Consumer Reports®

EXTERNAL AUDIENCE PROTOCOL

External Audience Protocol (EAP) - Home Security Cameras Privacy Testing

Purpose of this document:

This document is generated by the testing team to describe what tests are done in our evaluation of data privacy and security of home security cameras. Specifically, it refers to the relevant criteria and indicators from the Digital Standard that apply to this testing. It does not provide detailed information about our testing procedures.

Who was this created for?

The primary audience for this document is home security camera manufacturers, who are typically interested in understanding what our tests are looking for and what our ratings are based on.

External Audience Protocol (EAP) - Home Security Cameras Privacy Testing

Introduction

Residential security systems are increasing in popularity due to dropping prices and more consumer interest. They provide users with access to video and audio footage, live or recorded, over the internet, which presents the possibility for this data to be accessed, stored, shared, bought, sold, and stolen. Therefore, the security and privacy of these cameras is a primary concern for consumers and Consumer Reports. Not only do we need to test the performance of home security cameras (e.g. clarity, convenience) but also make sure the camera is protecting the owner, not monitoring them.

Test Description

Products are tested in accordance with the following criteria/indicators of the Digital Standard (https://www.thedigitalstandard.org/).

Privacy

1. Data Control - I can see and control everything the company knows about me.
    a. Users can control the collection of their information.
    b. Users can delete their information.
    c. Users can control how their information is used to target advertising.
    d. Users can obtain a copy of their information.
    e. Clear explanations of how users can control their data.
    f. Privacy controls exist and are effective.
2. Data Share - Data sharing is reasonably scoped and transparent.
    a. The company only shares information with third parties as is reasonably necessary to deliver service to consumers.
    b. The company clearly discloses what user information it shares with whom.
    c. The company clearly discloses the types of third parties with which it shares user information.
    d. The company clearly discloses the names of third parties with which it shares user information.
    e. The company clearly discloses whether it shares user information with government or legal authorities.
    f. Third-party domains contacted by the product are named in the privacy policy.
3. Data Use - Data usage is consistent with the context of the relationship with the user and is transparent.
    a. The company puts limits on the use of my data that is consistent with the purpose for which the data is collected.
    b. The company explicitly discloses every way in which it uses my data.

4. Data Retention and Deletion - I know how long the company keeps my information.
    a. All user information is deleted after users terminate their accounts or remove service from a device.
    b. Disclosure of timeframe in which user information is deleted after users terminate their account.
    c. Disclosure of how long each type of user information is retained.
5. Data Collection - I know what user information this company is collecting and when.
    a. Disclosure of the type of user information collected.
    b. Disclosure of how user information is collected.
    c. The device gives clear indication (e.g., lit LED) when cameras and microphones are active.
6. Minimal Data Collection - The only information the company requests from me is what's needed to make the product or service work correctly.
    a. The user information collected is only that which is directly relevant and necessary for the service.
    b. The product still works when all permissions not relevant to the product's functionality are declined.
7. Privacy by Default - The default settings in this product prioritize my privacy; to give up privacy, I actually need to change the settings.
    a. Targeted advertising is off by default.
    b. User interface settings that are optimal for privacy are set by default.
8. Data benefits - Every piece of data I share brings me a benefit; it doesn't just help the company.
    a. The company clearly discloses its purpose for collecting each type of user information.
9. Data benefits - Every piece of data I share brings me a benefit; it doesn't just help the company.
    a. The company clearly discloses its purpose for collecting each type of user information.
10. Terms of Service and Privacy Policy documents - I can easily find, read, and understand the privacy policy and/or terms of service.
    a. The company clearly discloses which Terms of Service (ToS) apply to the product/service in question.
    b. The ToS are easy to find.
    c. The company clearly discloses which Privacy Policy (PP) applies to the product/service in question.
    d. The PP is easy to find.
11. ToS & Privacy Policy change notification - The company provides clear notification when it changes its privacy policy and/or terms of service.
    a. Commitment to notify users about changes to the terms of service
    b. Maintains a public archive or change log of the terms of service
    c. Commitment to notify users about change to the privacy policy
    d. Maintains a public archive or change log of the privacy policy

Security

12. Encryption - Information I provide is encrypted so that it can't be easily read or used by attackers.
    a. All transmission of user communications is encrypted by default.
    b. All transmission of user communications is encrypted by a secure algorithm.
    c. Users can secure their content using end-to-end encryption.
    d. End-to-end encryption is enabled by default.
13. Known Exploit Resistance - The product is protected from known software vulnerabilities that present danger from attackers.
    a. The software is secure against known bugs and types of attacks.
    b. All known CVE or CWE should be fixed.
14. Authentication - A product has an authentication system that corresponds to the sensitivity of the user data it manages. And a product that has an authentication system resists attempts to break it.
    a. If a product supports user accounts, it has an authentication system for accessing those accounts.
    b. If the product uses a password/passphrase for authentication, it allows all reasonable characters as input.
    c. If the product uses a password/passphrase for authentication, it requires that passwords are at least 8 characters long.
    d. If the product uses a password/passphrase for authentication, the password/passphrase may be at least 20 characters long.
    e. If the product uses a password/passphrase for authentication, it requires that passwords are reasonably complex.
    f. If the product uses a password/passphrase for authentication, it is compatible with popular password managers.
    g. If a product is packaged with an account with default credentials, those credentials are unique to the instance of the product
    h. If a product has an authentication system, the user must authenticate each time they want to use the product
    i. If a product has an authentication system, it requires at least two pieces of information to authenticate users
    j. For products that handle sufficiently sensitive data, users can choose to use multi-factor authentication.
    k. 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.
    l. The product allows users to be notified via an out-of-band medium when account security settings are changed.
    m. 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.
    n. The product notifies users when account security settings have changed.

   o. If the product has an authentication system, it also has a system to prevent brute-force/dictionary attacks

15. Security Oversight - The company is a responsible caretaker of my data.
    a. The company has systems in place to limit and monitor employee access to user information.
    b. The company has an internal security team that conducts security audits on the company's products and services.
    c. The company commissions third-party security audits on its products and services.
16. Security Over Time - The product is kept protected with software updates for a clearly defined and communicated period of time (i.e., the product life cycle).
    a. The product life cycle is communicated to the potential owner before purchase.
    b. Software updates are authenticated.
    c. Automatic software updates
    d. Notification of software updates
    e. Ease of installation of software updates
    f. The software can be kept up-to-date for security issues.
17. Vulnerability Disclosure Program - The company is willing and able to address reports of vulnerabilities.
    a. The company has a mechanism (ex: a bug bounty program) through which security researchers can submit vulnerabilities they discover.
    b. The company discloses the timeframe in which it will review reports of vulnerabilities.
    c. The company commits not to pursue legal action against security researchers.