Missing, Present and Conflicting: A Large Scale Analysis of IoT Update Information in the EU Market

Swaathi Vetrivel
Delft University of Technology
S.Vetrivel@tudelft.nl

Michel van Eeten
Delft University of Technology
M.J.G.vanEeten@tudelft.nl

Carlos H. Gañán
Delft University of Technology
C.HernandezGanan@tudelft.nl

Abstract

Security updates are essential for protecting IoT devices, yet consumers often lack reliable information about how long devices will be supported. We conduct the first large-scale study of update duration disclosures in the European market, analysing 34,187 product pages across local retailers, EU Amazon sites, and Temu. Disclosure varies sharply: Dutch retailers, subject to regulatory oversight, list update durations for up to 92% of devices, while Amazon provides such information for fewer than 1% and Temu for none. For smart TVs, where EU rules mandate disclosure, coverage is higher but still inconsistent. Stated update durations vary between one and eight years, with smart TVs generally receiving the longest support. Comparing stated support durations across retailers, manufacturers, and the EU's central product database, we find widespread contradictions, with retailers often understating support relative to manufacturers. These inconsistencies limit the effectiveness of transparency mandates and risk misleading consumers. Our findings show that regulation can improve visibility, but only robust enforcement and standardized disclosure mechanisms ensure accurate and trustworthy information.

1 Introduction

Many Internet-of-Things (IoT) devices are released with weak security postures, making them attractive targets for cyberattacks. Even when manufacturers equip their IoT devices with robust security features, they remain susceptible to vulnerabilities discovered after release [10, 26]. Without timely security updates, these vulnerabilities can be exploited at scale, turning millions of interconnected devices into entry points for attackers.

Security updates ('patches') are therefore not just a best practice, they play a critical role, providing the means to retroactively patch security vulnerabilities in IoT devices. Recognising this, the provisioning of security updates has become the focus of legislation and policy efforts in different jurisdictions requiring IoT manufacturers to provide more transparency. Consumers should be informed at the time of purchase about how long a device will receive security updates. Update duration is a critical focus because, like a product warranty, it can be clearly disclosed at purchase and factored into consumer decisions, empowering buyers and incentivizing manufacturers to extend support.

The US Cyber Trust Mark [22], a voluntary IoT device labelling initiative, expected to take effect in late 2025, includes update support duration as part of its label. Similarly, in the UK, since April 2024, the Product Security and Telecommunications Infrastructure (PSTI) Act places a legal requirement on IoT device manufacturers to provide information to consumers about how long their products are supported by security updates [12]. The upcoming Cyber Resilience Act (CRA) in the European Union, which comes into full force in December 2027, mandates manufacturers to disclose the update support duration for their products. It also requires that security updates be provided for a device's entire expected use period, and at least for five years [17]. Another EU Regulation, on Energy Labelling [1], requires manufacturers to provide update duration information for smart TVs, along with the energy ratings, to be able to sell their products in the EU market. Manufacturers have to submit this information to a central, consumer accessible, database called the European Product Registry for Energy Labelling (EPREL).

Online stores are a critical interface where consumers engage with product information. If regulatory and voluntary efforts to inform consumers are having an effect, update duration should become visible on product pages. Large stores also have more leverage than consumers to get clear disclosures from manufacturers about their update support for a product. A complementary regulatory strategy is to require online stores to include this infor-

mation in their product pages. In the Netherlands, this strategy has been in place since 2020 when the Netherlands Authority for Consumers and Markets (ACM) [4] required major online retailers to provide update support duration information.

Despite these regulations emphasising provisioning of update support duration, there is very little empirical data on the presence of this information in the marketplace or on where this information exists, or even what update durations manufacturers are promising. The US Federal Trade Commission (FTC) recently conducted a small-scale study on 184 devices and found that nearly 89% of manufacturer product webpages failed to disclose software update durations [38]. The only academic study we are aware of reported that update duration was available for 20% of the 417 IoT devices that were analysed [43]. In sum, there is a lack of large scale systematic evaluation on the availability of update support durations and on the length of the durations currently promised. This gap makes it difficult to assess market transparency and hinders regulators and researchers from evaluating the effectiveness of current efforts to improve security update support.

In this paper, we address this gap through three research questions, focusing on online stores where update information can be collected at scale and is most relevant and visible to consumers. Since purchases typically form a contract with the store rather than the manufacturer, what the store discloses matters. Our first question is: *To what extent do online stores in the EU provide information on the update support duration of IoT devices?* To answer, we manually reviewed 4,600 product pages for five device types across 58 EU online stores: regional retailers, country-specific Amazon sites, and Temu.com. Of the 22 regional retailers, all 20 stores selling smart TVs provide update information for these, but only the Dutch retailers provide update info for all five device types. Among global players, Temu.com shows none, while different EU Amazon sites list update durations for different device types, but none for all.

Our second research question was *What percentage of devices include update support duration, and what is the distribution of the durations?* Building on the results from the manual analysis, we scraped 29,587 product pages: all device types on EU Amazon sites and two Dutch sites, plus smart TVs from all regional retailers. Amazon rarely provides this information (0.4%), despite having the update support duration field on every page. Dutch retailers disclose far more (15–92%), and smart TVs in particular show higher coverage (19.8–100%). Stated durations range from one to eight years, with smart TVs typically receiving the longest support.

Finally, we compare update information across sources—retailer sites, manufacturer websites, and for smart TVs, the EPREL database—asking: *How consistent are disclosed update durations across sources?* We focus on regional stores for smart TVs and on Dutch stores for all device types, as Amazon provides too little data. Moreover, Dutch retailers and smart TVs are a special case due to regulatory intervention and an in-depth analysis can help identify ways to improve the status quo elsewhere. We supplemented our dataset with manufacturer pages for 250 devices and EPREL entries for smart TVs. The results show major inconsistencies between retailers, manufacturers, and the central database, casting doubt on the overall reliability of update support information. In sum, our contributions are as follows:

- We present the first large-scale analysis of update information provisioning, focused on European online stores. We manually review 4,480 product pages for disclosures and scrape an additional 29,587 pages for characterizing the statements of update durations.
- We find empirical evidence for the impact of two regulatory initiatives, for Dutch online stores and for smart TVs across several countries, but also characterize significant gaps in compliance.
- For a smaller sample, we provide a comparison of update duration availability across three sources. Surprisingly, online stores have higher availability of update information than (between 15.2% and 91.5%) manufacturer websites (between 18% and 50%), while the EPREL database has update information for around 80% of the TVs analysed.
- For the same device models, we identify conflicting update information between stores, manufacturers and EPREL database, highlighting inconsistencies in the disclosures to consumers. We offer recommendations for different stakeholders to better support consumers making more security-conscious IoT purchase decisions.

2 Related Work

In this section we outline prior work on empirical analyses of update support durations, consumer expectations for update support, regulatory transparency mandates, and socio-legal perspectives on governance gaps.

Disclosure of IoT Update Information There is limited prior work on the availability of update support information. The FTC found that 89% of 184 device manufacturer webpages did not disclose update support duration [23]. An academic study of 417 devices across

two online stores [43] similarly reported valid information in only a fraction of product pages. Privacy International [28] checked 21 manufacturers across five device categories (smartphones, PCs, gaming consoles, tablets, smart TVs), finding that most provide unclear or missing information. These studies analyze small samples (hundreds of products) and focus solely on manufacturer disclosure. We present the first large-scale analysis of 26,898 product pages across 55 online stores in Europe, characterizing stated update support durations. While we also examine manufacturer disclosures, we emphasize online stores—where consumers actually interface with information and enter legal contracts with retailers, not manufacturers directly.

Consumer Preferences for IoT Updates Consumer research shows users expect security updates for reasonable periods that vary by device category [32, 42]. Privacy International [27] found 31% of users expect 2-10 years of updates for internet-connected home devices. While most smart home users believe updates are important, they are less concerned about support end dates [25]. However, consumers demonstrate willingness to pay more for lifetime updates versus 5-year support [36]. Qualitative interviews reveal users rarely associate updates with security and worry about manufacturers discontinuing support [24]. Survey research indicates update duration information explains 8-35% of variance in purchase choices [34]. We do not analyze consumer preferences but build on this work by studying information provisioning at purchase—knowing it influences choice and motivating our focus on retail channels where consumers engage with product descriptions.

Transparency and Disclosure Mandates Update duration disclosure exemplifies broader transparency regulations, most notably GDPR. Yet empirical studies reveal gaps between legal intent of such regulations and their practical outcomes. One study [14] documents how GDPR transparency rights fail to deliver substantive consumer empowerment despite formal compliance. Another [29] argues transparency alone cannot alter economic realities and is prone to exploitation. Another study [5] reasons that disclosure mandates routinely fail across contexts because they overwhelm consumers, go unread, or are gamed by regulated entities. Subsequent research [45] advocates moving beyond disclosure toward performance-based standards holding firms accountable for outcomes. Our findings extend these concerns to consumer IoT, where contradictions between retailer disclosures, manufacturer statements, and centralized databases show that transparency mandates alone yield missing, fragmented, unreliable information.

STS and Socio-Legal Perspectives Research on supply chain transparency stresses the importance of robust reporting and governance capabilities in conjugation with frameworks to collect, analyse and disseminate information [7]. The update duration contradictions we observe underline the need for better frameworks to organise disclosure of the information across the different channels. Prior work stresses on the distinction between 'visibility' (information gathering) and 'disclosure' (information sharing) [39]. Our findings reveal failures at both levels: manufacturers possess update duration information but fail to disclose it and even when disclosed, this information fails to propagate to retail channels where consumers make purchase decisions. On the retailers' side, digital governance scholarship shows platforms operate as private regulators [41], with their design choices shaping information access. Viewed from this lens, limited or conflicting update duration on retail channels could be an instance of 'strategic disclosure' – firms disclose selectively based on their assessment of costs, benefits and risks or a design choice that reflects business priorities rather than technical constraints. The revised Product Liability Directive (2024/2853) reinforces these incentives by extending strict liability to online platforms and other actors in the supply chain [20, 40].

3 Methodology

To address our first research question on the level of provisioning currently present in EU online markets, we manually analysed the online stores and identified the stores which provide update information. For our second research question on characterising the update support duration currently stated by retailers for different IoT device types, we do large scale data collection and analysis using web scraping and extraction techniques. In this section we detail the methodology followed for both.

For both research questions, we considered five IoT device types that have been shown to be popular in the consumer IoT landscape – IP cameras, smart printers, smart speakers [31, 43]. We scoped our analysis to the 30 countries in the European Economic Area (EEA) at the time of writing this paper: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.

3.1 Web Store Data Collection

To evaluate the update provisioning comprehensively, we wanted to systematically identify and analyse online stores popular in each of the countries. To do so, we used

Similarweb, a digital intelligence platform that provides market research and trends for websites and apps. Based on the results from Similarweb, we identified three types of online stores: local or region-specific platforms tailored to the domestic market, the Amazon store popular in that region and Temu, the Chinese e-commerce platform that is popular across Europe. In all EU countries, Temu was ranked in the top 5.

Table 1: Research Aims and Dataset Overview

Research Question	Research Aim	Websites and Device types	Count
RQ1	Evaluating Update provisioning on webstores	All five device types on: - 22 regional websites - 7 Amazon websites - 29 regional versions of Temu	4,480 product pages
RQ2	Quantifying update information presence and duration	All five device types on: - 6 Amazon websites (.de, .fr, .it, .nl, .es, co.uk) - 2 Dutch Websites (bol.com, coolblue.nl) Only smart TVs on: - 13 regional websites	29,587 product pages
RQ3	Comparing across sources	Manufacturer websites + EPREL Database	272 devices

Out of the 30 countries considered, Similarweb data was unavailable for 9. In these cases, we supplemented our analysis with Google search to identify the most prominent local online store. We searched for *'popular e-commerce websites in <countryname>'* and, based on the results, manually identified the leading local online store based on consumer or e-commerce blogs. We were not able to identify a local online store in eight of the 30 countries since the websites mentioned in the google results were not local to the region.

At the end of this step, we had a list of 22 local online stores and 7 Amazon websites that were popular across the EEA countries. Together with Temu, these 30 websites provide a starting point for our analysis. While the URL for Temu remains the same across Europe, the website allows users to select from 29 of the 30 EEA countries as their region and based on the region selected, the offerings vary. Although we analysed each of these 29 regional versions individually, we count Temu as a single website — rather than 29 separate ones — for simplicity.

3.1.1 Product Category Page Identification

In the next step, we identified the relevant product category page - the page that contains all listings for a particular product - for each of the 30 websites. We identified the product category pages for all five IoT device types: IP cameras, smart printers, smart speakers, smart TVs and smart watches. This approach is better than searching for categories like 'IP Cameras' since search results are often cluttered with auxiliary products (e.g., IP camera wall mounts, batteries, dummy cameras, etc.,). When no dedicated category existed, we used the closest match and applied filters — for example, selecting smart speakers from the general speaker category by filtering for WiFi connectivity.

3.2 Evaluating Provisioning: Manual Analysis of Online Stores

To answer our first research question, we manually evaluated the first twenty product links for each of the 5 device types, on each of the 30 websites to identify whether any update duration related information is available. We use product pages as the unit of analysis because they are the primary point of compliance for disclosing the update information. Although some devices have multiple pages due to different colours, sellers, bundles etc., we treat each page individually to capture all instances of disclosed information and avoid missing variations in update support details. The results of this evaluation feed into the next step.

3.3 Characterizing Update Durations: Large Scale Analysis

To answer our second research question, we scraped the websites and device type combinations that we identified in the previous step as containing update support duration information. We scraped the product links from the first fifty pages of each of the product category listings. Each page typically contained around 20-30 product links. Next, we opened each of these product links, saved the HTML pages and scraped the product data. We used BeautifulSoup, a Python library for parsing HTML, for scraping and extracting the product data – title, price, brand, and model details (where available), along with the product information or any specific fields identified in the previous step as containing update support duration information.

Next, we manually verified if the scraped information was accurate for 25 random listings of each device type and website combination, analysing 1,325 product pages overall. This step was crucial to make sure that the scraping scripts did not miss any update information.

3.4 Comparison Across Sources

To answer our third research question, we compared the update information between two online retail stores, between retailers and manufacturers and for smart TVs, also with the centralised database. We examined manufacturer websites since regulations emphasize their responsibility to provide update support details. Our objective with

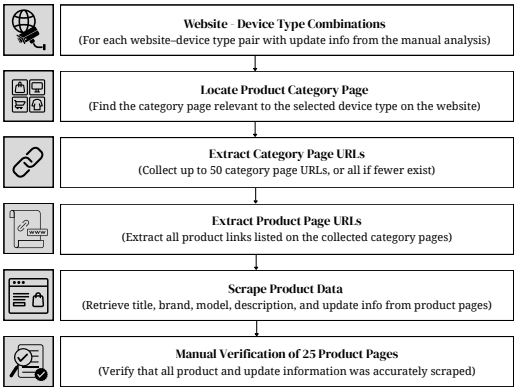

Figure 1: Workflow for Large Scale Analysis

this analysis was twofold. First, we wanted to compare whether the durations stated by the manufacturer were consistent with those stated on the online stores. Second, we aimed to check the overlap between devices with update information on online stores versus the manufacturer's website. Our hypothesis was that there would be a high degree of overlap, since if the information is available in one source, it should be straightforward to populate it in the other as well.

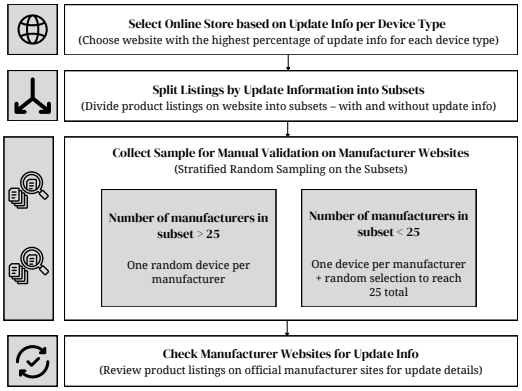

Figure 2: Workflow for Manufacturer Website Analysis

We used a stratified sampling strategy to select devices for manual validation. For each device type, we chose the online store with the highest percentage of products listing update durations. Listings were split into two groups (with and without update information), and at least 25 devices were randomly sampled from each, ensuring at least one per manufacturer. If fewer than 25 manufacturers existed, additional devices were randomly added; if more than 25, one device per manufacturer was randomly selected and 25 devices were randomly sampled from this pool. This yielded at least 50 devices per type with diverse manufacturer representation.

To find manufacturer-published update information, we searched Google using the manufacturer and model to find the product page on the manufacturer's website. If the page lacked update details, we repeated the search with the term 'update support duration' to capture cases where the information was presented in a separate page. This analysis was conducted in March 2025.

For the centralised database, we compared the smart TV details on the website[1] and got the details where available.

Table 2: Results of the Manual Analysis of Local Websites per Country

Country	Website	IP Camera	Smart Printer	Smart Speaker	Smart TV	Smart Watch
Belgium	bol.com	●	●	●	●	●
Bulgaria	emag.bg	○	–	○	●	○
Croatia	emmezeta.hr	–	○	–	●	○
Cyprus	skroutz.gr	○	○	○	●	○
Estonia	kaup24.ee	○	○	○	●	○
Finland	verkkokauppa.com	○	○	○	●	○
France	cdiscount.com	○	○	○	●	○
Germany	otto.de	○	○	○	●	○
Greece	skroutz.gr	○	○	○	●	○
Hungary	emag.hu	○	○	○	●	○
Iceland	elko.is	–	○	○	●	–
Latvia	1a.lv	○	○	○	●	○
Lithuania	pigu.lt	○	○	○	●	○
Netherlands	bol.com	●	●	●	●	●
Norway	clasohlson.com	○	○	○	–	○
Portugal	worten.pt	○	○	○	●	○
Romania	emag.ro	○	○	○	●	○
Slovakia	mall.sk	○	–	○	●	○
Slovenia	mimovrste.com	○	○	○	●	○
Spain	elcorteingles.es	○	○	○	●	○
Sweden	clasohlson.com	○	○	○	–	○

Legend: ● Update info present ○ No update info – Not sold

4 Provisioning of Update Duration Information on EU Online Stores

In this section we present the results of the first research question on the degree of update provisioning on EU online stores, starting with the local stores, then the Amazon stores and finally Temu.

4.1 Local Online Stores

Of the 30 EEA countries, 22 had a local online store ranked in the top five on Similarweb based on popularity; the remaining eight did not. Bol.com is popular in both Belgium and the Netherlands. As listings can vary by country, we set the relevant country or delivery location and analysed them independently, resulting in 21 unique local online stores across the 22 countries.

Table 2 lists the local websites analysed for each country and the availability of update information on the site. Of the 20 websites, five did not sell one or more of the device types considered, indicated with (–). Cases where a device type was sold but lacked update information are marked (○), and cases with update information

[1] https://eprel.ec.europa.eu/screen/product/electronicdisplays

are marked (•). The table highlights two patterns possibly driven by policy interventions. First, the Dutch site bol.com (also serving Belgium) provides update information for all device types, likely due to a requirement by the Netherlands Authority for Consumers and Markets (ACM)[4]. Second, update information for smart TVs appears on all local stores, possibly driven by an EU energy labelling directive that mandates reporting software and firmware support periods. We delve deeper into these in the next section on characterizing the update durations.

4.2 Amazon Stores

Next, we analyzed Amazon stores, focusing on the local storefronts for EEA countries. Of the 30 countries, 14 did not have Amazon among the top five popular sites. For the remaining 16, some shared the same regional Amazon website—for example, amazon.es was popular in both Spain and Portugal. We therefore analyzed seven Amazon sites: amazon.co.uk (Ireland), amazon.com (Bulgaria, Croatia, Hungary, Norway, Romania, Sweden), amazon.de (Austria, Denmark, Germany), amazon.es (Portugal, Spain), amazon.fr (Belgium, France), amazon.it (Italy), and amazon.nl (Netherlands). Delivery addresses were set locally to obtain relevant results.

Our manual analysis of 20 product links per device type showed that all the European Amazon websites have update support duration provisioning. In contrast, although amazon.com was popular in six EEA countries, it had no update information for any of the 100 devices analysed. We characterize the percentage of devices on the European Amazon websites with the update information and the duration specified in the next section.

4.3 Chinese Online Store - Temu

Next, we analysed Chinese Temu websites that are popular across Europe. As mentioned earlier, although Temu does not have region-specific domains, it provides an option to change the country or region on its website. Of the 30 EEA countries, only one — Liechtenstein — was not available in the list of regions. We analysed the remaining 29 regional versions of Temu for three types of IoT devices: IP cameras, smart speakers, and smart watches. At the time of our data collection, smart TVs and smart printers were not sold on Temu. We conducted a manual analysis of the first twenty product listings for each of the three device types across all 29 websites and found no update information on any of them.

5 Quantifying Update Support Durations

In this section, we answer our second research question. We quantify the presence and distribution of update support duration information across the websites and device types identified in the previous section as containing update information. The websites that have the update information for device types other than smart TV are bol.com and the six Amazon websites. To enable more comprehensive analysis, we also included another popular Dutch online store coolblue.nl [30], which would also help us better evaluate the effect of the Dutch intervention [4].

Table 3: Percentage of product links in each update status category across EU websites for all device types except smart TVs

Website	Update Info Field	IP Camera	Smart Printer	Smart Speaker	Smart Watch
bol.com	*Total Count*	1190	882	127	1152
	% Unavailable	0.0	5.4	0.0	0.0
	% Says Not Applicable	38.3	61.5	44.8	36.0
	% Specifies Duration	61.7	33.1	55.2	64.0
coolblue.nl	*Total Count*	248	111	79	319
	% Unavailable	14.9	100	58.1	6.3
	% Says Unknown	8.1	0.0	24.1	2.2
	% Specifies Duration	77.0	0.0	17.8	91.5
amazon.de	*Total Count*	738	882	26	954
	% Unavailable	73.6	7.7	23.1	15.2
	% Says Unknown	26.0	92.3	76.9	84.4
	% Specifies Date	0.4	0.0	0.0	0.4
amazon.es	*Total Count*	896	470	33	979
	% Unavailable	81.6	98.1	21.2	27.0
	% Says Unknown	18.4	1.5	75.8	73.0
	% Specifies Date	0.0	0.4	3.0	0.0
amazon.fr	*Total Count*	919	552	32	454
	% Unavailable	73.8	98.0	18.8	99.6
	% Says Unknown	25.8	1.8	81.2	0.4
	% Specifies Date	0.4	0.2	0.0	0.0
amazon.it	*Total Count*	797	818	32	410
	% Unavailable	84.4	97.4	28.1	95.9
	% Says Unknown	15.3	2.6	71.9	4.1
	% Specifies Date	0.3	0.0	0.0	0.0
amazon.nl	*Total Count*	1071	371	33	405
	% Unavailable	65.6	1.1	0.0	19.3
	% Says Unknown	33.1	94.9	100.0	79.8
	% Specifies Date	1.3	4.0	0.0	1.0
amazon.co.uk	*Total Count*	1236	721	1167	1203
	% Unavailable	73.5	9.3	69.6	20.8
	% Says Unknown	26.1	90.7	30.4	79.2
	% Specifies Date	0.4	0.0	0.0	0.0

On these eight websites, we scraped product links for IP cameras, smart printers, smart speakers and smart watches from the first fifty pages of product listings (or all pages if the total was less than 50). We categorise the presence of update information into three categories, the update field was (a) absent, we classify this as field unavailable, (b) present but says Unknown or Not applicable or (c) specifies a duration (e.g., At least 60 months after the introduction date) or date (e.g., Guaranteed software updates until 15 Sep 2031). bol.com and coolblue.nl list the duration while the Amazon websites list a date.

Table 3 reports the fraction of pages in each category across all the seven websites. On bol.com, the percentage of product links with update information ranges from 33.1% to 64%. The other Dutch website, coolblue.nl, has update information for 17.8% to 91.5% of product links,

with no smart printers having update support information. The distribution of update duration across both the bol.com and coolblue.nl ranges from 1 year to 7 years across all the device types except smart TV. We discuss smart TV separately in the next section.

In contrast to the Dutch websites, the vast majority of devices on the Amazon websites lack specific update information: 70.4% of product links have no update support duration field, while 29.3% display the field but list it as Unknown. Only 0.3% of all links specify a date. Across the four device types and six EU Amazon websites, only 51 product links specify a date. We started our data collection in 2024, but 18 product links (35.3%) listed a date in 2023 or earlier in the 'Guaranteed software updates until' field. Two links state a date in 2083, while the rest range from 2026 to 2031, with 13 April 2030 being the most common (41.2% or 21 product links).

Device type differences exist: IP cameras and smart watches have higher percentage of availability across both the Dutch websites and the EU Amazon websites. Within the Amazon websites, regional differences are also notable. The Dutch site, amazon.nl, performs best, with 4% of smart printers and 1.8% of smart TVs specifying dates, reflecting broader local compliance, though overall adherence to ACM requirements remains low (0–4%). In contrast, amazon.fr and amazon.it consistently show 0–0.4% of products with update information. Despite the UK PSTI Act [12], amazon.co.uk lists dates for only 0.1% of smart TVs and 0.4% of IP cameras, with no dates for other device types, suggesting UK consumers rarely receive useful update duration information despite policy and a dedicated field.

Smart TVs As noted in the Introduction, smart TVs represent a unique case under the Commission Delegated Regulation (EU) 2019/2013 [1], which introduced mandatory disclosure of software update support durations for electronic displays as part of the EU's revised energy labelling framework (effective March 2021). Smart TVs are the only IoT devices explicitly covered by this regulation, which requires product information sheets to state the minimum guaranteed availability of software and firmware updates alongside energy performance data. This requirement, linked to the ecodesign regulation for electronic displays (EU 2019/2021), supports EU policy goals on sustainability, transparency, and digital rights. It is intended to help consumers make informed decisions about device longevity, particularly software support for connected products [1, 2].

Our analysis found that all the local online stores and the EU Amazon websites included update information for smart TVs, though in varying formats. Retailers in Croatia (emmezeta.hr), Estonia (kaup24.ee), Latvia (1a.lv), Lithuania (pigu.lt), and the Netherlands (coolblue.nl) provided it in PDF product information sheets linked from their sites. On all six European Amazon websites, the sheets were available only as images, making the content unsearchable and less accessible. The other local online stores and the Dutch retailer bol.com displayed the QR code with the energy rating label in a product carousel image, which directed consumers to the product's EPREL page.

Table 4 shows the percentage of links per website that contained update information. None of the websites provided the sheets for all listed products. Data from the local stores in Croatia, Portugal and Slovenia could not be collected due to rate limiting measures and in the case of Croatia, website instability: the site frequently failed to load and often redirected product links to "not found" pages.

Table 4: Percentage of Smart TVs with product information sheet

Website	Country	Percentage of product pages with product information sheet
emag.bg	Bulgaria	48.7%
skroutz.cy	Cyprus	97%
kaup24.ee	Estonia	33.3%
verkkokauppa.com	Finland	50%
amazon.fr	France	46.4%
cdiscount.com	France	21%
amazon.de	Germany	91.8%
otto.de	Germany	100%
skroutz.gr	Greece	91%
elko.is	Iceland	100%
amazon.it	Italy	43.2%
1a.lv	Latvia	19.8%
pigu.lt	Lithuania	81.5%
amazon.nl	Netherlands	37.9%
bol.com	Netherlands	97.6%
coolblue.nl	Netherlands	54.2%
emag.ro	Romania	56%
mall.sk	Slovakia	100%
amazon.es	Spain	50.4%
elcorteingles.es	Spain	80%
amazon.co.uk	UK	41.2%

We observe substantial variation in the percentage of devices with update support information across countries and websites. Only local stores in Germany, Iceland and Slovakia contain update information for all the TVs while skroutz operating in Cyprus, Greece also shows high percentage (91-97%). On the other hand, less than 20% of smart TVs on Latvia's 1a.lv include the product information sheet. The Dutch websites also show a sharp difference. A little more than half (54.2%) of TVs on coolblue.nl have the update information compared to 97.6% on bol.com. Among the Amazon websites, Germany has the highest percentage of update information (91.8%) while UK has the lowest (41.2%). Consistent with the regulatory mandate requiring updates for eight years, the most frequently stated duration in product information sheets was also eight years. On some websites,

up to 93.5% of TVs specified an eight-year update period.

6 Comparison Across Sources

In this section, we move beyond quantifying the presence of update information to analyse update durations by device type. We compare the two Dutch retailers, manufacturer websites, and the centralised smart TV database to address our third research question. Amazon is excluded from this analysis, as it provides update information for only a negligible percentage of products.

6.1 Comparison between Dutch Retailers

Between the Dutch retailers, we first compare the distribution of update support durations across all the product links. Next, we also compare the update durations for the specific device models that are available on both the websites. To do so, we first filtered brands available on both bol.com and Coolblue, then extracted model names from product titles using regular expressions (e.g., E340 for a Eufy camera, C200 for a TP-Link camera, or Vivofit Junior 3 for a Garmin smartwatch). Model names were manually verified and edited where needed. Duplicate listings which are common due to color, material, or bundling variations, were dropped. From the resulting unique sets, we selected models appearing on both sites for direct comparison. Because only a few devices included all three fields, we focused only on the stated update support period, and excluded the release year and month. While this approach may have overlooked some cases where the same model was sold on both but without a distinctive model name, it also ensures that the devices we did compare were indeed the same models. Since coolblue.nl did not have any update information, we only compare for IP cameras, smart speakers and smart watches. We analyse the smart TVs separately.

On both bol.com and coolblue.nl, the update support duration information is presented in terms of number of months from the date of introduction of the device under the fields *'Support with updates'* and '*Guaranteed support with updates*' on bol.com and coolblue.nl respectively. There are also two additional fields which state the month and year of introduction (*'Introduction year'* and *'Introduction month'* on both websites). We discuss the results of our analysis for each device type and present the results for smart TV seperately (in subsection 6.3) since that is a special case.

6.1.1 IP Cameras

On bol.com, we collected data on 1,190 IP cameras from 247 brands. Of these, 61.7% (735 cameras) included update support information, but only 36.2% had all three key fields completed. Another 25.5% listed update support but lacked either the introduction year or month. In contrast, coolblue.nl offered had fewer listings, 48 cameras from 10 brands, yet about 80% included all three fields, showing more consistent update data despite the smaller range. As shown in Figure 3, both platforms most often listed update durations of 12 and 24 months.

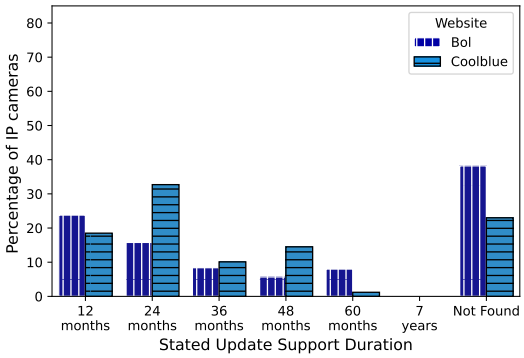

Figure 3: Comparison of update durations for IP cameras on bol.com and coolblue.nl

On Bol, 50 brands had at least three cameras, enabling intra-brand comparison. For 16 brands, the update duration was identical across models (standard deviation = 0), while the other 34 brands showed inconsistencies, with deviations up to 27.7 months. Price offered no explanation: expensive cameras were no more likely to receive longer support.

On Coolblue, only 7 brands had three or more devices, but variation was still evident. Ring (68 cameras) and Google (9) showed consistent support of 24 and 36 months, respectively, while Eufy and TP-Link varied. Interestingly, we found a small but statistically significant negative correlation ($r = -0.27$, $p < 0.01$) between price and update duration—contrary to the intuition that higher-priced cameras should be supported longer.

For the device model level analysis, we identified 38 models common to bol.com and coolblue.nl. Of these, 24 had update information listed on both websites. Half of these (12 models) showed identical information, while the other half (12 models) displayed conflicting durations, indicating significant inconsistency between the platforms. The discrepancies did not follow a clear manufacturer or brand pattern. All seven Ring cameras had inconsistent information, four of the Imou cameras were consistent while one was not, and among seven TP-Link cameras, three had information only on one website, three were consistent across both, and one was inconsistent.

6.1.2 Smart Speakers

We analysed smart speaker listings on bol.com (127 devices) and coolblue.nl (79 devices) to assess the availability of update support information. On Bol, 55.1% of speakers included some duration data, with 34.6% having all three fields (duration, introduction year, month) completed. In contrast, coolblue.nl showed far lower availability: only 15.2% had complete information, while 58.2% had the update field missing and 24.1% marked it as Unknown.

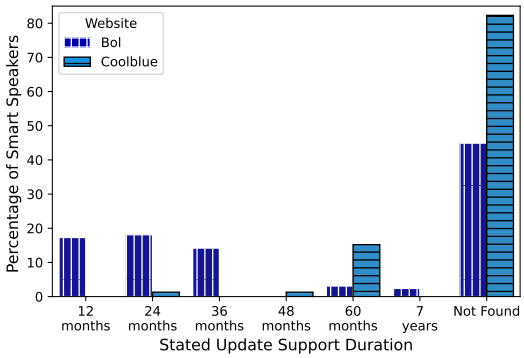

Figure 4: Comparison of update durations for Smart Speakers on bol.com and coolblue.nl

Figure 4 compares stated durations. On Bol, the most common values were 24 months (18.1%), 12 months (17.3%), and 36 months (14.2%), with a small fraction (2.4%) listing 7 years. Only two brands provided data for more than two devices: Kodak (8 speakers, all 12 months) and Bluesound (3 speakers, 36–60 months). On Coolblue, eight brands had more than two speakers listed, but only Denon provided update data. None of the others, including Apple, listed update support.

At the device model level, only ten models appeared on both websites. Of these, just two included update information on both, and in both cases the information conflicted: each speaker listed 24 months of support on bol.com but 60 months on coolblue.nl.

6.1.3 Smart Watches

We also analysed 1,152 smart watches on bol.com and 319 on Coolblue. On Bol, 64% of watches had update support information, but only 10 devices (all from TCL) included all three fields. By contrast, coolblue.nl listed durations for 91.5% of watches, with nearly all (except two) also including the introduction year—but none the month. As shown in Figure 5, both platforms reported durations ranging widely, with 24, 48, and 60 months the most common.

Across 54 brands with more than two watches (covering 58.7% of devices), market concentration was lower

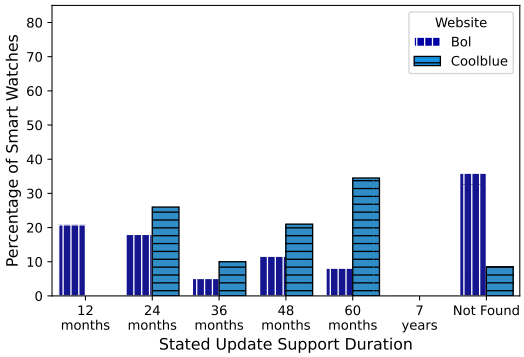

Figure 5: Comparison of update durations for Smart Watches on bol.com and coolblue.nl

than for printers. Within-brand variability was high: Apple ranged from 12–60 months (average 49.4), while Garmin averaged 41.8. A Kruskal–Wallis test confirmed significant differences across brands ($H(676) = 476.13$, $p < 0.001$). On Bol, we found a modest positive correlation between price and update duration ($r = 0.356$, $p < 0.01$), suggesting higher-priced watches tend to list longer support. Coolblue, by contrast, showed higher concentration: its 319 watches came from just 10 brands, with most listing a single consistent duration. Even Apple, Garmin, and Samsung showed consistency for the majority of models. Due to the smaller dataset, no correlation analysis was possible for Coolblue.

For the same device models of smart watches, we found 44 models common to both sites. Of these, 16 listed consistent information across platforms, while 18 listed conflicting durations. In addition to these cross-platform differences, we also observed contradictions within the same store. On bol.com, for instance, 30 listings of the Apple Watch Ultra were divided between 13 showing a duration of 24 months and 17 showing 48 months. Similarly, among 54 Apple Watch Series 10 listings, 53 stated 60 months while one listed only 24 months. Such inconsistencies are particularly noteworthy because Apple is a major brand with a reputation for tightly controlled product information. For consumers, this creates uncertainty about how long their devices will actually be supported, and raises concerns about the reliability of the update data published by retailers.

Taken together, these findings highlight a prevalent lack of consistency in update support information on bol.com and coolblue.nl, both between platforms and within the same retailer. In many cases, one store provided update information while the other did not, and when both did, the information often contradicted. This challenges the assumption that retailers simply act as passive channels for manufacturer-provided data. To better understand where these discrepancies originate, we

contacted customer service on both platforms, posing as potential buyers. bol.com did not respond, while coolblue.nl stated that update durations are based on 'internal case studies' but could not share any publicly available sources. Since update durations vary even within the same brand, these internal case studies appear to apply at the model level rather than at the manufacturer level. In any case, the discrepancies raise important questions about the true source of these durations and about which durations, if any, are aligned with the claims of the manufacturers.

6.2 Between Retailers and Manufacturer Websites

The consistencies identified raises the question of how these durations compare to what the manufacturers state. To address this, we analyse the update information stated by the manufacturers. As discussed in subsection 3.4, we checked for manufacturer disclosure for two sets of devices per device type: one set of devices that do have update information on the Dutch stores and one set that does not. To check whether update information was available on manufacturer websites, we first did a google search to locate the product page for each device on the manufacturers website (e.g., Apple Watch Series 10). Next, we searched for pages containing update information per device type (e.g., Apple Watch update support duration).

6.2.1 IP Cameras

Out of the 50 IP cameras analysed – 25 with update information on coolblue.nl and 25 without – 21 devices (42%) had update information on the manufacturer's website. Among the 25 devices with update information on coolblue.nl, 15 also had it on the manufacturer's site. In contrast, only 6 of the 25 devices without update information on coolblue.nl had it on the manufacturer's website. Notably, for only 3 of the 15 devices where both sources provided update information, the details were consistent. For one of these, an Ezviz camera, coolblue.nl states *'24 months after release date*' while the Ezviz website states *at least 2(TWO) years after the first shipment for sale [...] we may support for 3 years or longer if serious vulnerability is discovered'*.' This discrepancy matters because consumers relying solely on coolblue.nl's information would not know that the manufacturer allows extended support in critical situations, which could influence purchase decisions. Similarly, in 11 of the 12 cases where information was inconsistent, the manufacturer listed a longer duration. In these cases, coolblue.nl described the update period as "X months after the release date," while the manufacturer used phrasing such as "at least Y months" after the release date or after the device was last sold—where Y was consistently greater than X. This under-reporting suggests that consumers relying only on retailer information may make suboptimal choices, either avoiding products with longer support or underestimating the manufacturer's broader security commitment.

In our sample of 50 devices, we included devices from all 10 manufacturers due to our stratified sampling strategy, with each manufacturer contributing between one and 13 devices. Only TP-Link had update information on its website for half of its devices (3 of 6), while the other nine manufacturers either consistently provided or did not provide update information for all their devices. Although we usually found update information on the product listing page, for about a quarter of the devices it was listed on a separate webpage, either as a generic update policy for all the manufacturer's IP cameras or as a list of models with their update support durations.

6.2.2 Smart Printers

Only 12 of 50 (24%) smart printers in our sample of 50 devices, had update support information – 8 of which also had update information on bol.com and 4 of which did not. Only two of the 24 brands in our sample provide update information – HP and Oki. HP states '*... products are generally provided with a period of support for firmware updates for 36 months from date of purchase and sometimes longer*' for all of its devices while on Bol, the specified update duration varies across the seven HP printers listed. Only in one case does bol.com also mention an update duration of 36 months, for the majority (5 of 7) it states an update duration of 24 months, while for the remaining one it states 60 months. We observe a similar discrepancy between update duration stated on bol.com for the Oki printer, bol.com states 36 months, while the website states '*Our devices will be supported with security updates at least during the defined support period set out in the statement of compliance of such devices or longer where required by law. In addition, our devices may be supported with updates for up to five (5) years after the product end-of-life.*'

For both HP and Oki, the update information was on a separate page and not with the product listing on the manufacturer site. This implies that only consumers who are keen to double check the update duration will end up identifying the update duration stated by the manufacturers, the others will be influenced by the, often times, lower duration on bol.com or by the lack of update information on the manufacturer's product page.

6.2.3 Smart Speakers

Only 9 of 50 smart speakers (18%), from 5 of 24 manufacturers, in our sample have update support information

listed on the manufacturer website, six of which also had update information on Bol. One manufacturer, Sony, had the update information for only one of the two speakers in our sample. Of the nine smart speakers with update information, only one had this information directly in the product listing; in the remaining eight cases, it was provided separately. Here as well, we observe discrepancies between the duration specified on bol.com and the manufacturer website. For instance, Google states '*Google Nest connected home devices will receive automatic security updates for at least five years from the date we start selling them on the US Google Store*' but the duration on bol.com ranges between 12 and 36 months after the introduction date. Similarly, for a Sony speakers, bol.com states update support till January 2023 but the website promises support till December 2024, a full two years longer than the duration on Bol. In the case of Loewe, the update support duration stated on both are the same, 2 years, but Loewe's websites has a crucial additional piece of information – '*In addition we offer [...] latest available security update for that firmware free of charge for a period of 8 years after [...] model is released on the market.*' In all these cases, a consumer only looking at the bol.com website will get an impression that the manufacturer supports with updates for a shorter duration than what the manufacturer states.

6.2.4 Smart Watches

For smart watches, we observe an even split: half of the 50 devices in our sample (50%) have update information available on the manufacturer's website, while the other half do not. Among the 25 watches with update information on coolblue.nl, only 10 also have this information on the manufacturer's website. In contrast, 15 watches that lack update information on coolblue.nl do have it listed by the manufacturer. Of the 10 watches with update information available from both sources, six provide consistent details, while for three, coolblue.nl lists a longer update duration, and for one, a shorter duration. A similar even split is observed at the manufacturer level: five out of ten manufacturers provide update information for all their smart watches on their websites, while the remaining five do not. For 16 of the 25 watches with update information on the manufacturer's website, the information is included directly in the product listing, for the other 9 it is listed on a separate webpage.

Overall, we find that the manufacturer websites contain update information in between 18% (for smart speakers) and 50% (for smart watches) of devices. We also observe a pattern of update duration stated on online stores being lesser than that on the manufacturer websites across all the device types. This again challenges the notion of retailers being passive channels that publish manufacturer information. The retailer's promise might have more legal meaning than the manufacturer, since the consumer is entering a contract with the retailer, not with the manufacturer. All in all, the analysis for these three device types questions the usability of this information for a consumer.

6.3 Comparison of Retailers, Manufacturers and Database for Smart TVs

Similar to the manual validation of manufacturer websites for the other device types, we also checked manufacturer websites for update information related to smart TVs. There were 47 smart TV manufacturers with update information on bol.com and 11 without. We therefore checked the update information on the manufacturer websites for 72 smart TVs, 47 with update info on Bol, one from each manufacturer and 25 random devices without update info.

We found that only 25 of the 72 TVs (34.7%) had update information on the manufacturer website. The update information was either presented in the product sheet available on the website (in 13 cases) or via a QR that could be scanned to reach the EPREL database (8 cases) or both (4 cases). This lack of consistency in how the information is presented makes the information less useful from a consumer perspective who now has to spend additional time in figuring out where this information is located.

Of the 47 of 72 devices (65.3%) without any update information on the manufacturer website, three devices have the product information sheet but the update information field is empty. Two other devices have a QR code to take a user to the EPREL website which says the information is not available for that specific device.

With regards to manufacturers, three of the 27 manufacturers have the update information for some TV models but not others, seven have the information for all their models in our sample while the remaining 17 do not have the information for any of their TVs. In some cases these were smaller brands for which we were not able to identify any dedicated manufacturer website or information.

In summary, we find that despite the Energy regulation, manufacturer websites provide access to update information for TVs only in 34.7%. In contrast, the update information was present on manufacturer websites for 42% of IP cameras. As the regulation doesn't require this information to be published online, we next examine the EPREL database to see if it is provided there.

6.3.1 Validation of Centralised Database

The product information is uploaded by manufacturers and importers into a central European Product Registry

for Energy Labelling (EPREL) database[2], a mandatory step to comply with EU energy labelling regulations. Once the products are registered, the product information sheet can be downloaded in all EU languages. Consumers can access the information for a specific model by searching by brand and model name or by registration number. A QR code linking to the product information sheet on this database is also printed on the energy labels of the products. The ecodesign regulation 2019/2021 also mandates a minimum period of software support: it requires that manufacturers make the 'latest available version' of firmware available for at least 8 years after the last unit of a model is placed on the market, and likewise make security updates available for 8 years, free of charge [2].

We manually checked the EPREL website for the 42 devices without product information sheet or update information on the manufacturer website. We find that 34 of these have the update information on the EPREL database. This indicates that for 20 devices across 15 manufacturers, the information is available in the centralised database but the manufacturers do not link to it in any way from their own website. Moreover, 8 TVs do not have the update information even on the database despite the Energy regulation requiring manufacturers and sellers to provide this information to be able to sell their products [1].

Moreover, for the eight TVs with update information also available on Bol, we find inconsistent information between the bol.com website and the product information sheet from the EPREL database. The duration stated on bol.com ranges from one year to five years, in contrast to the 8 years that is stated in the product information sheet of all the TVs. In one notable case, for the same Samsung TV model, bol.com lists an update duration of 'at least 2 years', the product information sheet says 8 years, while Samsung's website states at least 5 years. Strictly speaking these are not inconsistent with each other, but in terms of guiding consumer purchasing decisions and providing assurances about updates, the differences are problematic.

7 Discussion

This study examines how EU online stores disclose IoT update support durations – a critical point of contact, since consumers often rely on product-page information when making purchase decisions. For our first research question on disclosure, we find marked differences across store types. Temu, a Chinese e-commerce platform, provides no update information for any device types. By contrast, Amazon and some local EU retailers do disclose update durations, although inconsistently.

[2] https://eprel.ec.europa.eu/screen/home

To answer our second research question, we quantify these differences. Amazon provides update information for only 0.4% of products despite a designated field on every page. Dutch stores show higher coverage: on bol.com, 33–64% of devices include update durations, while on coolblue.nl the range is 15.2–91.5%, depending on device type (subsection 6.1). Smart TVs have the best coverage: local retailers in all 22 EEA countries and six Amazon EU sites include update details (Table 4) as part of the energy ratings.

Our third research question on comparing online stores, manufacturer websites, and the EPREL database for smart TVs reveals notable inconsistencies. The same device often carries different stated durations depending on the source, raising concerns about reliability. Despite regulatory responsibility on manufacturers [12, 17], in line with earlier work [28, 38], we find update information is present on only 18–50% of manufacturer websites. On a positive note, the Energy Regulation [1] ensures 81% of smart TVs in our sample include update information in EPREL.

Conflicting Minimum Update Durations. We observe two main inconsistencies across Dutch stores, manufacturer websites, and EPREL. First, one source may contain information while others do not, indicating incomplete propagation. Second, different sources provide different minimum update durations. Dutch retailers frequently list shorter durations than manufacturers – in only one case is the retailer duration longer. Though technically consistent (e.g., at least two years' vs. at least five years'), these discrepancies signal systematic under-reporting. Importantly, retailer statements carry legal weight: under EU consumer protection law, the retailer is liable for ensuring product conformity. Consequently, consumers may rely on retailer-provided durations as contractually binding, suggesting that under-reporting may be deliberate (subsection 6.2). Under the revised Product Liability Directive (2024/2853) [20], which comes into effect in December 2026, manufacturers face potential liability if they fail to provide sufficient software updates or cybersecurity patches [15, 40]. Moreover, it also includes supply chain liability provisions which extend the responsibility to online platforms, importers, and fulfilment service providers [40].

Against this regulatory backdrop, inconsistent or missing update information raises a critical question: when update information is missing or contradictory across sources, which actor in the supply chain bears liability? Our findings suggest that retailers are not merely passive conduits passing manufacturer information. Instead, they appear to actively choose the published update durations based on internal assessments and their own risk calculus, which may reflect strategic positioning in anticipation of

liability risks.

Policy and Regulatory Context. Our findings across the policy contexts show mixed results. The UK PSTI Act, which legally requires manufacturers to disclose update details to consumers, appears to have had little effect, based on our analysis of amazon.co.uk and manufacturer websites. In contrast, the Dutch ACM intervention [4] and the EU Energy Labelling Regulation for smart TVs [1] are both associated with increased availability of update information within the respective contexts. Still, the results are far from ideal: information is often missing, retailer compliance is inconsistent, manufacturers frequently fail to disclose details, and the centralized database contains discrepancies compared to what consumers see elsewhere. Interestingly, we find little evidence of positive spillover effects beyond the jurisdictions directly targeted by regulation. One might expect that once update information is compiled and included in product descriptions, they propagate to other countries and store fronts, but this is rarely the case. For instance, although Amazon has the infrastructure to display update support information across all its EU store fronts, these fields are often left empty and are not carried over even when available on another national site (e.g., amazon.nl vs. amazon.de), echoing broader concerns about fragmented enforcement in EU digital markets [6, 35].

Consumer Advocacy. Consumer groups have also emphasised the need for better transparency. For instance, BEUC emphasizes clear, accessible information on security updates [8, 9], and Which? has advocated for stronger PSTI enforcement [33]. However, our findings suggest advocacy alone is insufficient without systematic monitoring and enforcement. The EU Consumer Protection Cooperation (CPC) Network offers cross-border coordination [6, 18], yet technical product disclosures like update durations require specialized expertise. Civil society organizations could aggregate update information across retailers and manufacturers [16], complementing regulatory enforcement and holding companies accountable for accuracy and consistency at the point of sale.

Recommendations Our analysis shows that regulations are not a silver bullet; enforcement mechanisms are essential to address market failures and information asymmetries [3]. The CRA mandates that manufacturers provide clear information on the security support period for products with digital elements [21], but our findings demonstrate that such mandates alone — as evidenced by the PSTI Act's minimal observable impact — do not guarantee compliance or ensure reliable consumer information. The Dutch ACM and Smart TV energy regulations illustrate that market surveillance, active monitoring and direct retailer engagement [19, 37], is crucial; without it, platforms might engage in symbolic rather than substantive compliance, strategically meeting baseline requirements only in jurisdictions subject to active oversight [13, 44].

In parallel with regulation, there is a need to support the development of systems and tools technical tools (APIs, widgets) to present update information consistently and enable third-party aggregation [11, 16], incentivizing manufacturers to compete on update duration. Consumer organizations like BEUC and Which? can also support development of tools and enforcement through independent monitoring and reporting [8, 9].

Regarding information display, we observe that manufacturers either present update information on product pages or in centralized databases, each mode serving a different consumer need. At the purchase stage, showing update details directly on product listings helps inform decisions. Post-purchase, a centralized repository offers convenience by consolidating update information across devices of a manufacturer. Ideally, manufacturers should adopt both approaches: maintaining a centralized database and linking it from individual product pages to maximize transparency and utility.

Limitations Our data collection period (December 2024–May 2025) coincides with a transitional regulatory landscape: some disclosure requirements were already in force (UK PSTI Act since April 2024 [12]), while others have been enacted but not yet fully applicable (the CRA entered into force December 2024 but its main obligations apply only from December 2027 [17, 21]). Consequently, our results cannot estimate compliance with future CRA requirements, though our analysis of the UK suggests that enacted disclosure mandates do not automatically produce compliance. Rather, our study provides an empirical baseline documenting disclosure practices across this mixed regulatory environment—enabling future research to assess whether the CRA and other emerging regulations produce measurable improvements over current practices.

Our analysis focused on the most popular devices leveraging the platform's own popularity rankings. We do not know how our findings generalize to other, e.g., less popular devices. That being said, we found near-zero compliance on all stores and product categories, except the Dutch retailers and smart TVs. It seems unlikely that other samples would have higher rates of compliance, especially as we would expect that popular devices would have a higher probability of complete product descriptions and disclosures. For the smaller Dutch sample, where we found the inconsistencies, the sampling can have more influence on the rates of compliance and the

degree of inconsistency across the different sources of update information. In the absence of data on price, ratings, reviews, and review counts across the retailers, we are unable to position our sample within the overall population. While prior work shows positive correlation between update disclosure and sales [43], further research is needed to examine whether the conflicting update durations and retailer under-reporting we document varies across different device categories and market segments.

While we observe conflicting values in some cases between the online store, manufacturer website and the centralised database, there is no ground truth. It is tempting to treat the manufacturer disclosure as ground truth, but the store enter into a legal contract with the buyers, so their disclosure actually has immediate legal impact. Moreover, we analysed claims about duration, not actual duration. It will take years to see if stores or manufacturers live up to their promises. It is beyond the scope of this paper to verify which duration will be followed in practice.

In each online store and manufacturer website, we manually checked the pages for update support information to the best of our ability. We also identified update information that was hidden under energy ratings, available only when scanning a QR code. While there might be corner cases that we might have missed, we are confident that we covered all areas of the stores where a consumer would look for the update information.

8 Conclusion

In this work, we analysed the availability of update duration information on online stores across EEA countries. We find that despite policy efforts, update information is often missing or inconsistent across retailers and manufacturers. Our findings highlight the need for stronger compliance checks and systems that make update information publicly accessible and consistent.

Acknowledgments

This publication is part of the RAPID project (Grant No. CS.007), financed by the Dutch Research Council (NWO). Additional support was provided by the INTERSCT project (Grant No. NWA.1160.18.301) and the THESEUS project (Grant No. NWA.1215.18.006), both funded by the Dutch Research Council (NWO).

A Ethical Considerations

The Ethics Review Board of our institution approved the study design and data management protocol. We evaluated our research design against the principles of the Menlo Report for ethical practices in computing studies [16]. Below, we provide a comprehensive stakeholder-based ethics analysis.

A.1 Stakeholders

The stakeholders that could be affected by this work include consumers and end users of IoT devices; online retailers whose websites we analyzed; IoT device manufacturers whose products and disclosures we studied; regulators and policymakers; and society at large. We discuss impacts and ethical principles for each stakeholder in detail below.

Consumers and end users. This work directly benefits consumers by exposing widespread lack of update information that leaves them vulnerable to security risks from unsupported devices. Our research does not involve any consumer personal data and creates no privacy concerns. We did not collect information like usernames and customer reviews which could contain personal information. All analysed data consisted of publicly available information that consumers would normally encounter. The publication of our findings empowers consumers to make better-informed purchasing decisions and provides evidence for advocating improved disclosure practices.

Online retailers. We did large scale analysis on product pages from online retailer websites. In order to minimise the load on the server, rather than scrape the pages directly from the website (which might trigger re-runs in case of failure) we downloaded the pages and scraped the information from these downloaded pages. The scripts to download the pages were fed links to specific product pages and were not general crawlers. We could not use APIs for data collection because not all of the websites provide them and even when available the costs are prohibitively high for research purposes. While there are minor reputational concerns for retailers who do not display the update information, we have mitigated this by objective reporting on the systemic issues in the market and focusing on policy implications rather than criticising individual retailers.

IoT device manufacturers. This work analyses publicly available information from manufacturer websites and product disclosures provided to retailers. We did not access any proprietary or confidential manufacturer data. Similar to the retailers, we only address the broader trends in the market rather than comment on specific manufacturers. Our research would also help manufacturers who might not be aware of the inconsistencies in the update support duration for their devices across the

different sources. Overall, the research creates positive incentives for better practices across the industry.

Regulators and policymakers. This research provides substantial benefits to regulators by offering empirical data related to existing regulations (Dutch ACM intervention, EU Energy Labeling Directive) and identifying compliance gaps to inform future enforcement of the Cyber Resilience Act and similar regulations. There are no identified harms to regulators from this research.

Society at large. The broader societal impact of this research is positive. With respect to 'justice', our study design aims to contribute to reducing information asymmetry for all consumers, not specific groups. Improved transparency in IoT security practices benefits society by enabling better-informed markets. The research promotes fairness by exposing information asymmetries that disadvantage consumers and providing evidence to support regulatory interventions. All stakeholders—large and small retailers, major and minor manufacturers—are treated equivalently in our analysis.

A.2 Ethical Principles

Beneficence. Our research provides substantial public benefit by documenting the current state of update duration disclosures, demonstrating the effectiveness of regulatory enforcement, and providing baseline data for measuring future Cyber Resilience Act compliance. The public interest benefits in consumer protection and IoT security substantially outweigh the minimal and mitigated commercial reputation concerns for some retailers and manufacturers.

Respect for Persons. All data collected was from publicly accessible sources intended for consumer viewing. No personal data about individual consumers was collected or analyzed. Retailers and manufacturers present this information publicly and voluntarily; our research analyses what they choose to disclose.

Justice. Our research does not disproportionately burden any vulnerable populations and promotes fairness by exposing information asymmetries that disadvantage consumers in the IoT marketplace.

Respect for Law and Public Interest. While commercial scraping for competitive purposes is typically prohibited, academic research for public interest is generally permitted under fair use principles. We also confirmed this with the legal advisor at our university. We implemented technical safeguards (rate limiting, distributed collection timing) to avoid service disruption, which is the primary concern in most Terms of Service. No authentication bypass or access to private data occurred; all data was publicly accessible.

The decision to publish was reached because the findings serve the public interest by informing consumers, policymakers, and regulators. Transparency about disclosure practices creates incentives for improvement across the industry. Withholding findings would perpetuate information asymmetries that harm consumers. The benefits of publication—better-informed policy, consumer awareness, and industry accountability—far outweigh minimal commercial reputation concerns. Our reporting approach using aggregate patterns, comparative analysis, and policy focus minimizes potential harms while maximizing public benefit.

B Open Science

In the spirit of open science, we fully support transparency and reproducibility of research. All data collected from the websites in this study have been shared at https://figshare.com/s/1064824a8f2a72c0e4f5, enabling other researchers to reproduce our results, verify our analyses, and build upon our work.

References

[1] Commission Delegated Regulation (EU) 2019/2013 of 11 March 2019 supplementing Regulation (EU) 2017/1369 of the European Parliament and of the Council with regard to energy labelling of electronic displays. https://eur-lex.europa.eu/eli/reg/2019/2013/oj, 2019. Annex V.

[2] Commission Regulation (EU) 2019/2021 of 1 October 2019 laying down ecodesign requirements for electronic displays pursuant to Directive 2009/125/EC of the European Parliament and of the Council. https://eur-lex.europa.eu/eli/reg/2019/2021/oj, 2019. Annex II, E.1.

[3] Ross Anderson. Why Information Security is Hard – An Economic Perspective. In *Seventeenth annual computer security applications conference*, pages 358–365. IEEE, 2001.

[4] Authority for Consumers and Markets (ACM). Consumers are now better informed about updates when purchasing smart devices, thanks to acm intervention. https://www.acm.nl/en/publications/consumers-are-now-better-informed-about-updates-when-purchasing-smart-devices-thanks-acm-intervention, Mar 2024. Accessed: 2025-02-25.

[5] Omri Ben-Shahar and Carl E Schneider. *More Than You Wanted to Know: The Failure of Mandated Disclosure*. Princeton University Press, 2014.

[6] Alexandre Biard. The Age of Consumer Law Enforcement in the European Union: High Hopes or Wishful Thinking? *European Journal of Risk Regulation*, 15(3):625–636, 2024.

[7] Marko Budler, Bernardo F. Quiroga, and Peter Trkman. A review of supply chain transparency research: Antecedents, technologies, types, and outcomes. *Journal of Business Logistics*, 45(1):e12368, 2024. e12368 JBL-Sep-2022-8308.R3.

[8] Bureau Européen des Unions de Consommateurs (BEUC). Keeping consumers secure: How to tackle cybersecurity threats through EU law. Position paper, BEUC, 2019.

[9] Bureau Européen des Unions de Consommateurs (BEUC). Cyber Resilience Act: Cybersecurity of Digital Products and Ancillary Services. Position paper, BEUC, 2022.

[10] Alina Bîzgă. 19 Zero-Day Vulnerabilities Affect Millions of IoT Devices Worldwide. https://www.bitdefender.com/en-us/blog/hotforsecurity/19-zero-day-vulnerabilities-affect-millions-iot-devices-worldwide, Jun 2020. Accessed: 2025-02-25.

[11] Lorrie Faith Cranor, Yuvraj Agarwal, and Pardis Emami-Naeini. Internet of Things Security and Privacy Labels Should Empower Consumers. *Communications of the ACM*, 67(3):29–31, 2024.

[12] Department for Science, Innovation and Technology (DSIT). The UK Product Security and Telecommunications Infrastructure (Product Security) Regime. https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime, Apr 2023–2024. Accessed: 2025-02-25.

[13] Vinit M Desai. Under the Radar: Regulatory Collaborations and their Selective Use to Facilitate Organizational Compliance. *Academy of Management Journal*, 59(2):636–657, 2016.

[14] Pierre Dewitte and Jef Ausloos. Chronicling GDPR Transparency Rights in Practice: The Good, the Bad and the Challenges Ahead . *International Data Privacy Law*, 14(2):106–133, 2024.

[15] David Drews, Lars Harten, and Thomas Wessel. Liability for software under the new European Product Liability Directive. https://www.ibanet.org/European-Product-Liability-Directive-liability-for-software, 2025. Accessed: 2025-12-14.

[16] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. An Informative Security and Privacy "Nutrition" Label for Internet of Things Devices. *IEEE Security & Privacy*, 20(2):31–39, 2021.

[17] European Commission. Cyber Resilience Act. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act, 2024. Accessed: 2025-10-14.

[18] European Commission. Enforcement of consumer protection. https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection_en, 2024. Accessed: 2025-12-14.

[19] European Commission, Directorate-General for Energy. Market Surveillance — Energy Efficient Products. https://energy-efficient-products.ec.europa.eu/policy-making/

market-surveillance_en, 2025. Accessed: 2025-12-14.

[20] European Union. Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC. https://eur-lex.europa.eu/eli/dir/2024/2853/oj, 2024.

[21] European Union. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directives (EU) 2020/1828 and (EU) 2022/2380 (Cyber Resilience Act). https://eur-lex.europa.eu/eli/reg/2024/2847/oj, 2024.

[22] Federal Communications Commission (FCC). U.S. Cyber Trust Mark. https://www.fcc.gov/CyberTrustMark, 2023–2025. Accessed: 2025-02-25.

[23] Federal Trade Commission. Smart Device Makers' Failure to Provide Updates May Leave You Smarting. https://www.ftc.gov/system/files/ftc_gov/pdf/smart-device-makers-failure-to-provide-software-updates-may-leave-you-smarting.pdf, November 2024. Accessed: 2025-02-21.

[24] Julie M Haney and Susanne M Furman. Work in Progress: Towards Usable Updates for Smart Home Devices. In *International Workshop on Socio-Technical Aspects in Security and Trust*, pages 107–117. Springer, 2020.

[25] Julie M Haney and Susanne M Furman. Smart Home Device Loss of Support: Consumer Perspectives and Preferences. In *International Conference on Human-Computer Interaction*, pages 492–510. Springer, 2023.

[26] GreyNoise Intelligence. GreyNoise Intelligence Discovers Zero-Day Vulnerabilities in Live Streaming Cameras with the Help of AI. https://www.greynoise.io/blog/greynoise-intelligence-discovers-zero-day-vulnerabilities-in-live-streaming-cameras-with-the-help-of-ai, Feb 2024. Accessed: 2025-02-25.

[27] Privacy International. Privacy international research shows that smart device security updates fail to meet consumers' expectations. https://privacyinternational.org/press-release/4964/privacy-international-research-shows-smart-device-security-updates-fail-meet, 2022. Accessed: 2025-02-25.

[28] Privacy International. We looked into the software support practices for 5 of the most popular smart devices (and the results may disappoint you). https://privacyinternational.org/report/4965/we-looked-software-support-practices-5-most-popular-smart-devices-and-results-may, 2022. Accessed: 2025-02-25.

[29] Agnieszka Jabłonowska and Giacomo Tagiuri. Rescuing Transparency in the Digital Economy: In Search of a Common Notion in EU Consumer and Data Protection Law. *Yearbook of European Law*, 42:347–387, 2023.

[30] Pleuni Jacobs. Top 10 online stores in the netherlands. https://ecommercenews.eu/top-10-online-stores-in-the-netherlands/, June 2024. Accessed: 2025-03-31.

[31] 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.

[32] Lorenz Kustosch, Carlos Gañán, Mattis van't Schip, Michel van Eeten, and Simon Parkin. Regulating Smart Device Support Periods: User Expectations and the European Cyber Resilience Act. In *34th USENIX Security Symposium (USENIX Security 25)*, pages 5149–5168, 2025.

[33] Alexander Martin. UK becomes first country to ban default bad passwords on IoT devices. https://therecord.media/united-kingdom-bans-defalt-passwords-iot-devices, April 2024.

[34] Philipp Morgner, Christoph Mai, Nicole Koschate-Fischer, Felix Freiling, and Zinaida Benenson. Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products. In *2020 IEEE Symposium on Security and Privacy (S&P)*, pages 429–446. IEEE, 2020.

[35] M Namysłowska. The Silent Death of EU Consumer Law and Its Resilient Revival: Reinventing Consumer Protection Against Unfair Digital Commercial Practices. *Journal of Consumer Policy*, pages 1–20, 2025.

[36] Majid Nasirinejad and Srinivas Sampalli. Evaluating Consumer Behavior, Decision Making, Risks, and Challenges for Buying an IoT Product. *IoT*, 4(2):78–94, 2023.

[37] Netherlands Authority for Consumers and Markets (ACM). Focus areas of ACM's oversight over the digital economy in 2025. https://www.acm.nl/en/publications/focus-areas-acms-oversight-over-digital-economy-2025, 2025.

[38] Alvaro Puig. How long will your smart device get software updates? It's hard to know. https://consumer.ftc.gov/consumer-alerts/2024/11/how-long-will-your-smart-device-get-software-updates-its-hard-know, November 2024. Accessed: 2025-03-31.

[39] ManMohan S Sodhi and Christopher S Tang. Research Opportunities in Supply Chain Transparency. *Production and Operations Management*, 28(12):2946–2959, 2019.

[40] Taylor Wessing. New Product Liability Directive 2024/2853: New product liability risks for products in the EU. Client briefing, January 2025.

[41] Natasha Tusikov. *Chokepoints: Global private regulation on the Internet*. University of California Press, 2016.

[42] Tanvi Vats, Neelima Sailaja, and Fabiana Anselmo Polido Lopes. Exploration of User Perspectives around Software and Data-Related Challenges Associated with IoT Repair and Maintenance against Obsolescence: User Study on Software and Data Interactions and Considerations for IoT Repair and Maintenance against Obsolescence. In *Proceedings of the 13th Nordic Conference on Human-Computer Interaction*, pages 1–17, 2024.

[43] 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 *33rd USENIX Security Symposium (USENIX Security 24)*, pages 7031–7048, 2024.

[44] Lauren E Willis. Decisionmaking and the Limits of Disclosure: The Problem of Predatory Lending: Price. *Md. L. Rev.*, 65:707, 2006.

[45] Lauren E Willis. Performance-Based Consumer Law. *U. Chi. L. Rev.*, 82:1309, 2015.