Consumer Reports
Digital Standard Test Summary Notes

Examining data privacy & data security in
Wireless Security Cameras | July 2020

Purpose of this document:

This document is what our testing team uses to record a summary of our testing process and findings. It includes information about testing methodology, highlights, and overall suggestions for improvement of this product category. It helps the team describe any significant insights of our current test batch.

How-to read this document:

- Section 1: An overview of testing methodology.
- Section 2: Highlights of some good practices and specific problems or issues we found in certain companies' products and some common industry-wide problems or issues.
- Section 3: Overall suggestions for improvement in this product area, explaining what changes we are looking for manufacturers to make in the interest of consumers.

Who was this created for?

This document is intended to summarize the key test results to the content creators and other colleagues within Consumer Reports, who may then use this information to produce material targeted to various audiences or platforms, such as a Consumer Reports article tailored for more public consumption.

Section 1: Methodology

Security Cameras were already a part of CR's testing program. Because of the potential risks in having these cameras in consumers' home and offices, we conducted an evaluation of Privacy and Security aspects of the cameras' functionality and manufacturers in accordance with the Digital Standard:

Data Privacy	Data Security
PP and ToS Documents	Authentication
PP and ToS Update Notification	Encryption
Data Control	Known Exploit Resistance
Data Sharing	Security Oversight
Data Use	Security over time
Data Retention and Deletion	Vulnerability Disclosure program
Data benefits	
Data Collection	
Minimal data collection	
Privacy by default	

Our evaluation process has three parts.

- Inspection of Product and Settings
    - We evaluate the setup process regarding privacy settings.
    - We check the account registration for personal information collection and the account authentication system.
    - We review the settings menus and look for post-setup controls related to data privacy and security.
    - We review the mobile app settings menus and look for post-setup controls related to data privacy and security.
- Light security audit
    - We run static analysis and dynamic analysis on the mobile remote application.
    - We capture and analyze network traffic on the product.
    - We research common vulnerabilities and data exposures of the product.
    - We conduct light penetration tests and disclose responsibly to companies if we find security vulnerabilities or bugs.
- Document Review

    - We gather privacy policies, terms of service, and other readily accessible public information for document review.
    - We evaluate claims and quotes from those documents to understand how companies may handle users' data.

2020 Testing Process

Scoring Scheme Changes

Compared to the 2019 scoring scheme, the 2020 scoring scheme placed additional emphasis on two areas.

1. Sensitive data - video and audio recordings
    a. Data collection
    b. Transparency around sharing with third parties
    c. Limits on use of data (for example, for AI training)
2. Security breaches - Credential Stuffing
    a. The credential stuffing was a popular attack on IP cameras in 2019.
    b. Top 10 security protection features
        i. Increased focus on 10 basic practices and features that we believe all connected cameras should have to improve the security of these products

Data Analysis

The following table shows the main types of data which may be collected by the security camera companies or service providers.

Data Type	Use	Expectations
Account Information	Keeps user's data secure	Should be kept secret and encrypted wherever possible
Personal Information	Establishes profile with manufacturer	Should not be used to identify user outside of product experience without explicit consent
Video Data	Core functionality	Should be encrypted and stored and accessed securely
Audio Data	Core functionality	Should be encrypted and stored and accessed securely
Image Data	Core functionality	Should be encrypted and

		stored and accessed securely
Control Data	Lets users interact with the camera	Should only be accessible by an authenticated & authorized user
Camera Device information	Network infrastructure	Should not reveal too much information about the user or user environment
Phone/Tablet device information	Network infrastructure	Should not be used to identify user outside of product experience without explicit consent.

As specified in the table above, IP Cameras record and handle sensitive data about users and their environments. Almost all IP Cameras store this data on servers operated by their manufacturer, and transmit that data to and from smartphone applications. Therefore, there are two key elements to examine in testing for privacy and security:

1. All video and audio should be captured, transmitted, stored and protected
2. The manufacturer or service provider should not use/share (or reserve the right to use/share) a user's video or audio data for any purpose (except the government or legal authorities) outside of core functionality without the user's explicit consent.

Section 2: Key Findings

The following is a summary of findings from our May 2020 test. 13 cameras had been previously tested and were re-tested and re-scored, while an additional 13 were newly tested.

Brand	Model name	Status
Arlo	Pro 3 VMC4040P	New
Arlo	Ultra VMS5140-100NAS	New
Blink	XT2	New
Blue by Adt	Indoor Camera	New
D-Link	DCS-8300LH	New
D-Link	DCS-8525LH	New
Eufy	Cam E 1-Cam Kit	New
Nest	Cam IQ Outdoor NC4100US	New
Ring	Stick Up Cam (Battery) 3rd gen	New

Toucan	TWC200WU	New
TP-Link	Kasa Cam KC200	New
TP-Link	Kasa Smart KC300S2	New
Zmodo	Sight SD-H2601	New
Amazon	Cloud Cam (Key Edition)	Re-visit
Arlo	Pro 2 Smart Camera VMC4030P	Re-visit
Canary	All-in-One CAN100USBK	Re-visit
Canary	Flex CAN600USBK	Re-visit
D-Link	DCS-2630L	Re-visit
Guardzilla	GZ360	Re-visit
Honeywell Home	C2 WiFi Security Camera	Re-visit
Logitech	Circle 2	Re-visit
Nest	Cam Indoor NC1102ES	Re-visit
Nest	Cam IQ Indoor NC3100US	Re-visit
Samsung	SmartThings Cam GP-U999COVLBDA	Re-visit
TP-Link	Kasa Cam KC120	Re-visit
Wyze	Cam V2	Re-visit

Privacy

The rank of privacy is: Google Nest > Canary > Blue by ADT > D-Link > Ring > Logitech > Blink > Amazon > TP-Link > Samsung> Wyze > Honeywell > Arlo > Eufy > Guardzilla > Zmodo > Toucan

- Data Control
  - No brand or model gets Excellent on data control. Most devices don’t clearly offer buttons for users to execute their digital rights (for example, data deletion, data request, data collection). Samsung offers a data request and data deletion button in their app (A good example!)
  - In Eufy, Guardzilla, Zmodo, and Toucan’s privacy policies, almost no information is relevant to how users can control their data.
  - Arlo, Canary, D-Link Wyze and Blue by ADT have limited amounts of data control information in their privacy policy. However, the rights they stated are only available to EU or Californian residents due to GDPR or CCPA.
- Data Sharing
  - All companies have a section in their privacy policy disclosing what information they are going to share with other companies.

    - Google Nest, Ring, Blink, Honeywell, Logitech, and Blue by ADT scores higher than other products in data sharing because they disclose a good amount of information related to what information/data they shared with whom.
    - Ring got an Excellent for data sharing. The company claims not to sell, rent, share personal data. The company provides a statement that says that they will only share data (especially personal data) with other parties only to complete the necessary services explained in the privacy policy.
- Data Use
    - The policies of Eufy and Honeywell don’t have detailed information regarding the use of the user’s recording.
    - D-Link's policies are reasonably apparent that the company deems themself the controller of users' video recordings. See the “Processor Vs Controller” table for more information.
- Data Retention and Deletion
    - The policies of Blink, Canary, Eufy, Guardzilla, Logitech, Ring, Samsung, TP-Link Wyze, Zmodo, and Toucank don’t claim that the company retains data only as long as relevant and reasonably necessary to provide service to the user.
    - Eufy, Wyze, and Zmodo didn’t offer controls or portals that allow users to delete their data not necessary to render service.
    - Canary and Honeywell offer portals that allow users to delete their data. However, the portal is only available for Californian and EU residents due to CCPA and GDPR.
    - Only the terms of Google Nest, Eufy, and TP-Link clearly state what happens to personal user information when they close or delete their account. Personal information is immediately and permanently deleted.
- Data benefits
    - No vendor clearly states that every piece of user data brings a benefit to the user.
    - However, Blink and D-Link appear to make the designation that they are not only a data processor but also the controller of users' video recordings. They reserved a broad range of rights to process and use users' video recordings for other purposes.
- Data Collection
    - Most companies’ privacy policies have a dedicated section to explain what they collect and how they collect from users. This is an improvement over the results from last year’s evaluation.
    - However, Guardzilla, Toucan, and Zmodo have less amount of information compared to other companies.

- Minimal data collection
    - Only the terms of Canary and D-Link mention that they attempt to minimize the amount of data collected.

Security

The rank of security is: Samsung > Arlo > Google Nest > Logitech > Wyze > Blink > Ring > D-Link > Canary > TP-Link > Amazon > Honeywell > D-Link > Eufy > Guardzilla

- Authentication
  - All companies implemented reasonably basic authentication systems for their products. (For example, a 2-piece account login portal, a verification-require device registration process, a good password change mechanism, etc.)
  - However, Eufy, Blink, D-Link, Honeywell, Canary, and TP-Link need improvements in their authentication system. For detailed information, check out “Top 10 security features” the companies should implement in their system.
  - Samsung meets 9 of the 10 security features, the most of any product.
- Encryption
  - We did not observe any sensitive information sent unencrypted during our testing.
- Known Exploit Resistance
  - No unfixed disclosed vulnerabilities were found in our tested devices.
- Security Oversight
  - Only the terms of Google Nest, Ring, Honeywell, and Canary state that they regularly conduct security audits or hire a third party to perform security audits for them.
  - Eufy, Honeywell, and Wyze have no mention of internal policies and barriers in place to monitor and limit employee access to personal user information.
- Security over time
  - No vendor states a defined time period for security update support.
  - Most companies claim they will provide updates to their product when it’s needed. However, Samsung has a clear statement that future updates may cause the device to stop working.
- Vulnerability Disclosure program
  - Eufy, Guardzilla, Ring, Blue by ADT, Zmodo, and Toucan have no official vulnerability disclosure program for security researchers to report their findings.

Privacy Coverage

We consider questions inspired by the Digital Standard while we review companies’ publicly available documents. However, not all questions are answered by the companies’ document. The following table shows the percentage of questions answered in our document review process.

Google Nest	94.29%
Samsung	85.71%

Arlo	82.86%
Canary	82.86%
Honeywell	82.86%
TP-Link	82.86%
Blink	80.00%
D-Link	77.14%
Ring	77.14%
Blue by ADT	77.14%
Logitech	74.29%
Amazon	71.43%
Wyze	65.71%
Toucan	57.14%
Eufy	54.29%
Guardzilla	54.29%
Zmodo	51.43%

In our document review process, we found Wyze, Toucan, Eufy, Guardzilla, and Zmodo's publicly available documents answer less than 70% of our questions. That means they should disclose more information regarding how they protect user's data privacy and data security in their public-facing documents like privacy policies or terms of use.

Overall Concerns and Advice for Consumers

- Many companies reserved broad rights to use collected data (including video feeds) for secondary purposes. After consumers purchase the IP cameras, the company becomes the service provider who provides features like live video stream, two-way communication, and others. As the service providers, the company should behave like a data processor to make these features work. However, not all companies do so. Some companies even claim to be data controllers who own user's data, including video recording. In our review process, we found Arlo, Eufy, Ring, Amazon, D-Link, Samsung, and TP-Link claim rights that resemble the rights of data controllers in their terms of use (or terms of service). For example, Eufy states "You grant to eufylife.com a worldwide, irrevocable, non-exclusive, royalty-free license to use, reproduce, adapt, publish, translate and distribute your user content in any existing or future media. You also grant to eufylife.com the right to sub-license these rights, and the right to bring an action for infringement of these rights." Some companies are trying to reserve as many rights as possible. Once a user agrees to those terms of services, the companies may use the user’s data for any purpose. (For example, companies may use users’ data for AI training.)

- In 2019, several stories broke regarding unauthorized access to people’s cams due to possible credential stuffing attacks. We advised consumers to stop using the same password for all accounts and turn on 2-factor authentication if possible. However, 7 out of 14 companies haven’t implemented 2-factor authentication for their accounts yet (Eufy, D-Link, Honeywell, TP-Link, Logitech, Canary, Guardzilla). We strongly suggest consumers buy cameras that support 2-factor authentication.

Main Take Away

2 Factor Authentication

2-factor-authentication system is an easy and effective way to reduce the risk of unauthorized logins. IP cameras are sensitive IoT devices that can record video and audio of a user's home or their office. Consumer Report recommends that all IP cameras should have 2-factor authentication available and prompt users to activate it in the setup process.

Questions in the workbook	Nest	Canary	Logitech	Wyze	Samsung	Blink	Arlo	Ring	TP-Link	D-Link	Amazon	D-Link	Honeywell	Eufy	Guardzilla	Toucan	Zmodo	ADT
Does the product prompt or direct users to set up 2FA in the setup process?	NO	NA	NA	NO	YES	YES	NO	YES	NA	NA	NO	NA	NA	NA	NA	NA	NA	NA
Does the product support multi-factor authentication?	YES	NO	NO	YES	YES	YES	YES	YES	NO	NO	YES	NO	NO	NO	NO	NO	NO	NO

Controller Claims

Who owns the video or audio data which is recorded by my camera? And who can access them? The question may seem simple. But, the answer is not always “users”. The following statements are from companies’ privacy policies.

Controllers	**Controller Coded Segments**	**Comments / Summary**

Arlo	Arlo does not claim ownership of Content you submit or make available for inclusion on the Arlo Services. Nevertheless, with respect to Content (including all related intellectual property rights) you submit or make available for the Arlo Services, you grant Arlo the following worldwide, royalty-free, nonexclusive, perpetual, irrevocable, sublicensable and transferable license(s), as applicable: the license to use, distribute, reproduce, modify, adapt, make derivative works of, publicly perform and publicly display such Content on the Arlo Services and other third-party platforms solely in connection with providing you the Arlo Services, as permitted through the functionality of the Arlo Services and under these Terms. You grant Arlo the right to maintain a copy of the Content (including all related intellectual property rights) for archival and legal purposes.	The user still maintains ownership of their video content, yet the company has the right to freely use shared video content royalty-free in any media format without compensation to the user. The company may also retain a copy of all video content.
Eufy	You grant to eufylife.com a worldwide, irrevocable, non-exclusive, royalty-free license to use, reproduce, adapt, publish, translate, and distribute your user content in any existing or future media. You also grant to eufylife.com the right to sub-license these rights, and the right to bring an action for infringement of these rights.	The user provides the company the right to freely use shared video content royalty-free in any media format without compensation. The company also has the right to license user-generated content to unstated third parties.
Ring	You hereby grant Ring and its licensees an unlimited, irrevocable, fee-free and royalty-free, perpetual, worldwide right to use, distribute, store, delete, translate, copy, modify, display, and create derivative works from such Content that you share through our Services including, without limitation, the Ring Neighbors feature or application, the Ring Community, or via a share link, for any purpose, and in any media format. You agree that you will indemnify Ring for all claims and resulting from Content you share through our Services, including, without limitation, the Ring Neighbors feature or application or Ring Community. If you see Content that you believe violates our Terms, please flag it in our mobile application or report it to us by emailing abuse@ring.com.	The user provides the company the right to freely use shared video content royalty-free in any media format without compensation.

Amazon	Contradictory statements: 3.3 Our Use of Your Files. We may use, access, and retain Your Files in order to provide the Services to you, enforce the terms of the Agreement, and improve our services, and you give us all permissions we need to do so. These permissions include, for example, the rights to copy Your Files, modify Your Files to enable access in different formats, use information about Your Files to organize them on your behalf, and access Your Files to provide technical support. Amazon respects your privacy and Your Files are subject to the Amazon.com Privacy Notice located here. If you do post content or submit material, and unless we indicate otherwise, you grant Amazon a nonexclusive, royalty-free, perpetual, irrevocable, and fully sublicensable right to use, reproduce, modify, adapt, publish, perform, translate, create derivative works from, distribute, and display such content throughout the world in any media. You grant Amazon and sublicensees the right to use the name that you submit in connection with such content if they choose. You represent and warrant that you own or otherwise control all of the rights to the content that you post; that the content is accurate; that use of the content you supply does not violate this policy and will not cause injury to any person or entity; and that you will indemnify Amazon for all claims resulting from content you supply.	The company provides contradictory statements regarding user-submitted content. The Photo/Video ToS states that the company may use "Your Files" content in any manner in order to provide the services to the user. The "General" ToS states that the company the right to freely use shared video content royalty-free in any media format without compensation. The company also has the right to sub-license user-generated content to unstated third parties. Despite this, the company maintains that the user still has full ownership and control of their user-submitted content.
D-Link	D-Link makes no claim of ownership of content such as photographs, videos, messages, information, or materials you submit or make available for or through the Services. However, you grant D-Link worldwide, royalty-free, nonexclusive, perpetual, irrevocable, sublicensable and transferable license(s) to use, distribute, reproduce, modify, adapt, make derivative works of, publicly perform and publicly display such content solely for the purpose of providing you the Services, as permitted by the Services and under the Terms of Use. You grant D-Link the irrevocable right to maintain a copy of such content (including all related intellectual property rights) for all legitimate business reasons and also archival and legal purposes.	The user provides the company the right to freely use shared video content royalty-free in any media format without compensation. The company also has the right to license user-generated content to unstated third parties.

Samsung	Subject to our Privacy Policy (where applicable), for all User Submissions and Device Data, you hereby do and shall grant SmartThings a worldwide, non-exclusive, perpetual, irrevocable, royalty-free, fully paid, sublicensable and transferable license to use, modify, reproduce, distribute, share, prepare derivative works of, display, perform, and otherwise fully exploit the User Submissions and Device Data in connection with the Services, and SmartThings's (and its successors' and assigns') business, including without limitation for promoting and redistributing part or all of the Services in any media formats and through any media channels (including, without limitation, third-party websites and services).	The user provides the company the right to freely use shared user submissions and device data royalty-free in any media format without compensation. The company royalty-free right to license user-generated content to unstated third parties.
TP-Link	. By posting or uploading any content to the Services (including, without limitation, posts, responses, videos, images, and audios) and/or providing any communication or material to TP-Link (collectively, “User Content”), you automatically and irrevocably: 1. Grant and assign to TP-Link a royalty-free, perpetual, non-exclusive, unrestricted, worldwide license to any and all rights in the User Content including without limitation copyright, together with all consents (if any) necessary to enable its reproduction, distribution, modification, publishing, and/or other exploitation by TP-Link and/or by any person authorized by TP-Link, by any means and in all media now known or hereafter devised, without payment or other references to you or any other person, and to advertise and promote such exploitation, for the full period of all such rights (together with any extensions and renewals) and insofar as possible in perpetuity; 2. Waive all moral rights in the User Content which may be available to you in any part of the world and confirm that no such rights have been asserted; 3. Appoint TP-Link as your agent with full power to enter into any document and/or do any act TP-Link may consider appropriate to confirm the grant and assignment, consent and waiver set out above; 4. Warrant that you have the rights to and are the owner of the User Content and entitled to enter into these Terms; 5. Confirm that no such User Content will be subject to any obligation, of confidence or otherwise, to you or any other person, and that TP-Link shall not be liable for any use or disclosure of such User Content; 6. Acknowledge and agree that TP-Link	The user provides the company the right to freely use shared video content royalty-free in any media format without compensation.

	may access, use, preserve and/or disclose the User Content to law enforcement authorities, government officials, and/or third parties, if legally required to do so or if we have a good faith belief that such access, use, preservation, or disclosure is reasonably necessary to: (a) comply with legal process or request; (b) enforce these Terms, including investigation of any potential violation thereof; (c) detect, prevent or otherwise address security, fraud or technical issues; or (d) protect the rights, property or safety of TP-Link, its users, a third party, or the public as required or permitted by law. TP-Link also reserves the right, but shall not be obligated, to remove any User Content from our servers at any time in its sole and absolute discretion.	

Section 3: Overall Suggestions for Companies

Data Security

- Most companies did well in implementing encryption to protect user’s sensitive data and had implemented protections against previously known exploits.
- However, there are some common issues found by our Security evaluation that are areas for improvement:
    - Security Oversight
        - Companies should disclose if they have policies and processes to limit employees’ access to users’ data.
        - Companies should disclose the security audit measures they have put in place for their product or server.
    - Security over time
        - Unsupported connected cameras could be vulnerable to new exploits if they are no longer receiving security updates. Companies should clearly disclose the support period for their products so that consumers can know what the support period is before they decide to purchase that product.
    - Vulnerability Disclosure program
        - Companies should set up proper vulnerability disclosure programs for security researchers to report the vulnerabilities or bugs they found. Good practices for this would include::
            - Having an easy access portal from the official website or a well-known bug bounty site (like HackerOne)
            - Disclosing the estimated timeline of the process
            - Committing to not pursue legal action on security researchers who report bugs or vulnerabilities.
- In addition, all connected cameras should include these 10 basic practices and features, in order to improve the security of these products:

    - Enable automatic firmware/software updates by default
    - Implement protections against credential stuffing and reuse.
    - Provide multi-factor authentication
    - Send email notifications to users when a login occurs from a new device or IP address.
    - Require that users sign back in after changing a password.
    - Confirm with the user when credentials are changed
    - Implement password creation rules for more secure passwords
    - Have compatibility with password managers - such as allowing very long passwords
    - Rate-limit login attempts to increase protection against brute-force dictionary attacks.
    - Provide a visible indication when cameras or microphones are active.

Data Privacy

- Our privacy evaluation consisted of reviewing device controls and UI settings, as well as reviewing the publicly available documentation. Overall, there are several areas where companies can improve their Data Privacy practices or transparency:
    - Data Control
        - The control of data collection and data retention and deletion should be easily accessible by users, and they should be able to easily obtain a copy of their data that was collected.
        - Practices that were put in place to satisfy California or European privacy standards should be available to all consumers, even if they’re not in California or the EU.
    - Data Use
        - Commit to using consumers’ data only to provide services to the user
        - Disclose how user data (especially audio/video data) is used.
    - Data Retention and Deletion
        - Disclose how long user data is retained.
        - Commit to delete the data after users delete their account