Purpose of this document:

This document is generated by the testing team to describe what tests are done in our evaluation of the privacy and security of Printers. Specifically, it refers to the relevant Criteria and indicators from the Digital Standard that apply to this testing. It also provides an overview of our testing methodologies.
Who was this created for?

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

Introduction

Small Office/Home Office (SOHO) are widely purchased by consumers to make printing easy and accessible at home. Printers were categorized as office supplies. The main focus was on usability and printing quality. However, due to changes in technology, printers now are also categorized as connected devices since users tend to connect to it via the network instead of a USB cable. The connection not only brings convenience to users but also brings privacy and security risks to the device. Therefore, Consumer Reports works with International Consumer Research & Testing (ICRT) to evaluate how secure the printer is by design compared to other modern IoT devices and how printer companies handle user data. The goal is to find and bring attention to areas, in privacy and security, that require improvements.

Test Description

Products are tested in accordance with the following criteria/indicators of the Digital Standard (https://www.thedigitalstandard.org/) and some of these criteria/indicators apply jointly to both the CR and to the ICRT IoT Test Program.

Joint Tests

1. Update
   a. Automatic firmware update is available and on by default.
   b. Update option should be easy to use and accessible by users on each user interface (ex. web application and mobile application.)
   c. Password Strength.

2. Policy
   a. The company claims a period of product support for the product, firmware, etc., beyond a limited product warranty.

3. Mobile App Permission
   a. Permissions should only be reserved for specific features of the device.
   b. No unnecessary permissions are reserved.
   c. The app still works when all permissions are declined.
   d. The app explains what happens if you decline the permissions asked.
   e. The app explains what happens if you decline the privacy policy.
4. Account Access Controls
   a. Authentication is available on each user interface (ex. web application and mobile application).
   b. The authentication system requires at least two pieces of information to log in. (ex. username and password)
   c. The authentication system rates failed login attempts.
   d. The authentication system is compatible with popular password managers.

5. Password
   a. No default password, or prompt users to change the default password when they set up the device.
   b. If there is a default password, it is random and unique.

6. Password Strength
   a. An account password contains any character you can type.
   b. The password has to be at least 8 characters.
   c. It allows a password that is more than 20 characters long.
   d. It disallows a password that is overly simple.

7. Resetting your password/ passphrase
   a. Users are able to use email, SMS, or push notifications to be notified when account credentials were reset.
   b. Password change requires the previous password. Or have access to a secondary system that is used to reset it.

8. Resistance to Known Exploits
   a. No unfixed CVEs exist on the device.
   b. No vulnerability is picked up by vulnerability scanners.

9. Encryption
   a. The communication on the device is encrypted by default.
   b. The communication on the mobile application is encrypted by default.
   c. The communication uses a well-known encryption method by default.
   d. The product/app uses valid SSL/TLS certificates.

10. Decommissioning of Product
    a. It is simple to find the controls for resetting the product.
    b. Users can factory reset the product.
    c. Users can’t view or access any of the previous user data after a factory reset.

Consumer Report Only Tests

Security
1. 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.

2. 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.

3. 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.

Privacy

1. Data Control - I can see and control everything the company knows about me.
   a. Users can control how their information is used to target advertising.
   b. Users can obtain a copy of their information.
   c. Clear explanations of how users can control their data

2. 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

3. 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

4. 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.

5. Data Use - The company explicitly discloses every way in which it uses my data.
   a. Disclosure of what user information is shared
   b. Disclosure of the types of third parties with which user information is shared
   c. Disclosure whether user information could be shared with the government or legal authorities
   d. Third-party domains contacted by the product are named in the privacy policy.
e. Disclosure of the secondary uses (or lack thereof) of data collected by using this product/service
f. Disclosure if the data collected in the usage of this product/service is not shared with 3rd parties
g. Disclosure that the company does use data collected in the usage of this product/service for targeted advertising or marketing

6. Privacy Policy & Terms of Service - I can easily find, read, and understand the privacy policy and/or terms of service and the company provides clear notification when it changes its 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 policies apply to the product/service in question.
   d. The privacy policies are easy to find.

7. Data Sharing - Data sharing is reasonably scoped and transparent.
   a. The company clearly discloses what user information it shares with whom.
   b. The company clearly discloses the types of third parties with which it shares user information.
   c. The company clearly discloses the names of third parties with which it shares user information.
   d. The company clearly discloses whether it shares user information with the government or legal authorities.
   e. Third-party domains contacted by the product are named in the privacy policy.

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.
Test Methodology

CR Privacy & Security Testing consists of three primary methodologies outlined below.

1. **UI/UX Evaluation**
   - Test the Password creation rules to determine the level of complexity required.
   - Test and look for requirements for additional user authentication options (Bio, MFA, PIN, and etc.)
   - Validate Firmware update options offered.
   - Validate Software update options offered.
   - CVE database known exploits lookup.
   - Review data control options in UI/UX.

2. **Technical Test**
   - Security features (Set up the device and note the privacy/security settings and features available to the user, such as cert pinning, root detection, backup option, stack protection, etc.)
   - Perform an extensive Brute-force dictionary attack.
   - Continuous network traffic capture, processing, and analysis to validate that all data is encrypted in transmission.
   - Data encryption at rest (Local file system inspection). Validate that all data created or information stored locally on the host device is encrypted.
   - Perform Vulnerability scanner testing (i.e., light penetration testing).
   - Confirm if CVE database known exploits are fixed.
   - Detect third-party tracker’s SDKs.
   - Analyze network traffic endpoints.

3. **Document Review**
   - CR reviews privacy policies, terms of service, EULA, and other public, legally binding, documentation to determine what practices a company commits to in writing.