September 5, 2024

Samuel Levine
Director of the Bureau of Consumer Protection
Serena Viswanathan
Associate Director of the Division of Advertising Practices
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Director Levine and Associate Director Viswanathan,

Consumer Reports and U.S. PIRG write to ask the FTC to create clear guidance to address the issue of software tethering which leads to several consumer harms, including locking features behind a subscription after the purchase of a device, and companies selling connected devices only to render them nonfunctional later using software. Both switching features to a subscription and "bricking" a connected device purchased by a consumer in many cases are unfair and deceptive practices.

Both practices are examples of how companies are using software tethers in their devices to infringe on a consumer's right to own the products they buy. While the FTC has taken some limited actions with regard to this issue, a lack of clarity and enforcement has led to an ecosystem where consumers cannot reliably count on the connected products they buy to last. Further measures will help alleviate the worst outcomes of software tethering, that is, making functions of a device reliant on embedded software that ties the device back to a manufacturer's servers. This software-server connection tethers the device to the manufacturer, giving the manufacturer post-purchase control of the software and changing the nature of ownership.[1]

Consumers increasingly face a death by a thousand cuts as connected products they purchase lose their software support or advertised features that may have prompted the original purchase. They may see the device turned into a brick or their favorite features locked behind a subscription. Such software tethers also prevent consumers from reselling their purchases, as some software features may not transfer[2], or manufacturers may shut down devices, causing a second-hand buyer harm.

In the last three months we have seen one business brick a device and another company limit the consumer's ability to resell their product by locking away features behind a subscription. In July customers who had spent $1,695 on a Snoo connected bassinet discovered that some of the features that originally were advertised with the product would become part of a new, $19.99

[1] Zittrain, J.L. (2008). Perfect Enforcement on Tomorrow's Internet. In R. Brownsword, & K. Yeung (Eds.), Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes. (pp. 125-156). Oxford: Hart Publishing.
[2] "Does Full Self-Driving (FSD) Transfer When You Sell a Tesla?" *Find My Electric*. July 25, 2024. https://www.findmyelectric.com/blog/does-full-self-driving-fsd-transfer-when-you-sell-a-tesla/

monthly subscription[3]. Happiest Baby, which makes the Snoo, told customers in June that it planned to move features such as a weaning mode, sleep tracking, car ride mode, and more to a premium service starting July 15. Customers who already had purchased the bassinet for those features don't have to pay the monthly fee, but if they want to resell their Snoo or give it to others, the new buyers will not have access to those features. Given the short shelf life of a bassinet and the cost of the Snoo, there is a thriving resale market for the device that Happiest Baby now can monetize.

Recent examples of a manufacturer bricking a connected device include Spotify, which in May told buyers of its $89.99 Car Thing device that support for the product would end in December 2024 only 22 months after Spotify first launched the product for sale[4]. Initially Spotify didn't even offer any sort of refund for device owners, but later did provide customers who complained refunds on their Spotify subscriptions.

Another example comes from July 2023 when a temperature regulating device called iKamand, which worked in conjunction with the Commando Joe smoker was discontinued. The device cost $250 and was sold through 2023. It was abruptly shut off ahead of the July 4th holiday after the company that made the iKamand device (Masterbuilt) was acquired by Middleby, which then launched a $1,700 competing product that used a different app.

Other products that have been bricked include a bevy of products from failed startups such as the Mellow sous vide cooker, the Juicero juicer, the Leelo smart plug, Kano smart computers for kids, Spire breath monitoring devices, and many more. Even established companies kill their connected products such as Google ending support for still operational Dropcam cameras in April 2024[5], Arlo ending support for early models of its cameras this summer[6], and Amazon ending support for its Halo line of wearables and health and wellness devices.

In some cases the decision to end support for a product is done well with advance notice, refunds, and a plan to recycle the non-working hardware. But in most cases, consumers end up with a hunk of e-waste that could still function with the right software, and a sense of disappointment. Add to this, consumers have spent money on a product without understanding the limited lifespan of that device. Knowledge of the expected lifespan and an understanding that the lifespan was reliant on software, not the physical failure of the device, would certainly change consumers' purchasing decisions.

---

[3] Jay Peters, "This $1,695 smart bassinet's best features are now behind a premium subscription." *The Verge*. July 7, 2024.
https://www.theverge.com/2024/7/20/24202166/snoo-premium-subscription-happiest-baby
[4] Stacey Higginbotham, "How to Kill a Smart Device: Spotify Car Thing Post Mortem" Consumer Reports Innovation. May 28, 2024.
https://innovation.consumerreports.org/how-to-kill-a-smart-device-spotify-car-thing-post-mortem/
[5] "Support for Dropcam and Dropcam Pro ended." Google Nest Help. accessed August 2, 2024.
https://support.google.com/googlenest/answer/9257288?hl=en
[6] "End of Life for Arlo Legacy Cameras and Arlo Services." Arlo. April 24, 2024.
https://kb.arlo.com/000063018/End-of-Life-for-Arlo-Legacy-Cameras-and-Arlo-Services

In general, when consumers buy a connected device, the software will fail long before the physical device does, and companies offer widely varying responses to these shut downs. For example, Ecobee supported its first-generation smart thermostats for 16 years and when it dropped support it assured consumers their thermostats would still control the customer's HVAC system. Awair stopped supporting some of its older air quality monitoring devices, by killing the app, but assured consumers that the LED on the physical product could still provide basic information about the air quality. Other companies kill software support and also the device itself, as Facebook did with its Portal product.

Even when a connected device retains software support through its app, it can lose functions that a consumer relied on the product for. For example, many connected devices launch with promises that they will work with specific ecosystems, such as Amazon's Alexa or Apple's HomeKit. But these functions are reliant on business agreements between the companies, and may founder. Chamberlain's MyQ garage door opener stopped working with a variety of smart home platforms after the makers of the garage door system stopped letting outside companies access its API[7].

Consumers only have to look to their bathrooms for another example of a company pulling support for a feature advertised at purchase. In 2020, Oral-B launched a $230 Guide toothbrush that functioned like an Amazon's Alexa speaker advertising on the box that it had "Alexa Built In." But in February of 2024, Oral-B killed the app that allowed users to connect that toothbrush to Alexa, meaning that users who buy the toothbrush today, or those who have lost a Wi-Fi connection to the toothbrush, have no ability to use the product as initially advertised[8]. The smart home is littered with examples of this sort of bait and switch for consumers.

Many of these examples are for relatively small purchases and have historically been shrugged off as consumers who are investing in the bleeding edge. It's easy to dismiss consumers who may have spent $350 in 2018 on a Levi's denim jacket that contained "smart sensors" to let the user control their phones by swiping on the sleeve only to see the app for this jacket shut down in April 2023[9]. However, consumers are buying more and more products that come with software tethers, including their cars and their major appliances. With smaller devices, the loss of control over physical devices, and consumers' lack of knowledge about when and how these products may fail represents a death by a thousand cuts. With larger products, uncertainty around how and when these products might fail represents the loss of a substantial investment and the creation of literal tons of waste.

---

[7] Jennifer Pattison Tuohy. "This smart garage door controller is no longer very smart." *The Verge*. November 8, 2023. https://www.theverge.com/23949612/chamberlain-myq-smart-garage-door-controller-homebridge-integrations

[8] Scharon Harding. "Oral-B bricking Alexa toothbrush is cautionary tale against buzzy tech." Ars Technica. June 5, 2024. https://arstechnica.com/gadgets/2024/06/oral-b-bricks-ability-to-set-up-alexa-on-230-smart-toothbrush/

[9] Kyle Bradshaw. "Google shutting down the Jacquard smart fabric app in April" *9to5Google*. March 28.2024. https://9to5google.com/2023/03/28/google-shutting-down-jacquard-app/

And companies don't have to proactively change the terms associated with their software tethered devices to cause consumers harm. They can also simply stop updating their software, letting them degrade as computer makers push out new operating systems, or refuse to continue to support the products with patches for potential security vulnerabilities. The FTC has documented this failure to issue security updates in its 2018 study[10] on mobile phone manufacturers rightly pointing out that there are two consumer harms associated with a failure to update. The first is that the failure to update products after a vulnerability is discovered renders the device vulnerable and less useful for the product owner (or actively harmful), but also that the failure to disclose how long a company plans to support software updates makes it impossible for a consumer to choose a product that will stay secure over time.

While the FTC's study involved mobile phone manufacturers, Consumer Reports's cybersecurity testing team has documented a lack of transparency around security updates for a wide range of IoT products including large appliances and popular security systems. For example, Consumer Reports is finalizing research that analyzes the publicly available documents and manuals provided by 22 different popular appliance makers to see what they said about the length of time each manufacturer provided software updates for their products. Out of the 22, only three brands — IKEA, GE and Fisher & Paykrel — provided a set time period over which they would provide cybersecurity and regular updates. Another four (Amana, KitchenAid, Maytag, Whirlpool) clearly said that they would provide support and or firmware updates for the product, but did not provide a specific time period. The rest provided only vague warranty information or didn't provide any information about longevity at all.

We expect the problem to get worse over time as more companies build "smart" products that connect to the internet or are app controlled. Thus, we are seeking clear guidance from the FTC, because despite the FTC's investigation into Google shutting down the Revolv home hub in 2016[11], the practice continues, leaving consumers stuck with products they cannot use, they cannot resell and are good only for the landfill.

The FTC has a number of tools at its disposal to help establish standards for IoT device support. While a formal rulemaking is one possibility, the FTC also has the ability to issue more informal guidance, such as its Endorsement Guides[12] and Dot Com Disclosures.[13] We believe the agency should set norms around the following five items:

---

[10] Press Release. Federal Trade Commission. "FTC Recommends Steps to Improve Mobile Device Security Update Practices." February 28, 2018. https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-recommends-steps-improve-mobile-device-security-update-practices

[11] https://www.ftc.gov/legal-library/browse/cases-proceedings/closing-letters/nest-labs-inc

[12] 16 C.F.R. § 255.0 July 26, 2023

[13] Federal Trade Commission. ".com Disclosures: How to Make Effective Disclosures in Digital Advertising." March 2013. https://www.ftc.gov/system/files/documents/plain-language/bus41-dot-com-disclosures-information-about-online-advertising.pdf

1. **Require disclosure of a guaranteed minimum support time on the product packaging**: Companies should plan for and disclose, to the consumer, their plans for both security updates but also anticipated engineering and cloud resources to keep a product functional to a certain date. This date can be extended at the company's discretion, but should represent the minimum amount of time that the consumer can rely on the product to keep working. The Federal Communications Commission has started down this path with its voluntary U.S. Cyber Trust Mark program that asks those that get the label to include a minimum support date by which consumers can expect to receive security updates, but also allows companies to state that they have no plans to include support time frames. The ability to ignore the requirement to post a minimum support date, and the voluntary nature of the FCC's program means there is still a sizable opportunity for companies to harm consumers by shutting down or stopping security updates for their connected devices without providing any compensation or even notice to consumers.

   Commensurate with mandated minimum support time frames on packaging, the FTC should also help establish minimum support expectations for different classes of devices. Consumers are using trial and error to figure out the expected lifespan of their connected products. But when it comes to cars, large connected appliances, or products installed in homes the agency should establish clear guidelines for an expected lifespan that matches software support to the hardware lifespan.

2. **Require companies to ensure that the core functionality of a product will work even if the internet connection fails or the software stops getting updated**. An e-bike should start without a connection to the server or control from an app. An oven should maintain its ability to heat food and a thermostat should still retain the ability to control an HVAC system.

3. **Encourage tools and methods that enable reuse if software support ends**. Companies could create and distribute tools and software to repurpose products so products provide continued use. Tools could include upgrades to hardware so manufacturers can continue software support, or software that would allow consumers to repurpose the hardware for offline use, and should be continually available for the reasonably likely lifespan of the hardware.

4. **Protect "adversarial interoperability."** One way products can be repurposed is when a competitor or third-party creates a reuse or modification tool -- something that adds to or converts the old device. These tools are often the subject of copyright lawsuits. For example, a company could build a tool to rewrite the software on a Sonos speaker, no longer supported by the manufacturer, so that speaker could continue to be used, but because of the legal liability, it is very unlikely a company would risk selling such a tool. Protecting adversarial interoperability incentivizes corporations to provide consumers with reuse options at the end of a product's life, ensures that entrepreneurs can innovate with alternative reuse options for hardware, and thereby enables competition in the

reuse market. The FTC has already come out in favor of allowing exemptions to the copyright law so consumers can repair devices they own[14]. Similar support of adversarial interoperability could revitalize the reuse market and ensure that far less hardware gets trashed when it loses software support.

5. **Conduct an educational program to encourage manufacturers to build longevity into the design of their products**. Much like the Cybersecurity Infrastructure and Security Agency has pushed its Secure by Design program to encourage companies to build security into their products from the beginning, we encourage the FTC to create a clear list of design principles that would promote the longevity of the connected products manufacturers sell. These principles could include repairability scores, replaceable batteries, modular electronic elements that allow for aged chips and modems to be swapped out, and requirements to calculate the ongoing cost of supporting every connected device sold. The effort could be modeled on the agency's 2017 Stick with Security guidance and Start with Security publication that was designed to inform companies about how to safeguard sensitive consumer data.

More consumer products will have software embedded into them, but it's time that enforcement catches up to the reality of millions of consumers who have experienced the unexpected loss of function in a product that should still work. Consumers are spending their hard-earned money on products without a clear understanding of when or how these products will fail. And when they fail at the whim of the manufacturers, they have little or no resource to recoup their money or keep the product operational.

Mandating companies include minimum support times on their connected products enables consumers to make informed choices about which products to purchase. Clear communications around the expected lifespan of connected products will help manufacturers allocate resources for their connected products and help regulators recognize egregious examples of software obsolescence. It will also help consumers understand the tradeoffs they may be making when they choose a connected product over a "dumb" one.

When possible, providing consumers with the tools to continue using their connected devices absent official support will help keep waste out of landfills and maintain the consumers right of ownership of a physical product. When providing those tools are impossible, the agency should consider those product subscriptions to be sold and marketed accordingly.

And finally, the agency should create a dedicated education campaign to encourage companies to design their software-reliant products with longevity in mind. Taking these steps will require the FTC to dedicate more resources to establish clear guidance and then enforce that guidance going forward. We call on the agency to make that commitment. Consumers are already being

[14] US Department of Justice and Federal Trade Commission. Exemptions to Permit Circumvention of Access Controls on Copyrighted Works Docket No. COLC-2023-004 March 14, 2024. https://www.ftc.gov/system/files/ftc_gov/pdf/ATR-FTC-JointComment.pdf

burned by software obsolescence, and absent guidance and enforcement, we are seeing companies roll the dice on selling connected devices that they have no intention of standing behind. This harms consumers who purchase these products in good faith and it harms the environment when those products end up in landfills.

Thank you for considering our request, and we are available if you have additional questions at, justin.brookman@consumer.org, stacey.higginbotham.consultant@consumer.org and lucas.gutterman@publicinterestnetwork.org.

Respectfully,

Justin Brookman
Consumer Reports

Stacey Higginbotham
Consumer Reports

Lucas Gutterman
U.S. PIRG

Elizabeth Chamberlain
iFixit

Hayley Tsukayama
Electronic Frontier Foundation

Denver Gingerich
Software Freedom Conservancy

Nick Lapis
Californians Against Waste

Birny Birnbaum
Center for Economic Justice

Paul Roberts
SRFF (Secure Resilient Future Foundation)

Peter Mui
Fixit Clinic

C. Eric Lundgren

BigBattery, Inc. : OutBack Power, Inc. : TitanGreen, Inc.

Heather Trim
Zero Waste Washington

Bonnie Monteleone
Plastic Ocean Project, Inc.

Suzie Fromer
Repair Cafe Hudson Valley

Dave West
Repair Cafe

Tara de la Garza
Inventurous

Nirvan West
Digitunity

Octavia Vinsmoke
Hamilton Computer Repairs