whether or not the app allows email, SMS, or push notifications to be used as notification when changes occur or account credentials need to be reset.
    - If the app does allow this option, select it.
- Go into settings, and change your password or another security setting. Then note if the app uses an out-of-band medium—such as by sending you a text or email—to send a notification of the change.
- If the product does not support user accounts with security settings, mark **NA.**
- If the product automatically sends out-of-band notifications, without user input, mark **PASS.**
- If the product allows user-selectable out-of-band notifications, mark **PASS.**
- If the product does not allow for or send out-of-band notifications, mark **FAIL.**

2) To change a password/passphrase/pin, a user must enter the previous password/passphrase/pin, or have access to a secondary system that is used to reset it.

- *Note: This indicator contains two opportunities for pass/fail.*
- Obtain a copy of the manufacturer's application for testing, and install it on a testing device. For these tests, it is sufficient to simply install the app directly from the relevant official app Store.
- Create an account and set up a password.
- While logged in to the app, attempt to change the password.
- Note whether or not you are required to enter the old password, or use an email account, phone number, or other second factors in order to reset the password.
- Next, log out and close out of the app. Reopen the app and look for a “forgot my password” link or button that enables you to reset the password. Determine whether the password reset option requires use of a secondary system such as an email account or phone number that the user has previously provided to the app as associated with that user.
- If the product does not support user accounts and password-based authentication, mark **NA.**

- If a product supports user accounts and password-based authentication, first assess what happens when the user is logged in:
    - If the product requires either entering an old password, or confirmation via a secondary system to change a password while logged in, mark **PASS.**
    - If the product does not require either entering an old password, or confirmation via a secondary system to change a password while logged in, mark **FAIL.**
- Next assess what happens when the user is not logged in:
    - If the product requires a secondary system such as an email account or phone number to reset passwords while logged out, mark **PASS.**
    - If the product does not require a secondary system such as an email account or phone number to reset passwords while logged out, mark **FAIL.**

3) The product notifies users when account security settings have changed.

- Obtain a copy of the manufacturer's application for testing, and install it on a testing device. For these tests, it is sufficient to simply install the app directly from the relevant official app Store.
- Create an account including setting a password and any other security settings like multi-factor authentication.
- Change the password or other security setting.
- Note whether you are notified of the change, and if so how (e.g. by email or text).
- If the product does not support user accounts and password-based authentication, mark NA.
- If the product notifies users when account security settings have changed, mark PASS.
- If the product does not notify users when account security settings have changed, mark FAIL.

4) If the product has an authentication system, it also has a system to prevent brute-force/dictionary attacks.

- Create an account including establishing a password.
- Attempt to log in to the app at least ten times using different incorrect passwords.
- If the product does not support user accounts and password-based authentication, mark **NA.**
- Note any limitations the app places on password attempts, including any messages that appear indicating how many more attempts you may make.
- If the app limits incorrect login attempts, mark **PASS**.
- If the app does not limit incorrect login attempts, mark **FAIL**.

Encryption

Criteria: Information I provide is encrypted so that it can't be easily read or used by attackers.

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ INDICATORS

1. Transmission of user communications or information is encrypted by default.
2. Transmission of user communications or information is encrypted using unique keys.
3. Users can secure their content using end-to-end encryption.
4. End-to-end encryption is enabled by default.
5. User information and communications are encrypted by default when at rest.

Methodology for Assessing Each Indicator

1) Transmission of user communications or information is encrypted by default.

- *Note: This indicator has been broken into two tests, one that marks what a company may say about their use of encryption and another that captures what the app is actually doing.*

a) Investigation and analysis of publicly available documentation.

- Search the application provider's website for any publicly available documentation regarding the use of encryption within the product.

- Determine whether the documents describe what if any types of encryption are used.

- If the provider describes the types of encryption in use and states that user communications or information are encrypted by default or automatically, mark **PASS**.

- If the provider describes any encryption even if they do not describe specific schemes, mark **PARTIAL PASS**.

- If the provider does not describe the use of any encryption, mark **FAIL**.

b) Inspect app traffic to check for TLS (transport layer security) encryption use.

- *Note: The Procedural Overview in the Digital Standard uses the term "SSL" (secure socket layer). While the terms TLS and SSL have popularly been used interchangeably, SSL no longer qualifies as a secure protocol. The implementation of SSL instead of TLS would constitute a FAIL condition in this methodology. For that reason we have opted to exclusively use the term TLS.*

- Obtain a copy of the manufacturer's application for testing, and install it on a testing device.

- Set up and configure the app, mimicking normal use.

- Capture the network communications from the app, and ensure that all communication between the app and any servers is encrypted.

    - The best way to capture packets between an app and the internet may vary based on your testing environment, but a Linux-based router, such as one running **OpenWRT**, should allow you to capture all traffic on a test wireless network. If you are running the app in an emulated environment, you should be able to capture traffic from the host system.

    - With a packet capture in hand, you can analyze the traffic with a tool like **Wireshark**.

- If the app uses TLS, or other recognizable encryption protocols, mark **PASS**.

- If the app does not use TLS or other recognizable encryption protocols, mark **FAIL**.

2) Transmission of user communications or information is encrypted using unique keys.

- Open and close the app multiple times, capturing the network traffic between the app and the app's servers.
    - The best way to capture packets between an app and the internet may vary best on your testing environment, but a Linux-based router, such as one running **OpenWRT**, should allow you to capture all traffic on a test Wireless network. If you are running the app in an emulated environment, you should be able to capture traffic from the host system.
    - With a packet capture in hand, you can analyse the traffic with a tool like **Wireshark**.
- Examine the network traffic between connections and determine if the app attempts to use new session keys when communicating with the server.
    - You should be able to find this by looking at the "Protocol" column in the Wireshark interface, for TLS, and the "Info" column for Client Hello, followed by Server Hello. Looking at those packets you will see fields for "Session ID," as well as the Server and Client "Random ID."
    - See if those fields change between opening and closing the app. If they do, that is evidence that new TLS session keys are being generated.
- If a new session key is used per session (or more frequently) mark as **PASS**.
- If a new session key is not used per session (or more frequently) mark as **FAIL**.

3) Users can secure their content using end-to-end encryption.

- Examine the settings for the app to determine if the user can enable end-to-end encryption or if it is already enabled by default.

    - Look around in the settings of the app you are testing to find what encryption settings are made available to users.

    - Note if end-to-end encryption can be enabled or disabled by the user.

- If the app does not allow for the creation or sharing of user content sent from one user to another or to a group of others, mark as **NA**.

- If the app provides an interface for enabling/disabling end-to-end encryption, mark **PASS.**

- If the app provides no interface for enabling/disabling end-to-end encryption, mark **FAIL**.

4) End-to-end encryption is enabled by default.

- If end-to-end encryption is user-configurable, check the settings to see if end-to-end encryption is the default selection.

- If the app does not offer any ability to communicate with other users or the company, so that there are no communications that could be protected by end-to-end encryption, mark **NA**.

- If end-to-end encryption is configurable, and enabled by default, mark **PASS**.

- If end-to-end encryption is configurable, and not enabled by default, mark **FAIL**.

5) User information and communications are encrypted by default when at rest.

- After configuring the app for normal usage, find any files touched by the app.

    - On Android, apps are supposed to write data to standard places (/data/data/<package_name> and/or /sdcard/Android/data/<package_name>). However, there is no technical limitation on where an app can write data to the sdcard.

    - One method is to use the “find” command before and after installing the app, as well as before/after configuring it. In a terminal or adb shell, run “find /sdcard -mmin -60” to get a listing of every file in the last 60 minutes.

- Examine the files, and note if data is left unencrypted.

- If data is stored in an unencrypted fashion, examine it to see if it contains what could be considered “user information” or “communications.”

- If the app does not store any data on the device, mark **NA**.

- If the app stores some data, but only less sensitive information like non-identifiable configuration settings, mark **NA**.

- If the app stores only encrypted data, mark **PASS**.

- If the app encrypts data such as user credentials, customer information, or other data that could be used to gather information on a user, or communication between users, but does not encrypt less sensitive information like non-identifiable configuration settings, mark **PASS**.

- If the app stores data such as user credentials, customer information, or other data that could be used to gather information on a user, or communications between users and does not encrypt it, mark **FAIL.**

Known Exploit Resistance

Criteria: The product is protected from known software vulnerabilities that present a danger from attackers.

See the test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

Notes:

- *This test contains only one criteria and only one indicator. However, the procedural overview in the Digital Standard separates out testing into three areas, Browsers, Apps, and Connected Devices.*
- *Common Vulnerabilities Exposures is a publicly available list of known software and firmware vulnerabilities, where each vulnerability is given a unique identifier and standardized description. It is operated by the MITRE Corporation, a U.S. non-profit that oversees federally funded research and development centers (FFRDCs). Each vulnerability is commonly known as a "CVE." In general, all well-known vulnerabilities will have CVEs. Searching the CVE list for the name of the piece of software you are analyzing, is the first step in testing against known vulnerabilities for software of all types.*

→ **INDICATORS**

1. The software is secure against known bugs and types of attacks.

Methodology for Assessing Each Indicator

1) The software is secure against known bugs and types of attacks.

Browsers

- Identify whether the product being evaluated has a browser component. For example, tablets, phones, and televisions may ship with browsers, whereas connected devices like fitness trackers, water sensors, and grills may not.

- Identify if the browser component is a recognizable web browser (e.g. Chrome, Firefox, Safari, etc.), a customized derivation of a recognizable web browser, or an unrecognized or custom web browser.

- You will be testing whether the product shipped with a vulnerable version of a browser, so you need to locate any CVEs affecting the installed browser. Search **the CVE database** using the name of the browser component you are testing (e.g. Chrome, Firefox, Safari, etc.), and the name of the manufacturer and product as keywords. Identify CVEs affecting the browser (read more about **effectively searching CVEs** here).

- For each CVE that you have identified as affecting the browser component you are testing, determine whether the CVE has been addressed in current versions of the software (e.g. the vulnerability has been patched in Chrome).

- Determine if the browser component you are testing is updated enough to address each identified CVE.

- If the browser is not updated, or it is unclear which version the browser component is based on, for each CVE that you have identified as affecting the browser determine whether the CVE's proof of concept code is posted publicly. Usually this will be linked from the CVE notice, or the documentation of the vulnerability linked from the CVE page.

- If the original proof of concept code for the CVE you are testing against is available, use it to test the browser for the issue defined in the vulnerability notice.

- If the CVE’s original proof of concept code is not available, devise custom code based on the detailed description of the vulnerability either in the CVE itself or in the reference linked from the CVE page, to test the browser for the issue identified in the vulnerability notice.

- Check if the browser is protected from the identified vulnerabilities.

- If the browser is protected from all the identified known exploits, mark **PASS**.

- If the browser is not protected from all identified known exploits, mark **FAIL**.

- If the product does not ship with a browser, mark **NA**.

Apps

- Search **the CVE database** using the app name as a keyword, and identify CVEs for the app.

- Identify whether the CVE's proof of concept code is posted publicly. Usually this will be linked from the CVE notice, or the documentation of the vulnerability linked from the CVE page.

- Review documentation from the app manufacturer to see if there has been a software update released that fixes any known vulnerabilities.

- Search online for any known/high-profile vulnerabilities for this class of app. For example, a "class of apps" could involve all media players on a platform, and the so-called "Stagefright" bug was a generic attack on a common Android media library, and had effects on many video apps.

- For each applicable CVE, identify whether the CVE's proof of concept code is posted publicly. Usually this will be linked from the CVE notice, or the documentation of the vulnerability linked from the CVE page.

- If the original proof of concept code for the CVE you are testing against is available, use it to test the app for the issue defined in the vulnerability notice.

- If the CVE's original proof of concept code is not available, devise custom code based on the detailed description of the vulnerability either in the CVE itself or in the reference linked from the CVE page, to test the browser for the issue identified in the vulnerability notice.

- If the app proves to no longer be vulnerable to known and published vulnerabilities, mark **PASS**.

- If after running provided or custom proof of concept code it is identified that the app has any of the following, mark **FAIL**:
    - Unpatched known vulnerabilities specific to the application.
    - Unpatched known vulnerabilities specific to its app class.

Connected Devices

- *Note: Where it is difficult to extract the firmware from a device for testing, there are more complex ways in which testers can attempt to extract the embedded codebase from a running chip, however these methods require specialized, expensive equipment that may not be available to non-expert testers. For our purposes we have not pursued the issue for this methodology. We will update this description if we have greater success when we test additional products.*

- Establish whether a connected device has software that runs on the device itself. Often this is the code that controls the actual non-internet facing part of the device, for example the code that actually interacts with a physical lock, or turns off a water faucet. These embedded devices use low-level processors where the device's operating code is written directly to a part of the chip—the product's firmware.

- Retrieving firmware from a device:

  - Sometimes this step will not be possible, in many cases these types of difficulties indicate code quality (it is more secure against tampering).

  - Check the manufacturer's site. Often an IoT device will not be self updating and will require a manual update, which requires downloading a firmware package. Failing that, firmware can be pulled from the chip itself.

- If you can find the firmware, attempt to identify what language it is written in, and any other details that can be used as keywords when searching for relevant CVEs.

- Search **the CVE database** using information gained about the firmware as keywords and identify existing CVEs for the connected device firmware.

- For each applicable CVE, identify whether the CVE's proof of concept code is posted publicly. Usually this will be linked from the CVE notice, or the documentation of the vulnerability linked from the CVE page.

- If the original proof of concept code for the CVE you are testing against is available, use it to test the app for the issue defined in the vulnerability notice.

- If the CVE's original proof of concept code is not available, devise custom code based on the detailed description of the vulnerability either in the CVE itself or in the reference linked from the CVE page, to test the browser for the issue identified in the vulnerability notice.

- If you can find and test the firmware, and it is not flagged as susceptible to know exploits, mark **PASS**.

- If after running provided or custom proof of concept code it is identified that the firmware has unpatched known vulnerabilities, mark **FAIL**.

Vulnerability Disclosure Program

Criteria: The company is willing and able to address reports of vulnerabilities.

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ INDICATORS

1. The company has a mechanism (ex: a bug bounty program) through which security researchers can submit vulnerabilities they discover.
2. The company discloses the timeframe in which it will review reports of vulnerabilities.
3. The company commits not to pursue legal action against security researchers.

Methodology for Assessing Each Indicator

1) The company has a mechanism (ex: a bug bounty program) through which security researchers can submit vulnerabilities they discover.

- Obtain and review a copy of the product's terms of service, review any other online documentation available.
- Look for language describing vulnerabilities, security research, or bug bounties.
- Look for an online submission form for bug reports.
- Review aggregator websites like Bug Crowd and HackerOne to see if programs are listed for the product or service.

- If a vulnerability submission mechanism exists, mark **PASS**.

- If a vulnerability submission mechanism does not exist, mark **FAIL**.

2) The company discloses the timeframe in which it will review reports of vulnerabilities.

- Obtain and review a copy of the product's terms of service, review any other online documentation available.

- Look for language describing vulnerabilities, security research, or bug bounties.

- Look for an online submission form for bug reports.

- Review aggregator websites like Bug Crowd and HackerOne to see if programs are listed for the product or service.

- If such a mechanism exists, review the documentation for any information about timelines, deadlines, timeframes, etc. for submission review.

- If a company timeframe for reviewing reports of vulnerabilities exists, mark **PASS**.

- If a company timeframe for reviewing reports of vulnerabilities does not exist, mark **FAIL**.

3) The company commits not to pursue legal action against security researchers.

- Obtain and review a copy of the product's terms of service, review any other online documentation available.

- Look for language describing vulnerabilities, security research, or bug bounties.

- Specifically review any terms of use or end user agreements and look for language like "access, tamper with, probe, scan, reverse-engineer, bypass, circumvent, interfere, etc."

- Review the documents for any mention of specific legislation that penalizes security research, for example the United States Computer

Fraud and Abuse Act (CFAA), or the United States Digital Millennium Copyright Act (DMCA).

- Review the documents for any mention of specific penalties for engaging in security research, ranging from disabling of the service or product to legal action against the researcher.

- Review the documents and potential vulnerability disclosure program information, looking for an explicit commitment not to pursue legal action for security research.

- If an explicit commitment not to pursue legal action against security researchers exists, mark **PASS**.

- If an explicit commitment not to pursue legal action against security researchers does not exist, mark **FAIL**.

- If the legal documents outline specific penalties or action that may be taken against security researchers, mark **FAIL**.

Security Over Time

Criteria: The product is kept protected with software updates for a clearly defined and communicated period of time (i.e., the product life cycle).

See this test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

→ **INDICATORS**

1. The product life cycle is communicated to the potential owner before purchase.
2. Software updates are authenticated.
3. Automatic software updates.
4. Notification of software updates.

Methodology for Assessing Each Indicator

1) The product life cycle is communicated to the potential owner before purchase.

- Obtain and review a copy of the product's terms of service, online warranty, and end user agreement, and review any other online documentation available on the company's website.
- Review any language that may appear in the exterior labelling of the product, if any, that a customer might be able to read before purchasing the product.

- Look for language describing timelines, deadlines, or any dates or lifespans associated with the product. For example, expiration of warranty, service limitations, scope of coverage, etc.

- Look for language describing updates, repair or replacement, or a commitment to maintain the product or software for a certain timeline.

- Look for language specifically describing software updates, patches, etc.

- If a product life cycle is described in any of these materials, mark **PASS**.

- If a product life cycle is not described, mark **FAIL**.

2) Software updates are authenticated.

- *Note: The Digital Standard lists the procedure for this indicator as "To Be Decided."*

- Obtain and review a copy of the product's terms of service, online warranty, and end user agreement, and review any other online documentation available on the company's website.

- Look for language specifically describing the process for software updates, patches, etc.

- Look for language about authentication or any other description of processes used to secure a software update and ensure that it is being sent from an authorized party.

- If a process for authenticating updates is described, mark **PASS**.

- If a process for authenticating updates is not described, mark **FAIL**.

3) Automatic software updates.

- Obtain and review a copy of the product's terms of service, online warranty, and end user agreement, and review any other online documentation available on the company's website.

- Look for language specifically describing the process for software updates, patches, etc.

- Look for language describing how these updates are installed, specifically whether users are obligated to install updates manually or whether the software is updated automatically by the provider.

- Examine software settings and product documentation to determine if automatic software updates can be enabled by the user.

- If the product can be updated automatically, mark **PASS**.

- If the product does not permit automatic updates, mark **FAIL**.

4) Notification of software update.

- Obtain and review a copy of the product's terms of service, online warranty, and end user agreement, and review any other online documentation available on the company's website.

- Look for language specifically describing the process for software updates, patches, etc.

- Look for language describing how these updates are installed, specifically whether users are obligated to install updates manually or whether the software is updated automatically by the provider.

- Look for language clarifying whether users will be notified of software updates, and by what mechanism they will be notified.

- If the documentation indicates that users will be notified of updates, mark **PASS**.

- If no information exists regarding notification, or if documentation specifically states that users will not be updated, mark **FAIL**.

Product Stability

Criteria: The software is reliable.

See the test in action:

- **Smart lock**
- **Smart pressure cooker**
- **Smart baby monitor**

Notes:

- *This test focuses on fuzzing software (providing unexpected, random, and/or invalid data to a program). Fuzzing is a well-established process within security testing, and is one of the most common means through which security vulnerabilities have been discovered. Due to its highly technical nature, and the per case specificity of the process, a comprehensive look at fuzzing in general (or even specifically the fuzzing of Android apps) is well beyond the scope of this methodology. Fuzzing experience or additional background reading are absolutely necessary for running this test.*
- *For an overview of the topic of fuzzing, as well as some information on popular fuzzing tools, and synopsis of recent research in the field see **this post**.*
- *Instead of attempting to cover a broad, complex, and ever evolving topic, this methodology identifies useful tools and documentation on fuzzing, and focuses on what types of fuzzing outcomes to look for.*
- *Given the case specific nature of every fuzzing test run against a piece of software, and the general documented **lack of industry benchmarks** making it difficult to compare the results of fuzzers, at this point it is not practical to provide a PASS/FAIL framework for this test. All of the results of this procedure should be qualitatively evaluated by testers based on the specifics of the software being tested and the background knowledge of how the software is supposed to operate.*

→ INDICATORS

1. The software is not susceptible to crashes.

2. If the program is forced to unexpectedly terminate, it shuts down in a safe and responsible fashion.

3. The software is not vulnerable to algorithmic complexity attacks.

Methodology for Assessing Each Indicator

1) The software is not susceptible to crashes.

- *Note:*

    - *This methodology only considers Android apps that are used to interact with physical connected devices, or self-contained Android applications being tested using the Digital Standard. We made this choice due to the open nature of Android, and the wide availability of free tools for inspecting Android app code. However, products may also use many other kinds of software that would be evaluated as part of Digital Standard testing. For example, many connected devices will have apps tailored for both Apple iOS and Android, or may run software that is unique to that specific product, but could be fuzzed. We recommend that the tester research the toolsets and best practices for fuzzing in the coding languages and/or platform environments of that other software,and use that information to craft additional rounds of fuzzing tests for that software.*

- *Note:*

    - *There are many tools and resources for fuzzing Android software, as well as multiple approaches to use for fuzzing an Android app. This methodology points towards one approach, though others may also yield valid results for these tests.*

    - *The **Security Testing** pages on the Android project page, particularly the documentation on **libFuzzer**, will cover the current state of Android app fuzzing.*

    - *For a background in fuzzing on Android, see **this paper** or the **accompanying lecture** delivered at a security conference in 2015, which walks through several approaches. Though somewhat dated, it does provide a good look at the landscape of the topic.*

- Obtain and configure a new version of the **American Fuzzy Lop (AFL)** fuzzing tool. The linked AFL page is a version of the main AFL project maintained by Google to include support for the Android platform.

- Using the documentation provided with AFL, run a variety of fuzzing tests on the app. These will require generating, or finding examples of, preseed files for the fuzzer. The AFL documentation covers how to generate appropriate seed files for your fuzzer.

- Run the tests for long enough to uncover crash scenarios. At minimum, a fuzz test should be run a few thousand times, but ideally leaving a test running for longer, and testing with more target devices will yield better and more reliable results. More test cycles will better isolate the causes of crashes, and increase the likelihood that a crash can be reliably reproduced, and that the correct input conditions to create a crash are logged by the fuzzing tool. The goal is to complete a high number of tests, however there is no predicting the amount of time each test will take to complete. Every variable in the test, from the size of the codebase being tested, to the hardware the test is running on will affect how long it takes to run.

    ◦ Determine whether crashes occur often enough that AFL can reproduce and group them over enough runs to feel confident they are not random.

- In order to see the code coverage information (what part of the library crashes occur in), you will need to obtain and configure **afl-cov**, which is a companion to the AFL program that takes AFL output and creates code coverage information. According to the project page, "code coverage is interpreted from one case to the next by afl-cov in order to determine which new functions and lines are hit by AFL with each new test case."

    ◦ Determine whether sufficient amounts of the software were covered in fuzz testings to find errors hidden deeply in software.

2) If the program is forced to unexpectedly terminate, it shuts down in a safe and responsible fashion.

- *Note:*

    ◦ *This methodology only considers the Android app that is used to interact with the product. We made this choice due to the open nature of Android, and the wide availability of free tools for inspecting Android app code.*

- *Note:*
    - *There are many tools and resources for fuzzing Android, as well as approaches to go about fuzzing an Android app. This methodology points toward one approach, though others may also yield valid results for these tests.*
    - *The* ***Security Testing*** *pages on the Android project page, particularly the documentation on* ***libFuzzer****, will cover the current state of Android app fuzzing.*
    - *For a background in fuzzing on Android, see* ***this paper*** *or the* ***accompanying lecture*** *delivered at a security conference in 2015, which walks through several approaches.*
    - *Typically a fuzz test will either crash (cause the program to quit or exit) or hang (cause the program to become unresponsive) a piece of software. This indicator investigates what state a system is left in when software is crashed, hung, or unexpectedly terminated.*
- Obtain and configure a new version of the **American Fuzzy Lop (AFL)** fuzzing tool. The linked AFL page is a version of the main AFL project maintained by Google to include support for the Android platform.
- Using the documentation provided with AFL, run a variety of fuzzing tests on the app. These will require generating, or finding examples of, preseed files for the fuzzer. The AFL documentation covers how to generate appropriate seed files for your fuzzer.
- Run the afl-fuzz tool with "-C" option, which will enable "crash exploration" mode. The AFL documentation **describes in greater detail** how to triage crash information to determine types of access an attacker could gain from crashing the app.
    - Determine whether the app crashes in an unsafe way that leaves code paths open, memory unreleased, or other potential attack surfaces for which an exploit could be written that could lead to the first step of a hack on the device, or access to private information from outside of the app.

3) The software is not vulnerable to algorithmic complexity attacks.

- *Note:*

    - *An algorithm is generally designed with its own average use case in mind. Algorithmic complexity attacks take advantage of "best-case" assumptions, and trigger the algorithm's "worst-case" behavior in order to exhaust system resources. What that is will vary by algorithm purpose, but as a simple example, assume a device checks for weather updates, and has a setting for how often to check, but does not limit that frequency. So where the designer assumed no one would need to check more often than every minute, the complexity attacker checks ten times a second, crashing the device. How to detect and guard against these types of attack through fuzzing is an area of active interest. For an overview of the issue see this **presentation**.*

- *Note:*

    - *Fuzzing for algorithmic complexity in Android apps has traditionally taken a great amount of specific knowledge of the libraries used in that app for the generation of custom preseed files. But **recent work** shows great promise in making that process automated for all Java libraries, which means that going forward less specific knowledge of algorithms used in Java libraries will be required for creating high-quality test preseed data.*

    - *Since the method described in the **HotFuzz paper** is so new, the tooling suggested has not yet matured to the point where good documentation has been written. Automated test generation will likely lead to improved testing.*

- Obtain and configure a new version of the **American Fuzzy Lop (AFL)** fuzzing tool. The linked AFL page is a version of the main AFL project maintained by Google to include support for the Android platform.

- Using background knowledge about the app and its libraries, craft preseed files that could take advantage of a complexity attack (for example providing maximum inputs into every field), and use them as part of an AFL test run. The kinds of background knowledge would include things like the coding language it is written in, what inputs it accepts, or how it is "supposed" to function when working as intended; gathering this knowledge will likely require additional product specific research.

    - Determine whether the app is susceptible to an algorithmic complexity attack, based on fuzzing results.

Personal Safety

Criteria: The company helps me protect myself from grief, abuse, and harassment.

→ INDICATORS

This test is “under discussion” and currently contains no indicators.

Open Innovation

Criteria: The company works to advance all technology and innovation, not just its own interests.

→ INDICATORS

This test is “under discussion” and currently contains no indicators.

Business Model

Criteria: I understand how the company earns its revenue.

→ INDICATORS

This test is "under discussion" and currently contains no indicators.

Repair Accessibility

Criteria: The product can be fixed by parties other than the manufacturer.

→ **INDICATORS**

The test is under discussion, so we will not be evaluating it, but it does have the following indicators:

1. The company does not use technical, feature-level, or legal means to block a consumer's ability to get a device repaired.

2. There is a competitive market of repair shops.

3. Repair shops, other than the manufacturer's, are supported by the original manufacturer.

Repair Penalty

Criteria: I am not penalized for getting the product properly repaired by a third party or for repairing it myself.

→ INDICATORS

The test is under discussion, so we will not be evaluating it, but it does have the following indicator:

1. The company does not penalize consumers (voided warranty, etc.) if they get the product repaired by someone other than the original manufacturer or their authorized representatives.

Data Benefits

Criteria: Every piece of data I share brings me a benefit; it doesn't just help the company.

→ **INDICATORS**

The test is under discussion, so we will not be evaluating it, but it does have the following indicator:

1. The company clearly discloses its purpose for collecting each type of user information.