Time Will Tell: A Longitudinal Analysis of the Evolution of Security and Privacy of Three IoT Device Types

Swaathi Vetrivel[*], Michel van Eeten[†], and Carlos H. Gañán[‡]

Delft University of Technology

Abstract

Despite significant efforts to enhance the security and privacy (S&P) of IoT devices in recent years, concerns about their S&P remain critical. A compelling question persists: are newer IoT devices genuinely better equipped with S&P features than their predecessors? In this study, we address this gap by leveraging longitudinal S&P testing and rating data from a European Consumer Association known for conducting rigorous, expert-driven assessments of IoT S&P. We focus on three widely used and mature IoT device types – IP cameras, smart printers and smart speakers – and analyse their S&P trends over the past decade. Our findings reveal that overall, S&P ratings have remained relatively stable over the years, with some fluctuations but limited improvement. Additionally, our analysis identifies a surprising trend. There is widespread inconsistent deployment of S&P features across successive device models by the same manufacturer, suggesting a lack of systematic improvement. Results from a Beta Regression Model emphasize the pivotal role of manufacturer-level factors, such as industry experience and headquarters location, in shaping S&P outcomes. These findings underscore the need to develop comprehensive guidelines to help manufacturers operationalise and integrate S&P best practices into their development processes to promote a systematic improvement of IoT S&P.

1 Introduction

Historically, numerous incidents have shaped the narrative of IoT devices having poor S&P, from the infamous Mirai botnet attacks [2] to a class-action lawsuit against Amazon due to multiple instances of Ring cameras being hacked [17] to the alarming case of Xiaomi cameras enabling users to view random video feeds from other users [35].

As a consequence, pressures on manufacturers have mounted to improve the security of their devices. These range from naming and shaming manufacturers [30] to regulatory investigations [10] to the development of new standards and guidelines [15, 29] and, last but not least, new legislation. For example, the EU's Radio Equipment Directive [8] has been imposing binding security requirements on an expanding array IoT product categories and upcoming Cyber Resilience Act will generalize this approach across a much wider range of products [9]. In the US, federal and state laws have also adopted IoT security requirements [19, 32].

These recent developments lead to a critical question: are newer IoT devices genuinely better equipped with S&P features than their predecessors? Singular incidents with IoT devices in the wild cannot reliably indicate trends. The assumption that newer IoT devices would have better S&P features compared to those from a decade ago while reasonable, remains largely unverified. The lack of empirical evidence is not surprising — rigorously assessing the longitudinal S&P features of a substantial number of devices across diverse market segments is a challenging and resource-intensive task, typically beyond the scope of academic research.

In this paper, we address this gap by collaborating with a European Consumer Association (ECA). The partner ECA belongs to a network of consumer associations in different European countries. This network collectively had nearly half a million paid subscribers. They use this funding for device testing. ECA and its peers coordinate to systematically evaluate and rate various aspects of IoT devices, including S&P features, through a network of federated labs across Europe. We obtained a unique dataset that contains S&P ratings from 213 S&P feature tests for 428 IoT devices from 23 manufacturers of three popular and mature device types: IP cameras (released between 2016 and 2024), smart printers (released between 2014 and 2023) and smart speakers (released between 2019 and 2023). These devices were selected for testing by the ECA when they began to gain popularity a few years ago. This allowed us to access longitudinal testing data spanning from the start of the tests to 2024. Moreover, IP cameras and smart printers are overrepresented among compromised IoT devices [2], making them particularly relevant for evaluating

[*]s.vetrivel@tudelft.nl
[†]m.j.g.vaneeten@tudelft.nl
[‡]c.hernandezganan@tudelft.nl

longitudinal trends in S&P features.

Using this dataset, we aim to answer the following research question: *How have the S&P ratings and features of three types of IoT devices evolved over the past years?* We first analyse the temporal trends in IoT S&P ratings over the past decade at both the device type level, so across different manufacturers, and at the level of individual manufacturers, across consecutive models of that device type. Our analysis shows that statistically, the S&P ratings of IP cameras and smart speakers show no significant temporal trend while the ratings of smart printers show a decrease over time. At the manufacturer level, we find that only 3 of 24 manufacturers show an increase in S&P ratings over time. About half of the manufacturers have stable S&P ratings while the remaining manufacturers show erratic changes over time with no clear trends.

Next, we delve deeper into the specific S&P features that underpin the ratings. We find a surprising trend: the stable ratings actually obscure changes at the feature level, meaning that some S&P features are added and some removed from one device to the next from the same manufacturer. This indicates a lack of systematic focus on S&P in the development process of IoT manufacturers. To understand the underlying factors that influence the S&P features, we construct a Beta Regression Model. The model shows that greater experience of the manufacturer both in terms of number of models per IoT device type and the age of the manufacturer increases the odds of having a higher proportion of positive S&P features. It also shows that manufacturers with headquarters in the US have higher odds of having positive S&P features. Overall, we find little evidence for overall improvements in S&P of IoT devices in the three device types, though with some surprising patterns at the level of specific features. In sum we make the following contributions:

- We present the first paper to systematically evaluate S&P features of IoT devices longitudinally. We analyse trends in deployment of S&P features across three IoT device types and across different models from the same manufacturer.
- We uncover a surprising trend in IoT S&P feature deployment. Basic features, such as software update support, are sometimes removed after being included, only to be reintroduced later. This pattern suggests that the S&P features of IoT devices may reflect the S&P of the underlying SDKs used or the differing S&P priorities among various product development teams, rather than a cohesive, overarching manufacturer policies.
- We develop a model to identify the factors associated with the presence of a higher number of robust S&P features in an IoT device. Our findings indicate that manufacturer characteristics have a stronger influence on the presence of S&P features than device-level factors like price.

The rest of the paper is structured as follows: section 2 reviews related work, section 3 provides an overview of the testing process at the ECA and section 4 contains the dataset description. In section 5 we present the analysis of trends in S&P ratings and in section 6, the trends in S&P features. In section 7, we construct a model to explore factors influencing IoT S&P. In section 8 we discuss our findings, offers recommendations and address the limitations, and conclude the paper in section 9.

2 Related Work

To the best of our knowledge, there are no prior papers that have investigated the trends in S&P across IoT device types or the evolution of S&P features on IoT device models from the same manufacturer. The closest is a study by Dong et al. [14] who analysed the Transport Layer Security (TLS) of IoT devices from the same vendor and found only a small fraction of TLS fingerprints are reused by vendors. Other papers have systematically evaluated the S&P of a wide range of IoT devices among which are some devices from the same manufacturer. For instance, Loi et al. [26] conducted independent tests of twenty IoT devices to develop a comprehensive security overview. Among these twenty, there are two manufacturers with two devices each and one manufacturer with three devices. Within this limited dataset, the security test results look quite similar. In contrast, a large scale analysis of IoT devices on home networks revealed that within a set of devices made by the same manufacturer, the percentage of devices with weak default credentials has a wide range from 1.4% to 97.1% [24].

2.1 IoT Vendor Studies

There have also been some prior work studying security practices, like patching, of IoT manufacturers and vendors. Nakajima et al. [28], in their pilot study, found that five out of the six vendors released patches on time. Pérez et al. [31] find similar results with a larger pool of 104 vendors and highlight that IoT-centric vendors release more patches on time than non-IoT-centric vendors. Further, they find no significant relationship between vendor size and patch availability suggesting an absence of economies of scale.

2.2 IoT Security Best Practices

There are many studies that aim to assist manufacturers in improving the S&P of their IoT devices. For instance, the US National Institute of Standards and Technologies (NIST) has outlined foundational security practices of manufacturers with the user at the centre [16] while other solutions are centred around the IoT product life cycle [41]. Bellman and van Oorschot [5] note that 70% of the best practices they analysed in their literature review related to early IoT device life cycle,

highlighting the crucial role of manufacturers in addressing IoT S&P.

A survey conducted by Akiyama et al. [1] among IoT professionals highlighted the complexity of the IoT software supply chain as one of the challenges in managing the IoT software components. Morgner and Benenson [27], through a case study on IoT standardisation, notes that large investments in security are not prioritised due to a lack of consumer demand.

2.3 Security Practices in Organisations

Other studies focus on understanding the S&P development processes within software development in general and not specific to IoT manufacturers. Through interviews with software developers, Assal and Chiasson [4] discovered that best practices in literature often overlook factors involving the team's operational strategies, company culture and security knowledge. Xiao et al. [40] argues that software development companies as social systems and the social factors like policies and cultures influence adoption of secure development tools. Similarly, Arizon-Peretz et al. [3] note that factors like organisational security climate, individualism vs collectivism, security self efficacy and proactive security behaviour influence the adoption of security by design principles.

In sum, our literature review underscores the lack of studies on evolution of S&P in IoT devices or on the evolution of the S&P development processes of manufacturers.

3 ECA Testing Methodology

In this section, we provide an overview of the testing methodology followed by our partner, a prominent consumer association in Europe, who wished the remain anonymous. The partner European Consumer Association (ECA) has around 420,000 paid members as of January 2025. The members get exclusive access to test results of different products including IoT devices. Since these test results are standardized across all European consumer associations, we cannot publicly share the specifics, as manufacturers might exploit this information to achieve a higher S&P rating instead of focusing on holistic improvements. However, we outline the process followed by the ECA, from including a new device type in testing to publishing the results on the website to highlight the rigour in the testing process.

For each device type tested, the ECA assembles a group of experts from various consumer associations across Europe. These experts collaboratively identify key feature/test categories like those mentioned in Table 1 and develop a list of fine grained features or tests specific to each device type and category. Each fine-grained feature is designed to be tested with a binary yes/no result for clarity and consistency. For example, under the category of 'Password Policy', one feature might be having a unique default password, which would be mapped to a specific test question 'Does the device have a unique default password?' This structured approach ensures that each overarching category is rigorously evaluated through multiple precise tests. The number and type of tests vary by category and device type; for instance, while password policy checks are standard across all devices, unique assessments like data security for smart speakers target specific usage contexts. This does not imply that data security is overlooked for IP cameras or smart printers, but rather that ECA prioritizes features most relevant to consumers for each device type. This feature identification and test development is an iterative process and the result is a comprehensive list of tests for each device type. Once the list of tests is identified, the experts also assign a weight to each test based on its relative importance. For example, a unique default password carries more weight than merely supporting ASCII characters. Once the team of experts agree on the tests and weightage, it is passed on to the network of federated labs where the testing is done.

Table 1: List of feature/test categories for each device type

IP Cameras	Smart Printers	Smart Speakers
Password Policy	Setup	Data Security
Standard Installation	Access Controls	Decommissioning
Android App	Password Policy	Password Policy
iOS App	Updates	Network Security
Updates	Permissions	Update Policy
Known Vulnerabilities	Encryption	iOS App
	Authentication	Android App
	Known Vulnerabilities	Privacy Policy
	Decommissioning	

This structured approach ensures objective, consistent testing, limiting subjective interpretation by lab technicians. While other testing methodologies using different S&P constructs might yield different results, we maintain that the rigorous, expert-developed ECA tests eliminate subjectivity and thoroughly assess critical S&P aspects and provide a reliable evaluation of a device's overall S&P posture. Hence, we use these ratings, and the underlying test results in conjunction with the conversion scale – to determine which test outcome gets a higher rating and is therefore better for S&P – in our analysis.

4 Dataset Description

The ratings collected are for three IoT device types – IP cameras, smart printers and smart speakers. In addition to the ratings, we also obtained the binary results from the underlying tests. Since we aimed to analyse manufacturer-level changes in S&P, we use data only from manufacturers with three or more devices. This approach ensures consistency in the data used for both trend and manufacturer analyses, and allows us to meaningfully analyse the trends within individual manufacturers and also the broader trends across manufacturers. In addition, we collected meta data like the release dates

to analyse the temporal dimension of S&P ratings. In some cases, the release dates were available in the ECA dataset, for others used other sources such as manufacturer websites, consumer product launch blogs, date first available on Amazon and so on. Moreover, since prior research has highlighted the importance of organisational factors in security [23, 25], we also collected four variables at the manufacturer level: the headquarters location, founding year and the employee size. These allow us to understand the relative influence of each of these factors in the S&P of IoT devices.

Table 2 gives an overview of the dataset for the three device types. The data set contains 14 IP camera manufacturers, 6 smart printer manufacturers and 3 smart speaker manufacturers. The number of devices per manufacturer varies both between manufacturers within each device type and across different device types. On average each IP camera manufacturer has 8.86 devices, with a median of 6 devices. In contrast, manufacturers of smart printers have an average and median of 53 devices, whereas smart speaker manufacturers have an average and median of only 4 devices. This stark difference reflects underlying market dynamics. The smart printer sector features a broader range of products from many manufacturers, resulting in a higher number of devices per manufacturer. In contrast, the smart speaker market is more concentrated, dominated by a few major players who offer limited product lines with mostly incremental updates.

The release date ranges differ per device type, with smart printers having the longest range of almost a decade, IP cameras having a range of eight years and smart speakers having the smallest range of about three and a half years. This also reflects the time periods when the device types saw an increase in popularity. With regards to the headquarters (HQ), almost half of the manufacturers (11/23) have HQ in the US, six in China, three in Japan and one each in the Netherlands, Sweden and Taiwan. Both the oldest (established in 1840) and the newest (established in 2016) manufacturers are IP camera manufacturers. The smallest manufacturer in terms of employees is an IP camera manufacturer with a mere 108 employees while the largest manufacturer is a smart speaker manufacturer with around 1.5 million employees.

5 Trends in IoT Security and Privacy Ratings

In this section, we address our first research question regarding the evolution of S&P ratings of three IoT device types over the years to understand the underlying trends. We examine trends at two levels: at the device type level across all manufacturers and also at the manufacturer level across different IoT device models from the same manufacturer.

5.1 Evolution of S&P Ratings at the Device Type Level

Figure 1 shows the distribution of S&P ratings of the three IoT device types over the years. The test results are available from 2014 for smart printers, from 2016 for IP cameras, and from mid-2019 for smart speakers. These dates reflect when each device type gained popularity, prompting the European Consumer Association to include them in their testing. Moreover, within the popular device types, the ECA chooses to test only the specific device models that are popular in the European market in order to maximise the effectiveness of the results for their members. The higher popularity of IoT devices tested by consumer associations has also been empirically verified in an earlier study [39].

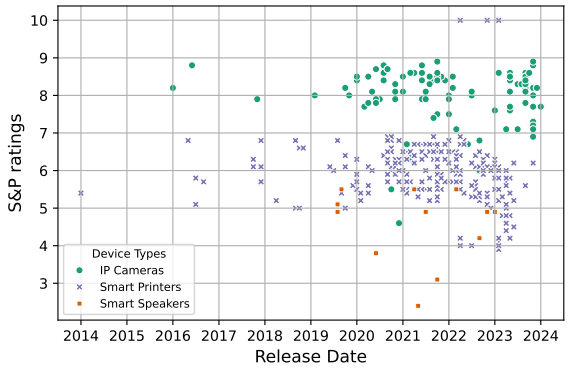


Figure 1: Temporal Evolution of S&P Ratings of IoT devices

We observe that the S&P ratings for each device type have different ranges. Smart speakers have the narrowest range and the lowest S&P ratings, ranging from 2.4 to 5.5, with an average of 4.39. Smart printers have a broader range of ratings from 3.9 to 10, with a higher average of 5.98. The S&P ratings of IP cameras range from 4.6 to 8.9, with an average of 7.9. This suggests that S&P profiles vary across IoT device types, highlighting the need to consider each type individually rather than treating grouping all IoT devices in a single category.

In order to systematically evaluate the trends in the S&P ratings of these devices, we conducted a statistical trend analysis using Mann-Kendall test, a non-parametric test that is commonly used to analyse time series. We used the pyMannKendall library in Python [20] to run the test for each device type separately. Our analysis showed no trend in the S&P ratings of IP cameras and smart speakers, and a decreasing trend for smart printers. This is inline with industry trends that show that printers were 68% more likely to be a source of a threat or breach in 2023 when compared to 2016 [34].

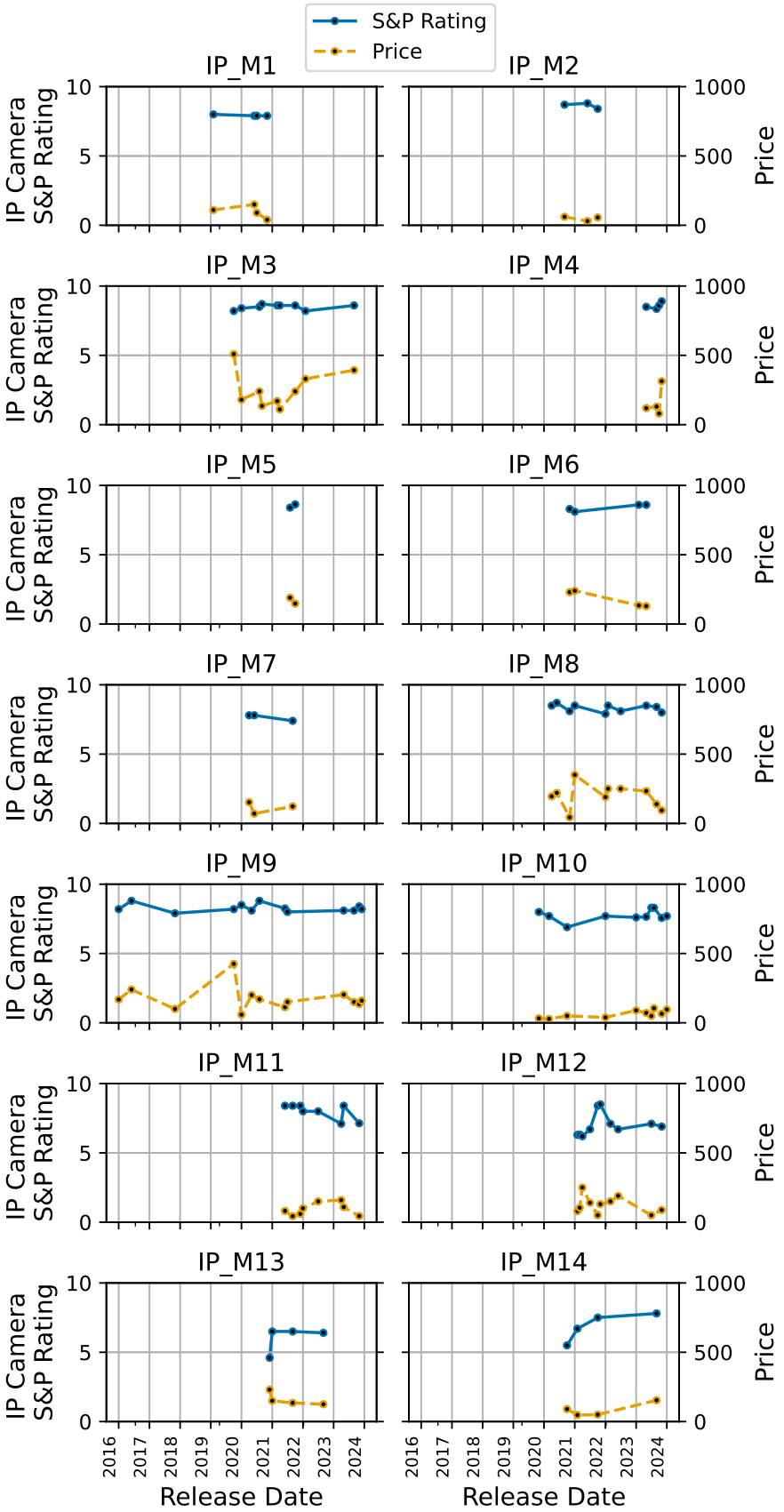


Figure 2: Evolution of S&P ratings and Price of IP cameras per Manufacturer

Device Type	# Tests	# Mfgs.	Avg. # Devices	Price Range	Release Date Range	Mfg. HQs	Founding Year Range	Mfg. Size Range
IP Cameras	79	14	8.8	$29.12 – $832.00	Jan 2016 - Jan 2024	China, Sweden, Taiwan, USA	1840 - 2016	108 - 182,502
Smart Printers	60	6	53	$46.70 – $861.10	Jan 2014 - Nov 2023	Japan, USA	1906 - 1991	9000 - 184,034
Smart Speakers	74	3	4.3	$29.50 – $665.60	Aug 2019 - Jan 2023	The Netherlands, USA	1943 - 2002	1,844 - 1,525,000

Table 2: Overview of the dataset

5.2 Evolution of S&P Ratings at the Manufacturer Level

Next, we study the temporal trends in the S&P ratings of different IoT devices from the same manufacturer. We analyse the ratings of each device type separately to understand if there are differences in manufacturer behaviour across the device types.

5.2.1 IP Cameras

The IP cameras in our dataset come from 14 different manufacturers. Each manufacturer has between 3 and 24 IP cameras. The average S&P rating for the 14 manufacturers ranges from 6.15 to 8.65. Figure 2 shows the evolution of S&P ratings and price of IP cameras over time. We observe three distinct temporal patterns. First, for nine manufacturers, IP_M1 to IP_M9, the S&P ratings have remained stable throughout the analysis period. Notably, all of these manufacturers started with high initial S&P ratings that have consistently stayed in the high ranges. The average S&P rating for the manufacturers in this group – 8.3 – is the highest of all three patterns. Second, three manufacturers, IP_M10, IP_M11 and IP_M12, show some fluctuations in the S&P ratings over time, with an average rating of 7.4. In the third pattern two manufacturers, IP_M13 and IP_M14, both started with a low S&P rating but have shown consistent increase over the observation period. Manufacturer IP_M13 has an average S&P rating of 6.2 and IP_M14 has an average S&P rating of 6.9. Overall, we find no decreasing trends in the S&P ratings of these manufacturers. Most manufacturers have maintained a stable rating over the years, a few show some fluctuations while a couple exhibit a steady increase in their S&P rating.

We observe fluctuations in the prices of IP cameras released by each manufacturer over the years, possibly due different market segments being targeted with the differential pricing. Consistent with earlier studies, we also find a statistically significant mild positive correlation between the price of IP cameras and the S&P rating [38].

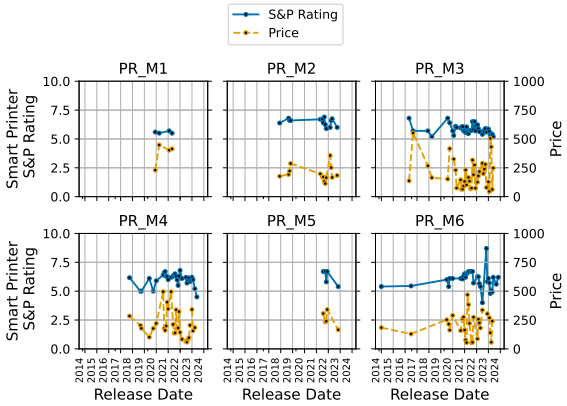
5.2.2 Smart Printers

There are six smart printers manufacturers in our dataset each with between 6 and 107 printers. We observe two temporal trends in the evolution of S&P ratings over time (Figure 3a). First, PR_M1 and PR_M2 have relatively stable ratings, while the ratings of the other manufacturers fluctuate. Notably, we do not observe any manufacturer with a consistent increase in S&P ratings. Moreover, unlike IP cameras, smart printer manufacturers with stable ratings do not have high S&P ratings. The average S&P ratings of PR_M1 and PR_M2, with a relatively stable S&P rating, is 6.3, while the average rating of the other four manufacturers is 5.9. PR_M1 has the lowest average S&P rating of 5.6, while PR_M5 has the highest with 6.3. We do not observe any statistically significant correlation between the S&P ratings and prices of smart printers.

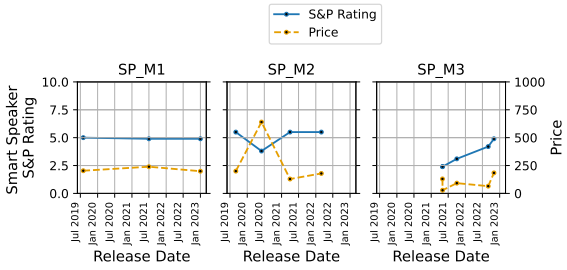
5.2.3 Smart Speakers

There are only three smart speaker manufacturers in our dataset, two with four devices and SP_M3 with five devices. The S&P ratings of the four devices from manufacturers SP_M1 and SP_M2 are almost identical with only a maximum of a 1.5 point variation. The five devices from SP_M3 show a higher variance. The average S&P ratings for the three manufacturers are 4.9, 5 and 3.4 respectively.

We find that each smart speaker manufacturer has a distinct temporal pattern (Figure 3b). Manufacturer SP_M1 maintains a stable S&P rating over time, with an average of 4.9. In contrast, manufacturer SP_M2, with an average of 5.1, shows a



(a) Smart printers



(b) Smart speakers

Figure 3: Evolution of S&P ratings and price per manufacturer for selected IoT device categories.

steep decline in the ratings of one of its devices. Manufacturer SP_M3 shows an increasing trend in S&P ratings, with an average of 3.4. The number of smart speakers in our dataset is insufficient to conduct statistical tests. However, visually, we observe a negative correlation between S&P ratings and price, consistent with earlier studies [38], particularly evident for manufacturer SP_M2.

6 Trends in IoT Security and Privacy Features

In this section, we analyse the evolution of S&P features captured by the tests. Similar to the ratings, we analyse both at the device type level and at the manufacturer level.

6.1 Evolution of S&P Features at the Device Type Level

At the device type level, we analyse the evolution of the S&P features to get a broader perspective of where the industry is moving in terms of IoT S&P.

6.1.1 IP Cameras

We find that IP Cameras have consistently had good S&P features in certain areas especially in Data Privacy and Permissions. For instance, all the cameras in our study have a thorough account deletion feature and do not leak any user data on account deletion. The apps on both Android and iOS allow for opting out of data collection, and for usage of main app features even when not all requested permissions are provided. However, we also find some room for improvement. For example, secure remote connections are still not commonplace, and apps often fail to explain the consequences of declining the privacy policy or denying permission requests. Additionally, support for some features has changed over the years. For instance, while all IP cameras since 2016 have update support, between 2017 and 2022 there was a decrease in the number of IP cameras providing automatic security updates. Moreover, since 2017, lesser number of devices provide a manufacturer statement about the duration of update support. On a more positive note, there has been a marginal increase in the number of devices supporting offline functionality since 2019.

6.1.2 Smart Printers

We find that only a few S&P features in smart printers have been consistently steady since 2014. This includes offline functionality, encrypted network communication, and online user access control. Some features have not improved over the years; for instance, communication is still only encrypted on the device and not on the mobile apps. Users lack options

for advanced content encryption, and secure connection protocols are generally not used. Moreover, secure communication support in most mobile apps has declined since 2021.

Nevertheless, we observe an improvement in certain S&P features over time. For instance, since 2019, an increasing number of printers offer automatic updates via the web portal. Regarding data privacy and permissions, we observe variations in the proportion of devices with privacy-friendly features. Between 2014 and 2016, all printers had personalised marketing disabled by default. This dropped to 20% by 2018, rose again by 2020, and has since declined – highlighting the fluctuating state of S&P features in smart printers.

6.1.3 Smart Speakers

The number of smart speakers in our dataset is much smaller than that of IP cameras and smart printers, a possible artifact of the high market concentration for smart speakers. We find that smart speakers have steady and robust S&P features in many areas, such as updates, account deletion, and factory reset — every smart speaker in our dataset supports updates and has automatic updates enabled. However, none of the speakers include a manufacturer statement about updates. Similarly, there is room for improvement in privacy and permissions, as none provide information to consumers on the consequences of denying access. Offline functionality was introduced in 2021-22, with about half of the devices supporting it, but this has since dropped to none.

6.2 Evolution of S&P features at the Manufacturer Level

Next, we study the changes in the S&P features between consecutive IoT device models from the same manufacturer. We define a 'change' as any feature variation between two consequent devices released by the same manufacturer. For instance, considering manufacturer SP_M1 who released smart speakers in July 2019, July 2021 and January 2023, we categorise as change, any feature change between the 2019 and 2021 models or between the 2021 and 2023 models. Since each test captures a unique aspect of a S&P feature, we use the term tests and features interchangeably based on the context for ease of reading.

We further classify each change as increasing, decreasing or mixed based on how it impacts the S&P rating. The ECA uses a conversion scale to translate the test results to S&P ratings. Based on this scale, we determine whether a feature change leads to an increase or decrease in the S&P rating. For instance, if a manufacturer has six devices and the first two devices do not support automatic updates but the last four do, we would categorise this as an increase in S&P since ECA's conversion scale gives a higher S&P rating to devices that support automatic updates. Conversely, if the first two devices support automatic updates but the last four do not, we would categorise this as a decrease in S&P since the lack of automatic updates in the latter devices would lower the rating. However, not all feature changes are consistent and we categorise these as mixed. For example, if the first two devices support automatic updates and the next two devices do not support while the last two do, we categorise this as mixed. Additionally, we also have a stable category to denote features that have remained stable over the duration of analysis. These classifications helps analyse a manufacturer's committent to S&P which would be reflected in the trends of feature changes across their devices over time.

Further, for each device type, we analyse the trends in specific features (eg: update support) that show a high degrees of changes across all manufacturers. This gives insights on specific features that are challenging for manufacturers to implement consistently across their devices.

6.2.1 IP Cameras

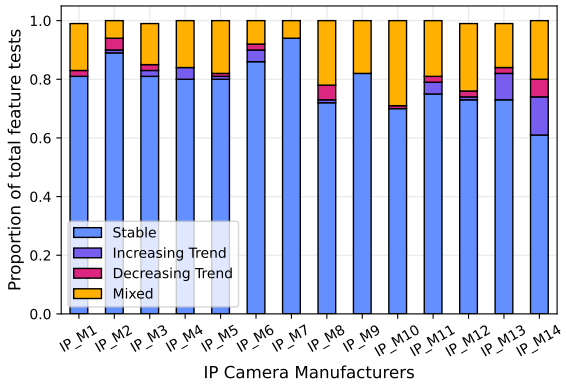


Figure 4: Proportion of feature changes per IP camera manufacturer in each temporal trend

In total there are 79 features that are tested for IP cameras and 60% of the features are stable across all devices from the 14 IP camera manufacturers. However, we also find all manufacturers have at least a few features that change between consecutive device models, the lowest being IP_M7 with 6.3% of feature changes and the highest IP_M14 with 39.2% changes between device models. We find a vast majority of these feature changes per manufacturer – ranging from half to all – have a mixed trend: they fluctuate between leading to an increase or decrease in ratings. IP_M13 has the highest number of changes (7 of 21) that led to an increase in rating while IP_M2 has the highest proportion of changes leading to a decrease (3 of 9). Three manufacturers do not have any changes that led to a decrease in S&P rating.

Figure 4 shows a stacked bar plot of the changes in for the four categories across the 14 manufacturers. Despite the observed positive correlation between the S&P rating and price at the device type level, we do not find any strong indication

of price-based deployment of S&P features. Next, we analyse the features that have a high number of changes across all manufacturers – automatic update support, open ports on a device, unauthenticated password reset, offline functionality, encrypted cloud communication and app permissions.

Automatic Update Support Automatic update support is crucial to ensure that an IP camera stays up-to-date with security patches. However, only 5 of 14 manufacturers have information on automatic update support for all their devices. For the remaining 9 manufacturers, the lab was not able to find the information for at least one of the devices, and in the case of IP_M8 and IP_M11, for about half of their devices. This highlights the difficulty of finding information related to automatic updates, and update support in general. When trained professionals struggle to find the information, it would be even harder for consumers. This aligns with another study that notes that information related to update support is not easily available even in trusted sources like user manuals and manufacturer websites [37].

Further, only two manufacturers, IP_M6 and IP_M9 offer automatic update support on all of their devices. In contrast, two other manufacturers, IP_M11 and IP_M12 - based on available update support information - do not offer automatic update support on any of their devices. Apart from these four manufacturers, all the other 10 manufacturers have at least one device that supports automatic updates and one device that does not. This inconsistency is intriguing, because if a manufacturer has the technical capacity to implement automatic updates on one device, they could potentially extend that capability to all subsequent devices. However, we see clear evidence of such capacity building over time in only two manufacturers. IP_M10 and IP_M13 did not initially offer automatic updates but introduced the feature in their later models. For the other eight manufacturers, the support for automatic updates remains inconsistent across their devices, reflecting a lack of systematic implementation.

Unnecessary Open Ports on a Device It is a common best practice to close unnecessary ports – those not needed for network functionality – to prevent unauthorised access. We find four patterns. Five manufacturers do not have any unnecessary open ports on any of their devices. Four manufacturers show a positive trend of improvement over time: their initial devices have open ports but not the latter devices. One manufacturer, IP_M13, has open ports on all their cameras. Lastly, four manufacturers have open ports on some of their cameras.

The first three patterns could be attributed to a manufacturer's security posture. Strong focus on security leading to a 'deny by default' stance, evolving security practices causing newer devices to have no unnecessary open ports, and a higher priority placed on ease of use reflected in all devices having open ports. The last pattern, with open ports on some but not others could indicate a lack of a strong manufacturer wide security posture.

Unauthenticated Password Reset Since most IP cameras do not have a UI interface, they are mostly managed through an app. While some IP cameras support password reset through the app or via sending an email to the registered email id, some other cameras do not have this support. Instead, the only option if a consumer has forgotten the password, is to reset the device to factory settings, typically done through a physical reset button on the camera. This allows anybody with physical access to the IP camera to reset the device and set a new password and is hence a vulnerability from the security perspective. Only six manufacturers do not allow such unauthenticated password reset on any their cameras, while five manufacturers have addressed it over time - their latter cameras block unauthenticated password reset. With the other three manufacturers, we again find an inconsistent pattern. IP_M1 and IP_M14 allow unauthenticated password reset on all their cameras except one while IP_M9 allows it on 9 of 24 devices.

Offline Functionality The primary functionality of IP cameras of four manufacturers is unavailable when the internet connection is lost, even if the loss is only temporary due to a lack of offline storage. Further analysis of the devices, based information on the internet like user manuals, shows that two manufacturers IP_M2 and IP_M3 support local storage via a dedicated device that has to be purchased separately while IP_M7 and IP_M11 only support cloud storage. In contrast, all devices from manufacturers IP_M5 and IP_M6 can be used even when the internet connection is lost temporarily. The other ten manufacturers have inconsistent support - some devices work through a temporary internet connection loss and some that do not. Of these, three manufacturers supported basic offline functionality in the earlier devices but not in the later devices. In contrast, only one manufacturer did not support offline functionality in the earlier devices but supports them in the later devices.

Three of the four manufacturers whose devices cannot perform the primary functionality without internet, also cannot perform basic functions if the cloud service permanently shuts down. All devices from IP_M5 and IP_M6 can withstand temporary loss of connectivity and two of the six devices from IP_M6 are also robust to the cloud service shutting down. We observe both an improvement and decline in offline functionality in face of cloud service shutting down over time. IP_M4 did not support offline functionality in the initial devices, but introduced it in the latter devices while three other manufacturers had offline functionality in the earlier devices but not in the latter devices. For three other manufacturers, some devices support primary functionalities even if the cloud service were to shut down while the others do not.

Encrypted Cloud Communication Most IoT devices connect to the cloud either for basic or advanced functionality. Due to a lack of user interface on most IoT devices, there are corresponding mobile apps that allow a consumer to configure and manage their IoT device, and enable remote access. The app typically connects to a cloud service for multiple functions – to act as a gateway to the device itself, to provide advanced data processing and analytics, for application hosting and so on. From a S&P perspective, it is crucial that - irrespective of the function - the communication with the cloud is secure, although the consequences of lack of secure communication might be worse in some functions than others.

In our analysis, we observe differences in the implementation of encrypted cloud communication between android and iOS apps. Half of the manufacturers offer encrypted communication on both android and iOS apps while two manufacturers support encrypted communication only on the iOS app and not on the android app. Moreover, while most manufacturers encrypt Personally Identifiable Information (PII) on both apps, three manufacturers send PII unencrypted for some devices. Of these three manufacturers, two manufacturers show a decline over time, they encrypt PII on their initial devices but not on the latter ones, while the other manufacturers shows improvement over time - their latter devices support PII encryption.

App Permissions We also observe differences between android and iOS apps in terms of the app permissions. While nine manufacturers do not request excessive permissions - more permissions that what is needed for device functionality - on either app, six manufacturers ask for excess permissions on the android app but not on the iOS app. Of these, two manufacturers have a positive trend: their initial devices ask for excessive permissions but the latter devices do not.

6.2.2 Smart Printers

Among the three device types under consideration, smart printers have the lowest proportion of features that are stable and the highest proportion that change over time. There are 60 feature tests for smart printers, and only one feature has remained consistent across all devices of all manufacturers. The remaining 59 features have changed in at least once printer from each manufacturer. Moreover, only one manufacturer (PR_M2) has a change that led to an increase and two manufacturers (PR_M3 and PR_M5) have a change each that led to a decrease. All the remaining 56 feature changes show a mixed pattern alternating between leading to increase and decrease in ratings. The proportion of features that change varies across manufacturers. PR_M6 has changes in 57 of 60 features (95%), while both PR_M1 and PR_M5 have changes only in five features (8.3%). Figure 5 shows the proportion of tests of smart printers that are stable and the proportion with changes that are increasing, decreasing or mixed. Similar to IP cameras, there is no correlation between the price of the printer and the availability of the S&P features tested. We now analyse features that have a high number of changes across all manufacturers: setup, web portal access, updates and mobile app privacy.

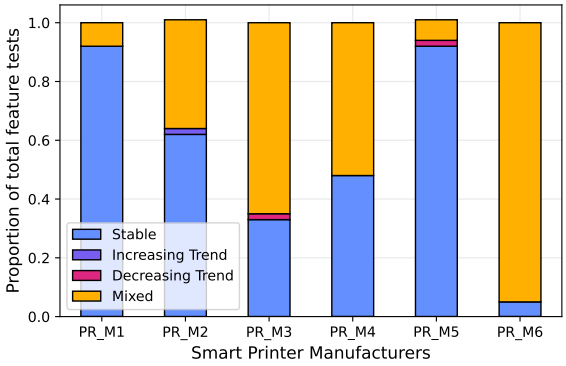


Figure 5: Proportion of feature changes per smart printer manufacturer in each temporal trend

Setup With respect to the setup of the printers, we find an inconsistency between devices from the same manufacturer in the modes supported during setup. Only two manufacturers create a WiFi access point for setup across all their devices. The remaining manufacturers create a WiFi access point only for a subset of their printers. However, this highlights the trade-off between ease of use and security: most devices that allow creating WiFi access points during setup can also connect to WiFi networks without a password or without security standards like WPA2.

Using HTTP for the admin configuration exposes sensitive information to interception and tampering due to the lack of encryption and integrity checks and has more been replaced by the more secure HTTPS. However, two manufacturers still use HTTP by default for admin configuration on all of their devices and the other four manufacturers use it on a majority of their devices despite supporting HTTPS. It is puzzling that manufacturers who have the capacity to use stronger, more secure protocols like HTTPS would still use HTTP as default in a majority of their devices. On similar lines, we find that only one manufacturer supports encrypted communication with the mobile app on all of their devices, the other support it on a majority of their devices but not all devices. Similarly, only three manufacturers have up-to-date TLS certificates on all of their devices, the others do not have up-to-date certificates in around 1 to 7% of their devices.

Web Portal Access Although brute force attacks are a common threat to web applications, only one printer manufacturer, PR_M4, protects against brute force attacks on the web portals of all their devices. In contrast, PR_M6 does not support

brute force protection on the web portal on any of their devices while the other four manufacturers support on some devices but not on the rest. Of these, only PR_M2 shows an improvement over time, introducing brute force protection their later devices.

By default, the web portals of all devices from two manufacturers, PR_M1 and PR_M5 do not have any default password - anybody on the same network with the IP address would be able to connect to the device. In contrast, PR_M2 has a default password for all their devices which is typically printed out of plain sight on the printer itself like on the bottom or in the battery cavity. The remaining three manufacturers have a default password for some of their devices but not for the others. Moreover, once configured, the authentication systems of PR_M1 and PR_M5 ask for both username and password, while the rest of the manufacturers use both only for some of the devices, the other devices ask for only a password. With regard to password reset, across all their devices, both PR_M1 and PR_M5 allow a password change without entering the previous, while PR_M4 requires the older password for a password change. The other three manufacturers require the old password on some of their devices but not on the other devices. This high level of variance in the implementation of even basic S&P functionalities like setup and passwords highlights a lack of a standardised approach to S&P at the manufacturer level.

Updates Five of the six manufacturers support one-click updates on some printers but not on the others. For the sixth manufacturer, no update procedure related information could be found. Moreover, none of the manufacturers offer consistent support on both the web portal and mobile app for automatic firmware updates. PR_M2 supports configuring automatic firmware updates from the web portal for a minority of devices but not from the mobile app. PR_M3 supports configuring automatic updates from both but only on a subset of devices. The remaining four manufacturers do not support automatic firmware update configuration via the web or app.

Mobile App Data Privacy The mobile apps of the printers from all of the manufacturers ask for a wide range of permissions from WiFi and fine location access to camera and cloud messaging permissions. Although some of these permissions might be not crucial for the basic functioning of the app, only the app of PR_M1 works across all devices even when the permissions are declined. In contrast, none of the devices of PR_M2 work if the permissions are declined. The apps of the other manufacturers work even when permissions are declined in some devices but not in the others.

With regards to the privacy policy, for none of the devices of PR_M1, the corresponding apps explain what happens if the privacy policy is declined. For the other manufacturers, it is explained for some devices but not for the others. From a user perspective, especially if it is an inexperienced user, such explanations are useful to understand the trade offs between privacy and functionality. A lack of consistency even among devices from the same manufacturer might cause frustrations to such users.

A deeper look at the app SDK reveals that targeted adverting is turned off by default for the apps of all devices of PR_M1. The other manufacturers have it turned off by default in some devices and turned on by default in other devices. This suggests that these decisions are probably made at the product level rather than based on a organisation wide S&P policy.

6.2.3 Smart Speakers

Of the three device types under consideration, smart speakers have the lowest proportion of tests with changes. There are 74 tests for smart speakers and 58 of these (78%) remain stable across all devices and manufacturers. Moreover, a majority of the feature tests with changes have a mixed trend. SP_M1 has a mixed trend for all changes. SP_M3 has one feature with an increasing trend and two with a decreasing trend while SP_M2 has one feature with a decreasing trend, the remaining feature changes show a mixed trend. Figure 6 shows the distribution of changes in each of the trends for smart speakers. SP_M3 has the highest percentage of features with changes – 21.6% (16 of 74) while SP_M1 and SP_M2 have only 4 and 5 features with changes (5.4% and 6.8% respectively).

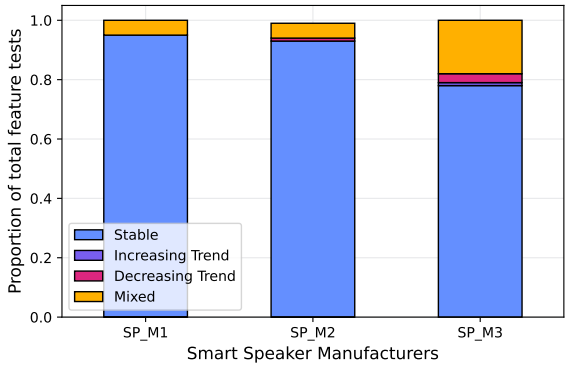


Figure 6: Proportion of feature changes per smart speaker manufacturer in each temporal trend

The S&P settings of smart speakers across manufacturers are relatively homogeneous. The main point of difference is the availability of offline functionality. While none of the devices of SP_M1 support any offline functionality, one of the four devices from SP_M2 - the most expensive, costing three times more than the next most expensive speaker – does support offline functionality. Two out of five devices from SP_M3 also support offline functionality, but there is no correlation with price.

7 Factors Influencing IoT Security and Privacy

To understand the factors influencing S&P features of IoT devices, we constructed a Generalized Linear Model (GLM) using the glmmTMB package in R [6]. The dependent variable in our analysis is the proportion of positive S&P features for each device. For example, if a smart printer achieves positive results, meaning results that are better for S&P, in 30 out of 60 S&P features, the proportion would be 0.5. Using the proportion of positive features allows us to compare the results across the three device types irrespective of the differences in the number of feature tests per device type. Additionally, compared to S&P rating, this allows for more transparency by eliminating the effect of the weights from the analysis. We use a Beta Regression Model which is best suited for proportions between 0 and 1.

We consider six predictor variables: two at the device level and four at the manufacturer level that have been identified in prior work as influencing an IoT devices' S&P [31]. At the device level, we include the categorical variable for device type and the device price. At the manufacturer level, we include the number of devices from the manufacturer in our dataset as a proxy for the diversity of device models they produce. We also account for the manufacturer's size (measured by the number of employees), the number of years since its founding, and the location of its headquarters. To standardise our analysis, we use scaled and centred values for variables such as price, number of devices, manufacturer size, and years since founding. Scaling ensures that all variables are on a similar scale, preventing any single variable from dominating the analysis. Centring adjusts the variables so their means are zero, which makes the intercept more meaningful and interpretation easier. Multi-collinearity tests showed that none of the variables were highly correlated, confirming their suitability for inclusion in the model.

We added the six variables in a step-wise forward manner, starting with the intercept only model and then adding the other variables, resulting in a total of seven models as shown in Table 3 in Appendix A.1. We evaluated different orders for adding the variables in the model but found no differences based on the ordering. To assess model fit, we used the Akaike Information Criterion (AIC), Bayesian Information Criterion (BIC), and Log-likelihood, based on established guidelines from the literature [7, 12, 18, 22]. The AIC helps balance model accuracy and complexity, reducing the risk of overfitting, while the BIC places greater emphasis on simplicity by applying a stronger penalty for model complexity. Thus, lower AIC and BIC values indicate a better-fitting model. The Log-likelihood measures how well the model accounts for the observed data, with higher values suggesting a better fit. Based on these criteria, we identified Model 6 to be best fit among the models in Table 3 (Appendix A.1) since it has the lowest AIC and BIC values and the highest log-likelihood among all the models.

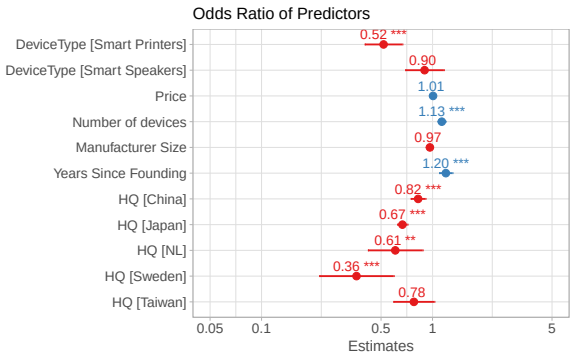


Figure 7: Odds-Ratio of the Predictors from the Beta Regression Model. For categorical variables, the following reference categories were used: DeviceType = IP Cameras, HQ = USA.

Figure 7 shows the odds ratio of each of the predictors. The odds ratio denotes how a one-unit change in a predictor variable affects the odds of observing a higher or lower proportion of positive S&P results. For instance, the device type of smart printers has an odds ratio of 0.52. This indicates that, all else being constant, a smart printer has 48% lower odds of having positive S&P features compared to the reference category of IP cameras. The estimates for the other two device-level variables — the device type of smart speakers and device price — are not statistically significant.

At the manufacturer level, three variables are statistically significant: number of devices, years since founding and manufacturer headquarters; the size of the manufacturers has no significant effect. We observe that, all else being equal, a one unit increase in the number of devices or the years since founding is associated with a 13% and 20% increase, respectively, in the odds of having positive S&P features. This suggests that a manufacturer with greater experience, whether measured by age or by having released more models, tends to have higher odds of positive outcomes in the S&P tests. With regards to headquarters location, we find that a headquarter located in China, Japan, the Netherlands or Sweden decreases the odds of having positive results in S&P tests compared to the reference category of having headquarters in the United States. Specifically, the odds are 12% lower for China, 33% lower for Japan, 39% lower for the Netherlands and 64% lower for Sweden. This indicates that IoT devices from manufacturers with headquarters in these countries are less likely to have devices with positive S&P results compared to devices from manufacturers based in the United States. This could be due to various factors such as differences in regulations, enforcement regimes, manufacturing practices, or organisation culture in different regions.

8 Discussion

The main objective of our study was to determine whether manufacturers have improved the S&P of IoT devices over the years. Overall, our analysis finds limited evidence of improvement and uncovers a surprising trend. There is widespread inconsistent deployment of S&P features in successive IoT device models from the same manufacturer. Our analysis shows that even basic and critical S&P features like software update support are sometimes removed after being included only to be reintroduced later. We observe such fluctuating, inconsistent S&P feature deployments across all device types and manufacturers, in varying degrees.

These inconsistencies bring to focus the crucial and often overlooked role of the development process of manufacturers in determining S&P outcomes. A lack of structured development process with checkpoints at critical junctures to assess the S&P requirements could be one of the reasons for the inconsistencies. These manufacturers might face resistance towards implementing these checks due to entrenched organisational norms and cultures [36]. Even within a structured and established S&P development process, the underlying complexities of the IoT supply chain can impact S&P at the manufacturer level [1] like technical and contractual limitations in SDKs provided by chip vendors. Differences in the S&P priorities and feature implementations across different product development teams could also contribute to these inconsistencies. Overall, these indicate a lack of coherent S&P development framework at the manufacturer level.

The results of the Beta Regression Model also highlight the crucial role of the manufacturers. It shows that the proportion of positive S&P features in an IoT device is influenced by the location of the headquarters of the manufacturer and their experience both in terms of the number of models produced and years since founding. Contrary to other studies that suggest price of the device influences S&P [39], our model results show that device price has no significant influence when manufacturer level attributes are taken into account.

The importance of manufacturer experience emphasises the need for targeted support for manufacturers, especially smaller and newer ones who lack the needed experience. Such support can help them establish and maintain consistent S&P development practices and processes. Moreover, while principles like security by design - recommended in policy standards – are valuable, manufacturers also need practical guidance to operationalise these principles within their development process [21]. Additionally, the differences in S&P trends across various IoT device types highlight the necessity for tailored support specific to the needs of the development process of each device type, rather than a one-size-fits-all approach. Manufacturers in need of an overhaul to the S&P development processes can be suggested adequate mechanisms to overcome the organisational resistance to change and implement mechanisms for continuous improvement. Similarly, manufacturers with an inconsistent S&P implementation across devices can be helped with creating a robust, structured approach to incorporating S&P within their development processes.

Overall, our results show that despite the introduction of various regulations and legislation, there has been little improvement in the S&P of the three IoT device types analysed in our study. Interestingly, our model results suggest that manufacturers headquartered in the US which operates under a less stringent regulatory environment compared to Europe, have higher odds of producing devices with more robust S&P features. This could be attributed to stricter enforcement actions [11] or the prevalence of legal repercussions, such as class action lawsuits, which are more common in the US [17]. These findings highlight the limitations of relying solely on market-driven regulations, which can lead to inconsistent S&P feature implementation based on the target market. Promoting awareness among manufacturers about codifying S&P best practices [33] into their development processes could help ensure consistency and reinforce existing regulations.

8.1 Limitations

Due to our contractual agreement with the ECA, we cannot disclose the partner details, the test specifics, or names of the manufacturers and devices. While this limits the verifiability of the test results, we would like to highlight the strong reputation and ethical standards upheld by European consumer associations which lends a high level of confidence in the integrity and reliability of the testing process. Furthermore, our feature-level analysis specifies exactly which functionalities have remained stable or changed, offering valuable insights even in the absence of full test disclosure.

Our analysis is based on a limited dataset of IoT device S&P ratings from three device types and 23 manufacturers, which may not represent all manufacturers or device types. However, since consumer associations select popular devices for testing [39], we believe the analysis reflects trends in widely used IoT devices in Europe. It may not, however, capture trends in niche or emerging IoT device types. Another limitation is the accuracy of release dates, which were collected from various sources and may not always be precise. While ECA tests have remained consistent over time, there may be minor lab-specific variations that might introduce slight inconsistencies. Nevertheless, since we focus on broader trends, our findings remain robust to such variations.

Our analysis focuses on S&P features assessed by the ECA, which include a wide range of common S&P attributes in line with regulatory best practices. This implies that our findings provide valuable insights into most commonly recommended S&P features but may not capture trends in more specialized or emerging S&P aspects. Finally, we acknowledge that there are factors influencing IoT S&P features like supply chain dependencies, firmware practices, or third-party integrations that we were not able to include in our model. Despite this,

the statistical significance of manufacturer-level factors in our analysis emphasizes the role of organisational processes in shaping S&P outcomes, extending beyond purely technical measures. Future research could explore these factors to provide a deeper understanding of the broader IoT S&P ecosystem.

9 Conclusion

In this paper, we analysed the evolution of S&P features over the past decade in 428 IoT devices from 23 manufacturers, focusing on three widely used and mature IoT device types: IP cameras, smart printers, and smart speakers. Our findings indicate that while IP cameras maintained consistently high S&P ratings, smart printers exhibited lower ratings with a slight declining trend, and smart speakers had the lowest ratings with no clear temporal pattern. At the manufacturer level, only a minority (3 out of 23) demonstrated improvement, while the majority (12 out of 23) maintained stable S&P ratings, and the remaining eight showed no clear trend in the ratings.

Our analysis also uncovers a surprising trend of inconsistent deployment of S&P features in subsequent device models of the same manufacturer. We find that the stability in ratings obscures such underlying inconsistencies. This highlights a need to help manufacturers operationalise S&P best practices within their development processes to ensure a more systematic and coherent focus on S&P across the development process.

Ethical Considerations

This research adheres to the Menlo Report's ethical principles of Respect for Persons, Beneficence, Justice and Respect for Law and Public Interest [13].

Respect for Persons: Our research does not involve any human subjects or the use of personally identifiable information.

Beneficence: To maximize benefits and minimize harm, we established a formal agreement with our partner ECA. This agreement granted us access to the valuable longitudinal data under conditions of strict confidentiality. This allows us to publicly share the insights from the data, maximising the benefits while minimising negative consequences such as manufacturers gaming the rating system by exploiting knowledge of test specifics. The anonymity also ensures that the additional insights that come from such longitudinal analysis of S&P features and ratings will not negatively impact the reputations of the manufacturers.

Justice: We ensured fair distribution of risks and benefits by carefully outlining the processes involved in evaluating IoT devices without disclosing the test specifics to ensure confidentiality of the rating systems.

Respect for Law and Public Interest: We respected the Non-Disclosure Agreement with our partner ECA and anonymised the partners name, the specifics of the tests, the names of the manufacturers and devices. We also aggregated the meta data in Table 2 to prevent de-anonymisation of the manufacturers and/or devices.

References

[1] Mitsuaki Akiyama, Shugo Shiraishi, Akifumi Fukumoto, Ryota Yoshimoto, Eitaro Shioji, and Toshihiro Yamauchi. Seeing is not always believing: Insights on IoT manufacturing from firmware composition analysis and vendor survey. *Computers & Security*, 133:103389, 2023.

[2] Manos Antonakakis, Tim April, Michael Bailey, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, Yi Zhou, Manos Antonakakis Tim April, Matthew Bernhard Elie Bursztein, Jaime J Cochran Zakir Durumeric Alex Halderman Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever Zane Ma, Joshua Mason, and Nick Sullivan Kurt Thomas. Understanding the Mirai Botnet. *USENIX Security '17*, 2017. URL https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

[3] Renana Arizon-Peretz, Irit Hadar, and Gil Luria. The importance of security is in the eye of the beholder: Cultural, organizational, and personal factors affecting the implementation of security by design. *IEEE Transactions on Software Engineering*, 48(11):4433–4446, 2021.

[4] Hala Assal and Sonia Chiasson. Security in the software development lifecycle. In *Fourteenth symposium on usable privacy and security (SOUPS 2018)*, pages 281–296, 2018.

[5] Christopher Bellman and Paul C van Oorschot. Best Practices for IoT Security: What Does That Even Mean? *arXiv preprint arXiv:2004.12179*, 2020.

[6] Mollie E. Brooks, Kasper Kristensen, Koen J. van Benthem, Arni Magnusson, Casper W. Berg, Anders Nielsen, Hans J. Skaug, Martin Maechler, and Benjamin M. Bolker. glmmTMB Balances Speed and Flexibility Among Packages for Zero-inflated Generalized Linear Mixed Modeling. *The R Journal*, 9(2):378–400, 2017. doi: 10.32614/RJ-2017-066.

[7] Peter Bruce and Andrew Bruce. *Practical Statistics for Data Scientists*. O'Reilly Media, 2017.

[8] European Commission. Radio Equipment Directive (RED), 2014. URL https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en. Accessed: 2024-11-14.

[9] European Commission. Cyber Resilience Act, 2022. URL https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act. Accessed: 2024-11-14.

[10] Federal Trade Commission. Ftc approves final order in asus privacy case, 2018. URL https://www.ftc.gov/news-events/news/press-releases/2016/07/ftc-approves-final-order-asus-privacy-case. Accessed: 2024-11-14.

[11] Federal Trade Commission. FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras, 2023. URL https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users. Accessed: 2024-11-14.

[12] Henry De and Graft Acquah. Comparison of Akaike information criterion (AIC) and Bayesian information criterion (BIC) in selection of an asymmetric price relationship. *Journal of Development and Agricultural Economics*, 2:1–6, 02 2010.

[13] D Dittrich and E Kenneally. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. Technical report, U.S. Department of Homeland Security, August 2012.

[14] Hongying Dong, Hao Shu, Vijay Prakash, Yizhe Zhang, Muhammad Talha Paracha, David Choffnes, Santiago Torres-Arias, Danny Yuxing Huang, and Yixin Sun. Behind the Scenes: Uncovering TLS and Server Certificate Practice of IoT Device Vendors in the Wild. In *Proceedings of the 2023 ACM on Internet Measurement Conference*, pages 457–477, 2023.

[15] ENISA. Guidelines for Securing the Internet of Things, 2020. URL https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things. Accessed: 2024-11-14.

[16] Michael Fagan, Katerina N Megas, Karen Scarfone, and Matthew Smith. *Foundational cybersecurity activities for IoT device manufacturers*. US Department of Commerce, National Institute of Standards and Technology, 2020.

[17] The Guardian. Amazon's ring camera comes under lawsuit over hacking threats, 2020. URL https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats. Accessed: 2023-10-25.

[18] David W. Hosmer, Trina A. Hosmer, Saskia le Cessie, and Stanley Lemeshow. A comparison of goodness-of-fit tests for the logistic regression model. *Statistics in medicine*, 16 9:965–80, 1997.

[19] H.R.1668. IoT Cybersecurity Improvement Act of 2020, 2019-2020. URL https://www.congress.gov/bill/116th-congress/house-bill/1668. Accessed: 2024-11-14.

[20] Md. Hussain and Ishtiak Mahmud. pymannkendall: a python package for non parametric mann kendall family of trend tests. *Journal of Open Source Software*, 4(39): 1556, 7 2019. ISSN 2475-9066. doi: 10.21105/joss.01556. URL http://dx.doi.org/10.21105/joss.01556.

[21] Ron De Jesus. How to operationalize privacy by design, 2020. URL https://iapp.org/news/a/how-to-operationalize-privacy-by-design. Accessed: 2024-11-14.

[22] David R. Anderson Kenneth P. Burnham. *Model Selection and Inference: A Practical Information-Theoretic Approach*. JSTOR, 2002.

[23] Sara Kraemer and Pascale Carayon. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics*, 38(2):143–154, 2007.

[24] Deepak Kumar, Kelly Shen, Benton Case, Deepali Garg, Galina Alperovich, Dmitry Kuznetsov, Rajarshi Gupta, and Zakir Durumeric. All Things Considered: An Analysis of {IoT} Devices on Home Networks. In *28th USENIX security symposium (USENIX Security 19)*, pages 1169–1185, 2019.

[25] Frank Li, Lisa Rogers, Arunesh Mathur, Nathan Malkin, and Marshini Chetty. Keepers of the machines: Examining how system administrators manage software updates for multiple machines. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 273–288, 2019.

[26] Franco Loi, Arunan Sivanathan, Hassan Habibi Gharakheili, Adam Radford, and Vijay Sivaraman. Systematically Evaluating Security and Privacy for Consumer IoT Devices. *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, 2017. URL https://api.semanticscholar.org/CorpusID:607695.

[27] Philipp Morgner and Zinaida Benenson. Exploring security economics in IoT standardization efforts. *arXiv preprint arXiv:1810.12035*, 2018.

[28] Asuka Nakajima, Takuya Watanabe, Eitaro Shioji, Mitsuaki Akiyama, and Maverick Woo. A pilot study on consumer IoT device vulnerability disclosure and patch release in Japan and the United States. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pages 485–492, 2019.

[29] NIST. NIST Issues Guidance on Software, IoT Security and Labeling, 2022. URL https://www.nist.gov/news-events/news/2022/02/nist-issues-guidance-software-iot-security-and-labeling. Accessed: 2024-11-14.

[30] Krebs on Security. Naming & shaming web polluters: Xiongmai, 2018. URL https://krebsonsecurity.com/2018/10/naming-shaming-web-polluters-xiongmai/. Accessed: 2024-11-14.

[31] S. Rivera Pérez, M. van Eeten, and C. H. Gañán. Patchy Performance? Uncovering the Vulnerability Management Practices of IoT-Centric Vendors. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 157–157, Los Alamitos, CA, USA, may 2024. IEEE Computer Society. doi: 10.1109/SP54263.2024.00154. URL https://doi.ieeecomputersociety.org/10.1109/SP54263.2024.00154.

[32] SB-327. Information privacy: connected devices., 2017-2018. URL https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327. Accessed: 2024-11-14.

[33] Martin Schulz and Lloyd A Jobe. Codification and tacitness as knowledge management strategies: an empirical exploration. *The Journal of High Technology Management Research*, 12(1):139–165, 2001.

[34] HP Online Store. The state of printer security, 2023. URL https://www.hp.com/th-en/shop/tech-takes/post/the-state-of-printer-security. Accessed: 2023-10-28.

[35] Ars Technica. Cache issue causes xiaomi cameras to show other people's camera feeds, 2020. URL https://arstechnica.com/gadgets/2020/01/cache-issue-causes-xiaomi-cameras-to-show-other-peoples-camera-feeds/. Accessed: 2023-10-25.

[36] Karen Van Dam, Shaul Oreg, and Birgit Schyns. Daily work contexts and resistance to organisational change: The role of leader–member exchange, development climate, and change process characteristics. *Applied psychology*, 57(2):313–334, 2008.

[37] Veerle van Harten, Carlos Hernández Gañán, Michel van Eeten, and Simon Parkin. Easier said than done: The failure of top-level cybersecurity advice for consumer iot devices, 2023. URL https://arxiv.org/abs/2310.00942.

[38] Swaathi Vetrivel, Veerle Van Harten, Carlos H Gañán, Michel Van Eeten, and Simon Parkin. Examining Consumer Reviews to Understand Security and Privacy Issues in the Market of Smart Home Devices. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 1523–1540, 2023.

[39] Swaathi Vetrivel, Brennen Bouwmeester, Michel van Eeten, and Carlos H Gañán. Iot market dynamics: An analysis of device sales, security and privacy signals, and their interactions. In *33nd USENIX Security Symposium (USENIX Security 24)*, pages 7031–7048, 2024.

[40] Shundan Xiao, Jim Witschey, and Emerson Murphy-Hill. Social influences on secure development tool adoption: why security tools spread. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*, pages 1095–1106, 2014.

[41] Narges Yousefnezhad, Avleen Malhi, and Kary Främling. Security in product lifecycle of IoT devices: A survey. *Journal of Network and Computer Applications*, 171:102779, 2020.

A Appendix

A.1 Beta Regression Estimates

Table 3: Beta Regression GLM Results

Dependent variable: Proportion of Positive S&P Features							
	Model 0	**Model 1**	**Model 2**	**Model 3**	**Model 4**	**Model 5**	**Model 6**
Predictors	*IRR*	*IRR*	*IRR*	*IRR*	*IRR*	*IRR*	*IRR*
(Intercept)	0.76 (< 0.001)	0.89 (< 0.001)	0.89 (< 0.001)	1.12 (0.011)	1.09 (0.057)	1.11 (<0.097)	1.46 (< 0.001)
DeviceType [Smart Printers]		0.79 (< 0.001)	0.79 (< 0.001)	0.56 (< 0.001)	0.58 (< 0.001)	0.56 (< 0.001)	0.52 (< 0.001)
DeviceType [Smart Speakers]		0.84 (0.073)	0.84 (0.078)	0.87 (0.134)	1.09 (0.444)	1.08 (0.504)	0.9 (0.420)
Price			0.99 (0.667)	1.01 (0.598)	1.00 (0.785)	1.01 (0.730)	1.01 (0.606)
Number of Devices				1.21 (< 0.001)	1.21 (< 0.001)	1.21 (< 0.001)	1.13 (< 0.001)
Manufacturer Size					0.94 (0.002)	0.94 (0.003)	0.97 (0.06)
Years since Founding						1.01 (0.648)	1.20 (<0.01)
HQ [China]							0.82 (< 0.001)
HQ [Japan]							0.67 (< 0.001)
HQ [NL]							0.61 (0.008)
HQ [Sweden]							0.36 (< 0.001)
HQ [Taiwan]							0.78 (0.075)
Observations	428	428	428	428	428	428	428
R2	0.000	0.072	0.072	0.135	0.145	0.146	0.255
AIC	-892	-931.3	-929.5	-972	-979.6	-977.8	-1101.3
BIC	-883.9	-915	-909.2	-947.6	-951.1	-945.3	-1048.6
LogLik	448	469.6	469.7	492	496.8	496.9	563.7