Loyola of Los Angeles Law Review

Volume 57 | Number 1 Article 2

Spring 5-28-2024

Global Product Liability for Dumb 'Smart' Home Devices

Michael L. Rustad

Layth Hert

GLOBAL PRODUCT LIABILITY FOR DUMB 'SMART' HOME DEVICES*

*Michael L. Rustad** & Layth Hert****

The number of smart homes globally has increased to 300 million, and the smart home market is expected to reach approximately $181.4 billion by 2025. These new developments, however, are accompanied by related security risks. The attack surface for smart home devices poses latent dangers because of inadequate security that enables cybercriminals to gain access to such devices.

This Article proposes extending product liability to address security vulnerabilities in smart home devices. Part I examines the ubiquity of smart home devices. Part II sets forth the breadth of security vulnerabilities in connected devices, confirming the need to clarify that product liability applies to software and to create a global standard that reduces compliance costs for smart home device makers. Part III develops a detailed global standard for smart home device product liability, aligning U.S. product liability law with the proposed revision of the European Union's Product Liability Directive 85/374/EEC.

.

---

* The title of our Article is inspired by *The Wall Street Journal* article entitled *Stressed by Smart Tech? Consider These 'Dumb' Devices*. *See* Justin Pot, *Stressed by Smart Tech? Consider These 'Dumb' Devices*, WALL ST. J. (Apr. 15, 2022), https://www.wsj.com/articles/stressed-by-smart-tech-consider-these-dumb-devices-11650039709 [https://perma.cc/DG65-JYVN].

** Michael L. Rustad, Ph.D., J.D., LL.M. is the Thomas F. Lambert Jr. Professor of Law and Co-Director of the Intellectual Property Law Concentration at Suffolk University Law School in Boston, Massachusetts. Abbas Kizilbash contributed useful research and editorial comments. Professor Rustad's faculty assistant Seth Markley made helpful editorial and substantive suggestions to improve this article. Finally, Professor Rustad appreciates the assistance of his wife, Chryss J. Knowles, for her editorial contributions.

*** Judicial Law Clerk, Connecticut Superior Court; J.D., Suffolk University Law School, May 2023, Intellectual Property Law Concentration with Distinction; B.A., Boston University, May 2020.

TABLE OF CONTENTS

INTRODUCTION 55
I. SMART HOME DEVICES' UBIQUITOUSNESS 57
A. Leading Smart Home Providers 57
B. Common Smart Home Devices 62
II. SECURITY RISKS OF SMART HOME DEVICES 63
A. Security and Privacy Vulnerabilities 63
B. Examples of Smart Home Vulnerabilities 66
III. PRODUCT LIABILITY TO ADDRESS DEFECTS IN SMART HOME DEVICES 67
A. Extending Product Liability to Software in Smart Home Devices 67
B. Conceptualizing Product Defects in Smart Home Devices 68
1. Manufacturing Defects 68
2. Design Defects 69
C. Tests for Design Defect 71
1. Consumer Expectation Test 72
2. Risk/Utility Test for Smart Home Devices 73
3. Risk/Utility with Reasonable Alternative Design Adapted to Smart Home Devices 74
4. Failure to Warn or Inadequate Warning for Vulnerabilities in Smart Home Devices 75
5. Malfunction Theory as a Substitute for a Defect 76
D. Strict Product Liability Extended to Smart Home Devices 76
1. Resolving Legal Lag 78
2. Extending European-Style Product Liability to Smart Home Devices 80
3. Shielding Smart Home Device Product Liability from Contractual Waivers 81
CONCLUSION 82

INTRODUCTION

"A smart home is a residential building with several interconnected smart systems; these embedded systems provide some advanced digital services to users, such as remote healthcare monitoring, the intelligent management of utilities, high-level security surveillance, etc."[1] Home security and smart home devices include doorbells, locks, cameras, lighting, thermostats, refrigerators, dishwashers, and ovens.[2] Smart homes give the homeowner "extensive access to many aspects of their home, even from a remote location."[3] The number of smart homes increased from 50 million in 2021 to 57.6 million in 2022; by 2023, the number climbed to 63.4 million.[4]

The number of smart homes globally has increased to 300 million.[5] The global "Smart Home" market is projected to reach $181.4 billion by 2025.[6] In 2023, the number of smart homes in the United States rose 10.2 percent from 2022 to a total of 63.43 million, which represents 48.7 percent of total U.S. households.[7] "[A]s many as 69.91 million households . . . are actively using smart home devices in

1. Mohammad Ali Nassiri Abrishamchi et al., *Smart Home Privacy Protection Methods Against a Passive Wireless Snooping Side-Channel Attack*, 22 SENSORS, Nov. 2022, at 1, 2, https://www.mdpi.com/1424-8220/22/21/8564 [https://perma.cc/EC3B-YTWA].

2. *Home Security for Smart Homes: Integrating Security with Home Automation*, STAYSAFE.ORG, https://staysafe.org/home-safety/home-security-for-smart-homes-integrating-security-with-home-automation/ [https://perma.cc/3Q2Z-HM5J]; Jack v. Ring LLC, 91 Cal. App. 5th 1186, 1191 (Ct. App. 2023) ("Ring LLC (Ring) manufactures and sells home security and smart home devices including video doorbells, security cameras, and alarms."); *23% of Broadband Homes Own 3 or More Smart Home Devices: Parks*, COMMC'NS DAILY (Feb. 12, 2021), https://communicationsdaily.com/article/2021/02/12/23-of-broadband-homes-own-3-or-more-smart-home-devices-parks-2102110026 [https://perma.cc/79N8-KZ9A] ("About 23% of U.S. broadband households owned three or more smart home devices in Q4, up from 19% in 2019 . . . ."); *see also* Aliza Vigderman & Gabe Turner, *Best Smart Home Security Systems of 2023*, SECURITY.ORG (Nov. 3, 2023), https://www.security.org/home-security-systems/best/smart-home/ [https://perma.cc/3UDG-BRRU].

3. Ziv Chang, *Inside the Smart Home: IoT Device Threats and Attack Scenarios*, TREND MICRO (July 30, 2019), https://www.trendmicro.com/vinfo/fr/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios [https://perma.cc/A7KN-U3P7].

4. *US Smart Home Statistics (2018-2027)*, OBERLO, https://www.oberlo.com/statistics/smart-home-statistics [https://perma.cc/KGE9-FDUD] [hereinafter *US Smart Home Statistics (2018-2027)*].

5. Alexis Curls, *Top 35 Smart Home Facts and Statistics*, TODAY'S HOMEOWNER (Dec. 31, 2023), https://todayshomeowner.com/smart-home/guides/smart-home-facts-and-statistics/ [https://perma.cc/Y5XD-CZAA].

6. *Revenue of the Smart Home Market Worldwide from 2018 to 2027*, STATISTA (Aug. 17, 2023), https://www.statista.com/forecasts/887554/revenue-in-the-smart-home-market-in-the-world [https://perma.cc/P79M-CA98].

7. *US Smart Home Statistics (2018-2027)*, *supra* note 4.

2024."[8] Google Home and Amazon Echo enable connected smart devices to work together and be controlled remotely:

> With Amazon Alexa and Google Assistant, you can set up routines for your devices to work together and do multiple things at once, such as adjusting the temperature and lighting when you get home. With Apple HomeKit, you can control your devices with Siri voice commands, or from an Apple Watch, and create scenes to trigger several devices at the same time. Using IFTTT, a service that many of the top smart home brands support, you can link various internet-connected devices and easily program them to respond to real-world events, such as setting your lights to turn on automatically at sunset. And the rollout of Matter, a new smart home interoperability standard, makes it easier than ever to set up and integrate connected gadgets.[9]

Oberlo projects the following smart home statistics:

> Smart home statistics show that the US smart home market is set to continue growing. Annual growth rates of 10.2% have been forecast from 2024 to 2027. This means that in 2024, the number of smart homes in the US is estimated at 69.91 million. This will rise to 77.05 million in 2025, before growing to 84.92 million in 2026. By 2027, there will be 93.59 million households using smart devices in the US.[10]

The global smart home market is predicted to reach $137.9 billion by 2023, "growing at a CAGR [Compounded Annual Growth Rate] of 13.61% between 2017 and 2023."[11] The global expansion of smart homes is due to the "increasing adoption of smart home devices, rising

8. *Id.*

9. Angela Moscaritolo, *The Best Smart Home Devices for 2023*, PC MAG. (June 30, 2023), https://www.pcmag.com/picks/the-best-smart-home-devices [https://perma.cc/V3XV-U5F3].

10. *US Smart Home Statistics (2018-2027)*, *supra* note 4.

11. Newstex, *Smart Home Market by Product (Lighting Control, Security Access Control, HVAC, Entertainment Other Control, Home Healthcare, Smart Kitchen, and Home Appliances*), RELEASEWIRE (Oct. 25, 2018, 3:30 PM), https://plus.lexis.com/document/?pdmfid=1530671&crid=532dd632-0513-44fc-bc9d-800a88e184ad&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A5TK1-4MF1-F03R-N0SG-0000000&pdcontentcomponentid=484276&pdteaserkey=&pdislpamode=false&ecomp=n74k&earg=sr0&prid=3f9a4532-c3a1-4040-b5ab-1883c9213d41 [https://perma.cc/38LG-D5L4].

demand for home automation, advancements in connectivity technology, and growing awareness of energy efficiency."[12]

As the technology of connected devices evolves, so will security vulnerabilities that will inevitably lead to injuries, loss of life, and property damage.[13] This Article recommends extending product liability to smart home devices, thus enabling consumers to have legal recourse when software inevitably fails.

Part I examines the expansion of smart home gadgets enabling consumers to access home appliances and devices remotely. Part II documents the seamy side of smart home devices with security vulnerabilities. This part of the Article calls for clarification that product liability should apply to software and the need for a global standard that reduces compliance costs for smart home device makers.

To achieve these goals, we propose implementing a federal product liability statute for smart home devices under which consumers have tort remedies when software fails and causes personal injury, death, or the invasion of privacy. Part III develops a detailed global standard for smart home device product liability. Our proposed reform introduces provisions to address liability for defective software in smart home devices, extending product liability to encompass smart home devices to compensate consumers for damages caused by security vulnerabilities. This suggested reform aligns U.S. product liability law for smart devices with the new directive on liability of defective products updating the European Union's Product Liability Directive of 1985.[14]

I. SMART HOME DEVICES' UBIQUITOUSNESS

A. Leading Smart Home Providers

"A smart home is an application of ubiquitous or pervasive computing or environment. Several synonyms are used [to refer to the]

12. SkyQuest Tech. Consulting Pvt. Ltd., *IoT Smart Home Market: Transforming the Modern Home and Revolutionizing Living*, YAHOO! FIN. (Apr. 4, 2023), https://finance.yahoo.com/news/iot-smart-home-market-transforming-123000104.html [https://perma.cc/43JP-7G3E] (defining smart homes).

13. *See* Davey Winder, *Confirmed: 2 Billion Records Exposed in Massive Smart Home Device Breach*, FORBES (July 2, 2019), https://www.forbes.com/sites/daveywinder/2019/07/02/confirmed-2-billion-records-exposed-in-massive-smart-home-device-breach/ [https://perma.cc/PJ92-QM2H].

14. Press Release, Eur. Comm'n, New Liability Rules on Products and AI to Protect Consumers and Foster Innovation (Sept. 28, 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5807 [https://perma.cc/KF8V-KEQY].

smart home, e.g., smart house, home automation, domotique, intelligent home, adaptive home, and aware house."[15] Technological advancements and the rise of e-commerce have led smart home devices to emerge on the market, particularly products like smart speakers.[16] Today, people rely extensively on smart home devices for everyday needs, particularly when it comes to the ease and convenience that accompany such devices and services.[17]

By accessing home appliances and devices remotely, users can accomplish certain tasks before arriving home.[18] Smart energy systems monitor electricity usage by implementing security as well as safety features.[19] Nine of the leading smart home providers are (1) Google Nest, (2) Amazon Alexa, (3) Apple HomeKit, (4) ecobee, (5) Bosch Smart Home Solutions, (6) Philips Hue, (7) Tuya Smart, (8) Belkin (Wemo), and (9) Wink.[20]

15. Muhammad Raisul Alam et al., *A Review of Smart Homes—Past, Present, and Future*, 42 IEEE TRANSACTIONS ON SYS., MAN, & CYBERNETICS, PT. C 1190, 1190–91 (2012).

16. *US Smart Home Statistics (2018-2027)*, *supra* note 4.

17. Alam et al., *supra* note 15, at 1191.

18. *Id.* at 1190.

19. *Id.*

20. Caroline Forsey, *The 13 Best Smart Home Devices & Systems of 2021*, HUBSPOT (Feb. 24, 2021) https://blog.hubspot.com/marketing/smart-home-devices [https://perma.cc/5JRX-E6TB]; *The Best Smart Home Companies in 2021: A Complete Overview*, BUDDY CO., https://www.buddycompany.com/post/best-smart-home-companies [https://perma.cc/XB47-EQZK]; *Tuya Smart Showcases New IoT Device Connectivity Capabilities at 2021 Mobile World Congress (MWC)*, CISION PR NEWSWIRE (June 28, 2021), https://www.prnewswire.com/news-releases/tuya-smart-showcases-new-iot-device-connectivity-capabilities-at-2021-mobile-world-congress-mwc-30132 1106.html [https://perma.cc/SBY9-CQ5K].

Chart One: Leading Smart Home Providers

Name of Company	***Country Headquartered***	***Affiliated Smart Devices***
Google Nest[21]	United States[22]	Google Nest Hub,[23] Google Nest Doorbell,[24] Nest Mini,[25] Nest Audio,[26] Nest Thermostat,[27] Google Nest Protect Smoke & Co,[28] Nest x Yale Lock[29]

21. *Welcome to Google Nest*, GOOGLE, https://store.google.com/au/category/connected_home?hl=en-GB [https://perma.cc/B7VA-HBWH].

22. *Mountain View (Global HQ)*, GOOGLE, https://www.google.com/about/careers/applications/locations/mountain-view/ [https://perma.cc/QQ3R-LJ72].

23. Bethan Girdler-Maslen, *The Google Nest Hub Hits Its Lowest Ever Price at John Lewis*, T3 (Apr. 19, 2022), https://www.t3.com/news/the-google-nest-hub-hits-its-lowest-ever-price-at-john-lewis [https://perma.cc/4WJ7-TWUU] ("The Google Nest Hub acts as the centre of your smart home operations and controls all your other smart devices and Google apps via touch or voice control. For example, you can watch streaming apps, see your favourite pictures from Google Photos, ask Google a question, change the temperature on your Nest thermostat and much more.").

24. Jim Martin, *How to Use Google Nest Cameras and Doorbell with Alexa*, TECH ADVISOR (May 13, 2022, 11:28 PM), https://www.techadvisor.com/article/746402/how-to-use-google-nest-cameras-and-doorbell-with-alexa.html [https://perma.cc/WK8G-C4XW].

25. *Nest Mini*, GOOGLE, https://store.google.com/product/google_nest_mini?hl=en-US [https://perma.cc/2B9L-5M7S].

26. *Nest Audio*, GOOGLE, https://store.google.com/us/product/nest_audio?hl=en-US [https://perma.cc/YK9H-ZN5G].

27. Charlie Fripp, *Best Google Nest Thermostat*, BESTREVIEWS (Apr. 7, 2022), https://bestreviews.com/articles/home/thermostats/home-best-google-nest-thermostat [https://perma.cc/H4VE-485W].

28. *Nest Protect Smoke and CO Alarm*, GOOGLE, https://store.google.com/us/product/nest_protect_2nd_gen?hl=en-US [https://perma.cc/Z5L3-AU6R].

29. *Next x Yale Lock*, GOOGLE, https://store.google.com/us/product/nest_x_yale_lock?hl=en-US [https://perma.cc/YPK9-ZP4A].

Amazon Alexa[30]	United States[31]	Echo smart speakers,[32] Echo Dot,[33] smart bulbs,[34] security systems,[35] and appliances[36]
Apple HomeKit[37]	United States[38]	Smart lights, bulbs, locks, motion sensors, room quality monitors, outlets, switches, thermostats, and an ecosystem for other smart device makers[39]
Ecobee (Canadian Home	Canada[41]	Smart Thermostats, Smart Sensors, and Ecobee switches[42]

30. *What is Alexa?*, AMAZON, https://developer.amazon.com/en-GB/alexa [https://perma.cc/WGM9-ZZ56] ("Alexa is Amazon's cloud-based voice service available on more than 100 million devices from Amazon and third-party device manufacturers. With Alexa, you can build natural voice experiences that offer customers a more intuitive way to interact with the technology they use every day.").

31. *Corporate Offices*, AMAZON, https://www.aboutamazon.com/workplace/corporate-offices [https://perma.cc/WBS2-RHSL].

32. *The Best Amazon Echo Smart Speakers of 2023*, REVIEWED, https://reviewed.usatoday.com/smarthome/best-right-now/the-best-amazon-echo-smart-speakers [https://perma.cc/8YAW-Z8XT].

33. Ty Pendlebury, *Amazon Echo Dot (5th Gen) Review: The Best Echo on a Budget*, CNET (July 29, 2023, 3:00 AM), https://www.cnet.com/home/smart-home/amazon-echo-dot-5th-gen-review-the-best-echo-on-a-budget/ [https://perma.cc/F2PD-UMDS].

34. Amazon Basics—Smart A19 LED Light Bulb, AMAZON.COM, https://www.amazon.com/Amazon-Basics-Smart-Light-Changing/dp/B09BFRLZZ5 [https://perma.cc/RF3D-QDGA].

35. Molly Price, *How to Set Up Alexa Guard Plus on Your Amazon Echo Smart Speakers and Displays*, CNET (Feb. 8, 2021, 12:11 PM) https://www.cnet.com/home/smart-home/how-to-set-up-alexa-guard-plus-on-your-amazon-echo-smart-speakers-and-displays/ [https://perma.cc/ULW3-VKGP].

36. Victoria Giardina, *The 20 Best Smart Home Devices on Amazon in 2023*, NY POST (Feb. 1, 2023, 2:56 PM), https://nypost.com/article/best-smart-home-devices-on-amazon/ [https://perma.cc/NZM3-4GPX].

37. *See* Kate Kozuch, *Apple HomeKit: What Is It, and How Do You Use It?*, TOM'S GUIDE (Oct. 13, 2020), https://www.tomsguide.com/us/apple-homekit-faq,review-4195.html [https://perma.cc/3AXK-6QZW] ("Apple HomeKit is a system that lets you control all of the best smart home devices, so long as they're compatible. It gives you control over your smart thermostat, lights, locks and more in multiple rooms, creating comfortable environments and just the right ambiance with a tap on your smartphone. You can even use it to control your devices remotely.").
Id.; *see, e.g.*, Press Release, Belkin, Wemo Stage Scene Controller Available Now (Apr. 22, 2021), https://www.belkin.com/pr-wemo-stage-scene-controller-available-now.html [https://perma.cc/M9B3-RQVU] (detailing how Wemo users can integrate their lights and appliances using Apple HomeKit).

38. *Apple Park*, APPLEINSIDER, https://appleinsider.com/inside/apple-park [https://perma.cc/24RF-S28W].

39. Smart Home Accessories, APPLE.COM, https://www.apple.com/shop/accessories/all/homekit [https://perma.cc/2MV3-XUK6].

41. *Smart Home Leader Ecobee Opens New Toronto Headquarters to Further Innovation and Growth*, CISION, https://www.newswire.ca/news-releases/smart-home-leader-ecobee-opens-new-toronto-headquarters-to-further-innovation-and-growth-656471323.html [https://perma.cc/P3JH-WGZC].

42. Ecobee Switch+ Smart Light Switch, AMAZON.COM, https://www.amazon.com/ecobee-Switch-Smart-Amazon-Built/dp/B0798LCLJ5 [https://perma.cc/63AG-T9D6].

Automation Companies)[40]		
Bosch Smart Home Appliances[43]	Germany[44]	Motion Sensors, Environmental Sensors, Smart Sensors[45]
Philips Hue[46]	The Netherlands[47]	Philips Hue Play,[48] Gradient Lightstrips, Smart Table Lamp[49]
Tuya Smart[50]	China[51]	Robot Vacuums, Smart Cameras, Smart Pet Products, Smart Locks, Smart Kitchen Appliances, and Smart Gateways/Sensors[52]

40. *See* Daniel Golightly, *Ecobee Smart Thermostat Enhanced Review—Everything You Need & Nothing You Don't*, ANDROID HEADLINES (June 7, 2020), https://www.androidheadlines.com/2022/06/ecobee-smart-thermostat-enhanced-review.html [https://perma.cc/Y2TR-U53G] ("Smart home company ecobee has been at or near the top of that market almost since its inception, offering great deals on everything from cameras to myriad sensors and thermostats. The company recently offered to send out its latest Smart Thermostat, the ecobee Smart Thermostat Enhanced, for review."); *accord* Gary Ng, *Ecobee Launches Smart Thermostats 'Premium' and 'Enhanced' in Canada*, IPHONE CANADA (May 17, 2022), https://www.iphoneincanada.ca/2022/05/17/ecobee-launches-smart-thermostats-premium-and-enhanced-in-canada/ [https://perma.cc/7GAF-3MUH]; *see also* Press Release, Ecobee Honored by EPA and U.S. Department of Energy as 2022 ENERGY STAR Partner of the Year, ECOBEE (May 5, 2022) https://www.ecobee.com/en-us/newsroom/press-releases/ecobee-honored-by-epa-and-u-s-department-of-energy-as-2022-energy-star/ [https://prema.cc/53NN-Q67E]. "[T]his award recognizes ecobee's demonstrated leadership and commitment to improving energy efficiency through its continued innovations, including its ecobee smart thermostats, and intelligent software platform, eco+, designed to improve energy efficiency, benefiting both consumers and the planet." *Id.*

43. *See Master Your Home with Smart Appliances*, BOSCH, https://www.bosch-home.com/us/experience-bosch/home-connect [https://perma.cc/RA69-FP9M]. "You know the feeling when some days just go your way? That's the philosophy behind Bosch connected appliances with Home Connect. Now you can intelligently manage and organize household tasks through the simple convenience of smart appliances with Home Connect." *Id.*

44. *Bosch Smart Home—Business Information*, ZOOMINFO, https://www.zoominfo.com/c/bosch-smart-home-gmbh/421136742 [https://perma.cc/5N57-MDDR].

45. *Sensing Solutions for Smart Homes & IoT*, BOSCH, https://www.bosch-sensortec.com/applications-solutions/smart-home/ [https://perma.cc/6GG8-XE33].

46. *Philips Hue*, CRUNCHBASE, https://www.crunchbase.com/organization/philips-hue [https://perma.cc/4CSD-YLKM].

47. *Id.*

48. Search Results for 'Philips Hue Products,' AMAZON.COM, https://www.amazon.com/s?k=philips+hue+products [https://perma.cc/6Q8T-BEEP].

49. *See* Rikka Altland, *Philips Hue Launches B2G1 FREE Sale on Smart Bulbs and Starters, Plus 50% Off Mood Lighting*, 9TO5TOYS (June 13, 2022, 10:28 AM), https://9to5toys.com/2022/06/13/philips-hue-mood-lighting-sale/ [https://perma.cc/VUC9-NUV7]; *see also* Search Results for 'Philips Hue Products,' AMAZON.COM, https://www.amazon.com/s?k=philips+hue+products [https://perma.cc/6Q8T-BEEP].

50. *See Tuya Smart*, EQUAL OCEAN, https://equalocean.com/company/tuya-smart [https://perma.cc/GY24-NJHE].

51. *Id.*

52. *How Tuya Accelerates Your Smart Home Business*, TUYA, https://pages.tuya.com/expo/contact_form? [https://perma.cc/5SLH-HQ66].

Belkin (Wemo)[53]	United States[54]	Wemo Smart Plugs, Wemo Stage Scene Controller, Wi-Fi Smart Dimmers, Belkin Wemo Wi-Fi Switch, and Wemo Smart Light Switch 2D Gen[55]
Wink[56]	United States[57]	Wink Hub, Wink Motion Sensor, Wink Door/Window Sensor, Wink Siren and Chime[58]

B. Common Smart Home Devices

According to one industry leader, "[s]marter cities, cars, homes, machines and consumer devices will drive the growth of the Internet of Things along with the infrastructure that goes with them, unleashing a wave of new possibilities for gathering data, predictive, analytics and automation."[59] The use of smart home devices has increased significantly; now, more than half of American adults have installed at least

53. Jake Smith, *Foxconn Buys Belkin, Linksys and Wemo for $866 Million*, ZDNET (Mar. 26, 2018) https://www.zdnet.com/home-and-office/networking/amazon-says-new-eero-max-7-wi-fi-device-will-let-you-download-a-4k-movie-in-seconds/ [https://perma.cc/8C5M-W8D8].

54. *Id.* ("Founded in 1983, Belkin is headquartered in Los Angeles, CA with more than 1,400 employees worldwide. Belkin completed its acquisition of network hardware-maker Linksys from Cisco in March 2013.")

55. *See* Wemo WiFi Smart Dimmer, BELKIN, https://www.belkin.com/wifi-smart-dimmer/P-WDS060.html [https://perma.cc/58LC-EFE8]; WeMo Smart Light Switch 2nd Gen, AMAZON.COM, https://www.amazon.com/WeMo-Smart-Light-Switch-2ND/dp/B07RT8H9WH?th=1 [https://perma.cc/M4BY-22ZQ].

56. *Wink*, CRAFT, https://craft.co/wink [https://perma.cc/5CPJ-8X45] ("Wink is an IoT technology company. It designed a platform that keeps users connected to their home—no matter where they are. All brands are connected through a single app, so users don't need a different one for every product. Simple controls allow them to monitor and manage everything in home.").

57. *Wink Headquarters and Office Locations*, CRAFT, https://craft.co/wink/locations [https://perma.cc/JJ3M-U3X8].

58. Products, WINK, https://www.wink.com/products/ [https://perma.cc/425P-9ESL].

59. Mohana Ravindranath, *IBM, AT&T to Partner on Connected Cities, Internet of Things*, WASH. POST (Feb. 18, 2014, 3:40 PM), https://www.washingtonpost.com/business/on-it/ibm-atandt-to-partner-on-connected-cities-internet-of-things/2014/02/18/de3e5e04-98bc-11e3-80ac-63a8ba7f7942_story.html [https://perma.cc/2MSC-4FW6]. The term "the Internet of Things" (IoT) is used throughout this Article and refers to:

> a *network of physical devices, vehicles, appliances and other physical objects that are embedded with sensors, software and network connectivity that allows them to collect and share data*. These devices — also known as "smart objects" — can range from simple "smart home" devices like smart thermostats, to wearables like smartwatches and RFID-enabled clothing, to complex industrial machinery and transportation systems. Technologists are even envisioning entire "smart cities" predicated on IoT technologies.

What Is the Internet of Things (IoT)?, IBM, https://www.ibm.com/topics/internet-of-things [https://perma.cc/YDV6-VV5W] (emphasis added).

one smart device in their home.[60] Smart devices may be incorporated in a new residence but many are added after construction.[61] For example, smart speakers like Amazon Echo or Google Nest, Roombas, and smart TVs are accessories to a finished home.[62]

While their advantages are apparent when it comes to efficiency and ease of use, many smart devices contain latent defects that threaten American households. Part II of this Article presents the security and privacy risks of smart home devices.

II. SECURITY RISKS OF SMART HOME DEVICES

A. Security and Privacy Vulnerabilities

Smart home devices have become commonplace in today's world, especially considering their convenience, in light of consistent technological advancements. These new developments, however, are accompanied by related security risks. In considering the various security and privacy vulnerabilities, the full breadth and extent of smart home devices will be appraised. Smart home devices pose hidden dangers because of inadequate security that enables cybercriminals to gain access to such devices.[63]

Smart home devices with known security susceptibilities enable cybercriminals to break into smart home networks.[64] Machine-to-machine communications of internet-connected home devices such as thermostats, baby monitors, and refrigerators are "creating a new level of risk—by providing hackers with new vulnerabilities to exploit."[65]

"Companies that provide [IoT] consumer products, such as Internet-enabled washing machines, thermostats, baby monitors, and security cameras," can also exploit consumer data as well as transfer and

60. Bret Kinsella, *Over Half of U.S. Adults Have Smart Home Devices, Nearly 30% Use Voice Assistants with Them—NEW REPORT*, VOICEBOT.AI (June 20, 2022, 3:35 PM), https://voicebot.ai/2022/06/20/over-half-of-u-s-adults-have-smart-home-devices-nearly-30-use-voice-assistants-with-them-new-report/ [https://perma.cc/38KX-5AXR].

61. *15 Popular Smart Home Devices That Are Changing the Way We Live*, URBAN ACRES (Feb. 26, 2022) https://urbanacres.com/blog/15-popular-smart-home-devices-that-are-changing-how-we-live/ [https://perma.cc/45M7-U9CY].

62. *Id.*

63. David Paddon, *Popularity of 'Smart Home' Devices Raises Cybersecurity Risks*, GLOBE & MAIL (Dec. 3, 2017), https://www.theglobeandmail.com/technology/popularity-of-smart-home-devices-raises-cybersecurity-risks/article37171086/ [https://perma.cc/UE2P-5CT2].

64. Chang, *supra* note 3.

65. Paddon, *supra* note 63.

disclose it to third parties, thus endangering consumers.[66] Cybercriminals could hack into smart home devices, such as smartwatches, in order to access connected devices, like security cameras, thermostats, or door locks, generating a material threat to personal security.[67] "For example, if someone loses their watch or it is stolen, and they do not have anti-theft settings enabled, [a criminal] could unlock their home's locks and enter their home."[68]

Smart home devices increase efficiency and convenience but can also enable cybercrime if left unsecured. "Smart home systems can leave owners vulnerable to serious threats, such as arson, blackmail, theft and extortion."[69] Eight of ten Internet of Things (IoT) devices have known security flaws, "creating a tremendously vulnerable IoT landscape. Many IoT devices are not designed with security in mind or built-in, and as a result many IoT devices have considerable security risks—both physical and digital—and also suffer from big privacy issues."[70]

A review of security and privacy policies for mobile phone applications conducted in the European Union "reported that some apps and mobile app stores offer a permissive environment which leads to

---

66. Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1372 (2017); *see* Jiahong Chen & Lachlan Urquhart, *'They're All About Pushing the Products and Shiny Things Rather Than Fundamental Security': Mapping Socio-Technical Challenges in Securing the Smart Home*, 31 INFO. & COMMC'NS TECH. L. 99, 108 (2022). One technical lead at an IoT company stated:

> [I]f you compromise someone's heating, that will—on its own it doesn't sound like a big deal because you could just turn it down but then there's the elderly, which may not be able to turn down their heating or turn up their heating. So, in winter, or the summer, that could actually be potentially lethal.

Id.

67. *How Exposed Smartwatches and Other Wearable Devices Are to Cyberattacks*, CE NOTICIAS FINANCIERAS ENG. (June 16, 2022), https://plus.lexis.com/document/?pdmfid=1530671&crid=cd11da91-43b7-4ba0-bc69-1523306aa7b6&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A65PS-CR81-JCG7-84S6-00000-00&pdcontentcomponentid=443607&pdteaserkey=&pdislpamode=false&ecomp=n74k&earg=sr0&prid=c044c9ea-303c-49dc-a688-957588a93404 [https://perma.cc/DW6J-V9FY].

68. *Id.*

69. Earlence Fernandes, *Security Risks in the Age of Smart Homes*, CONVERSATION (May 29, 2016, 9:00 PM), https://theconversation.com/security-risks-in-the-age-of-smart-homes-58756 [https://perma.cc/DZZ8-VKZ9].

70. BullGuard, *New Dojo Intelligent IoT Vulnerability Scanner App Provides Consumers with Deep Insight into the Cybersecurity Risks in Their Smart Homes*, CISION PR NEWS WIRE (June 5, 2018, 9:00 PM), https://www.prnewswire.com/news-releases/new-dojo-intelligent-iot-vulnerability-scanner-app-provides-consumers-with-deep-insight-into-the-cybersecurity-risks-in-their-smart-homes-300659759.html [https://perma.cc/9S7N-JMW6].

malicious or risky apps being available to users."[71] The SAM Seamless Network, an Israeli company, evaluated the security weaknesses of IoT devices. It concluded that 47 percent of the most vulnerable devices were smart home security cameras, "followed by smart hubs such as Google Home [and] Amazon Alexa."[72] The largest number of attacks on these devices originated in China, followed by the United States.[73]

With the rise of connected homes via smart home devices, cyberattacks are becoming increasingly ubiquitous.[74] A home equipped with smart home networks receives an average of five attempted attacks per device per day.[75] For example, cybercriminals target security cameras because they can easily access these devices due to consumers' use of default passwords and usernames to connect to their home network.[76] Smart home attacks include "hackers remotely controlling smart lights and smart TVs, unlocking IoT-enabled doors, and remotely turning on and streaming video from smart cameras."[77] An anonymous attacker reprogrammed a Milwaukee home thermostat to over thirty degrees Celsius, or eighty-six degrees Fahrenheit.[78]

Cybercriminals can use WeMo to attack smart TVs and other devices: once the hacker has "established a foothold on the network and [is] able to open arbitrary ports, any machine connected to the network

71. MARIAM ELGABRY & SHANE JOHNSON, SYSTEMATIC REVIEW OF SECURITY AND PRIVACY RECOMMENDATIONS FOR NON-MOBILE APPS AND APP STORES 2 (2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1123167/Non-Mobile_Apps_Literature_Review_UCL.pdf [https://perma.cc/K7ZH-YLGT].

72. SAM Seamless Network, *New Research Exposes the Vulnerabilities of Smart Home Networks Through Security Cameras and Smart Hubs*, CISION PR NEWSWIRE (June 12, 2019, 2:00 PM), https://www.prnewswire.com/news-releases/new-research-exposes-the-vulnerabilities-of-smart-home-networks-through-security-cameras-and-smart-hubs-300866213.html [https://perma.cc/LE7E-S89S].

73. *Id.*

74. *Connected Homes Are Expanding, So Is Attack Volume*, HELP NET SEC. (Dec. 20, 2022), https://www.helpnetsecurity.com/2022/12/20/connected-homes-attack-volume/ [https://perma.cc/C739-FCAD].

75. *Smart Home Security Devices Most at Risk in IoT-Targeted Cyber Attacks*, HELP NET SEC. (June 13, 2019), https://www.helpnetsecurity.com/2019/06/13/iot-targeted-cyber-attacks/ [https://perma.cc/MU8J-TWFJ].

76. David Priest & Taylor Martin, *Practical Ways to Prevent Your Home Security Cameras from Being Hacked*, CNET (July 22, 2023), https://www.cnet.com/home/security/practical-ways-to-prevent-your-home-security-cameras-from-being-hacked/ [https://perma.cc/VXW5-C56M].

77. Ali, *supra* note 5.

78. *Id.*

is at risk."[79] In addition, third-party hardware used to make the appliances "smart" can itself contain defects, errors, or unsecure configurations that leave the device vulnerable.[80] For example, in 2016, a research team exposed "an SQL injection flaw in [the WeMo smartphone app] configuration mechanism that could allow attackers to write an arbitrary file on the device in a location of their choosing. The vulnerability can be exploited by tricking the device into parsing a maliciously crafted SQLite database."[81] Part III of the Article will explain the intersection between data security and product liability, focusing on smart home devices deployed with insufficient security.

B. Examples of Smart Home Vulnerabilities

Researchers have advised Amazon Alexa users to avoid putting the device in bathrooms and bedrooms because they may be at risk of having their private conversations recorded.[82] "Amazon can save anything you say to Alexa, and depending on your smart home devices, you could be sharing your Wi-Fi network with strangers without realizing it."[83] The Amazon Alexa, plugged in and connected to Wi-Fi, should be alert at all times to provide the user or consumer with the help required.[84] With that comes risk, as any information communicated to the Amazon Alexa is stored indefinitely on company servers.[85] In 2017, researchers revealed extensive security issues involving

79. Douglas McKee, *'Insight' into Home Automation Reveals Vulnerability in Simple IoT Product*, MCAFEE (Aug. 20, 2018), https://www.mcafee.com/blogs/other-blogs/mcafee-labs/insight-into-home-automation-reveals-vulnerability-in-simple-iot-product/ [https://perma.cc/J778-EQWW].

80. Lucian Constantin, *Update Your Belkin WeMo Devices Before They Become Botnet Zombies*, COMPUTERWORLD (Nov. 4, 2016), https://www.computerworld.com/article/3138991/security/update-your-belkin-wemo-devices-before-they-become-botnet-zombies.html [https:perma.cc/R38K-4JUG].

81. *Id.*

82. Aurora Bosotti, *Cyber Expert Pinpoints 'Disturbing' Reason Amazon Alexa Should Not Be Placed in Bedrooms*, EXPRESS (Jan. 2, 2023), https://www.express.co.uk/news/us/1716038/Amazon-Alexa-warning-bedroom-bathroom-recording-privacy-cyber-expert-dxus [https://perma.cc/FDY7-Y4KE].

83. Will Greenwald, *New Amazon Echo Device? 8 Alexa Settings to Change Immediately*, PCMAG (June 28, 2022), https://www.pcmag.com/how-to/amazon-alexa-app-settings-to-change-immediately [https://perma.cc/RZ5W-WM58].

84. *Set up Alexa in a Few Easy Steps*, AMAZON, https://www.amazon.com/alexa-setup-guide/b?ie=UTF8&node=17978645011 [https://perma.cc/62CQ-2AZC].

85. Nate Nelson, *Novel Attack Turns Amazon Devices Against Themselves*, THREAT POST (Mar. 7, 2022, 4:30 PM), https://threatpost.com/attack-amazon-devices-against-themselves/178797/ [https://perma.cc//G4W7-4DZ5]; *see* Ionut Arghire, *Amazon Alexa Vulnerabilities Could Have*

Wink's Hub 2.[86] Wink and Insteon failed to store "sensitive credentials securely on their associated Android apps."[87] Furthermore, "the Wink cloud-based management API does not properly expire and revoke authentication tokens, and the Insteon Hub uses an unencrypted radio transmission protocol for potentially sensitive security controls."[88]

Researchers tested a total of sixteen commonly used smart devices and determined that 80 percent of these networked devices were susceptible to attacks, enabled by fifty-four security defects.[89] Part III proposes extending product liability as a remedy for injuries and privacy invasions enabled by security vulnerabilities in smart home devices.

III. PRODUCT LIABILITY TO ADDRESS DEFECTS IN SMART HOME DEVICES

A. Extending Product Liability to Software in Smart Home Devices

Product liability currently applies where the consumer or business can establish that a defect proximately caused their injuries.[90] Any company that creates a product which "enters the stream of commerce owes a duty of reasonable care to design, manufacture, and/or warn regarding its product; the product is defective due to a breach of this duty; the manufacturer's breach of its duty is the proximate cause of plaintiff's injuries."[91] Plaintiffs in product liability actions will typically assert claims for negligence, strict liability, or breach of

---

Exposed User Data, SEC. WEEK (Aug. 14, 2020), https://www.securityweek.com/amazon-alexa-vulnerabilities-exposed-user-data/ [https://perma.cc/NN6R-WLVX].

> The attacks involved a Cross-Origin Resource Sharing (CORS) misconfiguration and Cross Site Scripting (XSS) bugs identified on Amazon and Alexa subdomains, which eventually allowed the researchers to perform various actions on behalf of legitimate users. Successful exploitation of these vulnerabilities could allow an attacker to retrieve the personal information of an Alexa user, as well as their voice history with their Alexa, but also to install applications (skills) on the user's behalf, list installed skills, or remove them.

Id.

86. Sam Huckins, *Multiple Vulnerabilities in Wink and Insteon Smart Home Systems*, RAPID7 (May 10, 2019), https://www.rapid7.com/blog/post/2017/09/22/multiple-vulnerabilities-in-wink-and-insteon-smart-home-systems [https://perma.cc/2NQJ-6QEE].

87. *Id.*

88. *Id.*

89. Ali, *supra* note 5.

90. Williams v. Bob Barker Co., No. 2:21-cv-00436, 2023 U.S. Dist. LEXIS 1116, at *8 (S.D. W. Va. Jan. 4, 2023).

91. *Id.*

warranty, depending on the jurisdiction.[92] To prevail in a smart home product liability action, the plaintiff must demonstrate that:

> (1) the defendant was engaged in the business of . . . selling the product; (2) the product was in a defective condition unreasonably dangerous to the consumer or user; (3) the defect caused the injury for which compensation [is] sought; (4) the defect existed at the time of sale; and (5) the product was expected to and did reach the consumer without substantial change in condition.[93]

In 2022, the European Commission's proposal to update its Product Liability Directive expanded damages to include data loss.[94] In particular, in the context of a data breach, the U.S. Court of Appeals for the Ninth Circuit has "found that an individual's loss of control over the use of their identity due to a data breach and the accompanying impairment in value of PII constitutes non-economic harms."[95] The American Law Institute Reporters of the *Restatement (Third) of Torts* categorizes three paradigmatic product defects: (1) manufacturing defects; (2) design defects; and (3) warnings/instruction defects.[96]

B. Conceptualizing Product Defects in Smart Home Devices

1. Manufacturing Defects

A smart home device "contains a manufacturing defect when [it] departs from its intended design."[97] A manufacturing defect contrasts from a design defect in that the former occurs in only a small percentage of units in a product line.[98] A smart home manufacturer's failure

92. *Types of Defective Products Liability Claims*, HG, https://www.hg.org/legal-articles/types-of-defective-product-liability-claims-42070 [https://perma.cc/F63V-RJMQ].

93. Khybery v. Weber-Stephen Prods. LLC, No. HHB-CV20-6061498-S, 2022 Conn. Super. LEXIS 2699, at *3 (Conn. Super. Ct. Dec. 16, 2022) (citing Giglio v. Connecticut Light & Power Co., 429 A.2d 486, 488 (1980)).

94. Press Release, *supra* note 14.

95. Smallman v. MGM Resorts Int'l, No. 2:20-cv-00376-GMN-EJY, 2022 U.S. Dist. LEXIS 199399, at *11 (D. Nev. Nov. 2, 2022); *see* Flores-Mendez v. Zoosk, Inc., No. C 20-04929 WHA, 2021 WL 308543, at *3 (N.D. Cal. Jan. 30, 2021).

96. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2 (AM. L. INST. 1998); *see also Chapter Two | Types of Defect*, SHANNONWEB, https://www.shannonweb.net/pl/chapter-two-types-of-defect/ [https://perma.cc/RD3P-K47Y] (hereinafter *Chapter Two | Types of Defect*).

97. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2.

98. *Chapter Two | Types of Defect*, *supra* note 96.

to comply with its own design specifications regarding assembly of device is an example of a manufacturing defect.[99]

Section 2 of the *Restatement (Third)* treats manufacturing defects in a different way from design and warning/instruction defects.[100] For manufacturing defect cases, the *Restatement* applies a "departure from design" standard, while using a "risk-utility balancing test" for warning/instruction defect cases.[101] A manufacturing defect for smart home devices occurs "when the product departs from its intended design even though all possible care was exercised in the preparation and marketing of the product."[102]

Manufacturing defects will rarely be found in smart home devices, as it is improbable that a single smart device will be programmed incorrectly. Nevertheless, if smart devices are customized, it is possible that a single unit would not be programmed correctly, providing a direct analogy to a manufacturing defect.[103] It is predicted that manufacturing defect cases will not occur frequently in smart home product liability litigation.[104]

2. Design Defects

The overwhelming number of defective smart home device cases will be tried under a design defect cause of action.[105] One study sought to "raise awareness about the widespread vulnerabilities found in the

99. *See* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2 (conceptualizing defect under strict liability when a manufactured product deviates from its intended design); *cf.* Isham v. PADI Worldwide Corp., Nos. 06-00382, 06-00386, 2007 U.S. Dist. LEXIS 62419, at *18–21 (D. Haw. Aug. 23, 2007).

100. Douglas E. Schmidt et al., *A Critical Analysis of the Proposed Restatement (Third) of Torts: Product Liability*, 21 WM. MITCHELL L. REV. 411, 413 (1995).

101. *Id.*

102. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2.

103. *See* Katheryn A. Andresen et al., *Recent IoT Class Actions Highlight Need for Manufacturers & Vendors of Connected Products to Be Aware of Liability Risks*, NILAN JOHNSON LEWIS (Jan. 28, 2020), https://nilanjohnson.com/recent-iot-class-actions-highlight-need-for-manufacturers-vendors-of-connected-products-to-be-aware-of-liability-risks/ [https://perma.cc/H2JG-XZ4R].

104. J Royce Fichtner & Troy J. Strader, *Will Products Liability Litigation Help Protect IoT Users from Cyber-Physical Attacks?*, 31 J. INT'L TECH. & INFO. MGMT. 79, 89 (2022).

105. *Id.* ("Products liability claims against IoT device manufacturers will most likely center on allegations that insufficient cybersecurity constitutes a defective design."); *see also* Ali, *supra* note 5.

> The IoT vendors fail to provide the required special-purpose security solutions. Further, smart home devices often run small operating systems such as INTEGRITY, Contiki, FreeRTOS, and VxWorks, whose security solutions are not as robust as those of Windows or Linux-based systems. Most commonly available devices, once deployed, cannot be upgraded to update the security capability against the evolving cyber-attacks.

Id.

most common smart gadgets in the US home," in which researchers investigated twenty-four connected devices.[106] Researchers detected critical design flaws that increase attack likelihood in twenty-two out of the twenty-four smart devices.[107] Among the connected devices studied include "security cameras, motion sensors, smart home environmental monitoring [devices], connected doorbells, garage door openers and smart locks."[108]

Damages or losses due to software programming errors in smart devices are often more difficult to determine and quantify.[109] When a smart home appliance has been compromised, "companies may find it more difficult to demonstrate real dollar counts for damage that is often intangible—in the form of lost files, downtime, and reduced client trust."[110]

As established in Part II, security vulnerabilities were overwhelmingly the greatest defect in devices produced by the nine leading smart home providers.[111] "The connections between billions of networked smart devices and the associated data transfer poses a myriad of liability questions. These questions may be compounded by the fact that many smart devices lack rigorous security protocols, turning them into 'weak points' susceptible to manipulation by hackers."[112] Unlike the products regulated by traditional product liability, connected smart devices incorporate software, which is an intangible set of

106. Luana Pascu, *Critical Design Flaws Found in Popular Smart Devices Sold Across the U.S.*, BITDEFENDER (May 08, 2019), https://www.bitdefender.com/blog/hotforsecurity/critical-design-flaws-found-popular-smart-devices-sold-across-us/ [https://perma.cc/U67W-2F5U].

107. *Id.*

108. *Id.*

109. *See* Shannon Flynn, *Product Liability in IoT: Who Is Responsible for Vulnerabilities?*, IOT MAG. (Aug. 24, 2021), https://theiotmagazine.com/product-liability-in-iot-who-is-responsible-for-vulnerabilities-847256b8eb96 [https://perma.cc/TAY9-3DFZ].

110. *Id.*

111. *See Flaws in the Design of IoT Devices Prevent Them from Notifying Homeowners About Problems*, HELP NET SEC. (May 7, 2019), https://www.helpnetsecurity.com/2019/05/07/iot-design-flaws-identified/ [https://perma.cc/P3QM-LVH5]; Jamie Leventhal, *Security Flaws Found in Popular Smart Home Devices*, PBS (Nov. 6, 2019, 12:32 PM), https://www.pbs.org/newshour/science/security-flaws-found-in-popular-smart-home-devices [https://perma.cc/2EMV-PPPT]; *see also* Ali, *supra* note 5 ("A 2021 research project revealed that typical smart homes are vulnerable to a high number of data attacks. Reported instances of smart home attacks have included hackers remotely controlling smart lights and smart TVs, unlocking IoT-enabled doors, and remotely turning on and streaming video from smart cameras.").

112. Dani Alexis Ryskamp, *Expert Witnesses and The Internet of Things: Assessing Product Liability in Smart Devices*, EXPERT INST. FOR ATT'YS (June 23, 2020), https://www.expertinstitute.com/resources/insights/expert-witnesses-and-the-internet-of-things-assessing-product-liability-in-smart-devices/ [https://perma.cc/SN5Q-KPEW].

instructions.[113] The next section applies the two foremost design defect theories to smart home devices that incorporate software that fails.

C. Tests for Design Defect

Security weaknesses create even greater hazards due to smart devices' connectivity and interoperability.[114] The multifaceted nature of smart devices does not change the manufacturer's duty to the consumer, user, or business to reasonably design its digital products. Courts are likely to apply either a consumer expectation test or a risk/utility test to determine if a given smart device is defectively designed.[115]

On the one hand, the consumer expectation test examines whether "a product's design is defective if it has failed to perform as safely as its ordinary consumers would expect when used in an intended or reasonably foreseeable manner."[116] On the other hand, the risk/utility test evaluates whether "the design embodies 'excessive preventable danger,' that is, the risk of danger inherent in the design outweighs the benefits of such design."[117]

---

113. S. Cent. Bell Tel. Co. v. Barthelemy, 643 So. 2d 1240, 1246 (La. 1994).

> In its broadest scope, software encompasses all parts of the computer system other than the hardware . . . . In its narrowest scope, software is synonymous with program, which, in turn, is defined as "a complete set of instructions that tells a computer how to do something." Thus, another definition of software is "a set of instructions" or "a body of information."
>
> When stored on magnetic tape, disc, or computer chip, this software, or set of instructions, is physically manifested in machine readable form by arranging electrons, by use of an electric current, to create either a magnetized or unmagnetized space. The computer reads the pattern of magnetized and unmagnetized spaces with a read/write head as "on" and "off", or to put it another way, "0" and "1". This machine readable language or code is the physical manifestation of the information in binary form.

Id. (citations omitted).

114. *See* Nicholas Sutrich, *Is This the Beginning of the Demise of Smart Home Security Cameras?*, ANDROID CENT. (Jan. 13, 2023), https://www.androidcentral.com/accessories/smart-home/is-this-the-beginning-of-the-demise-of-smart-home-security-cameras [https://perma.cc/LWP5-9C9Y].

115. *See* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2 (AM. L. INST. 1998).

116. Torres v. City of Madera, No. CIV F F 02-6385 AWI LJO, 2005 U.S. Dist. LEXIS 34672, at *21–22 (E.D. Cal. July 11, 2005).

117. *Id.*; *see* 1 COMPUTER CONTRACTS § 1.02 (2023) (highlighting the consumer expectation test and risk-utility test as applied in autonomous vehicle product liability). *But see* Emily Frascaroli et al., *Let's Be Reasonable: The Consumer Expectations Test Is Simply Not Viable to Determine Design Defect for Complex Autonomous Vehicle Technology*, 2019 J.L. & MOBILITY 53, 60 (2019).

> [A] product is defective in design either (1) if the product has failed to perform as safely as an ordinary consumer would expect when used in an intended or reasonably

1. Consumer Expectation Test

In proving a design defect, a plaintiff may deploy the consumer expectation test "by demonstrating that 'the product failed to perform as safely as an ordinary consumer would expect when used in an intended or reasonably foreseeable manner.'"[118] This test assumes that the manufacturer establishes consumers' expectations for a particular product in the form of advertising and other pitches determining purchasing decisions. Under the "consumer expectation" test, a plaintiff must demonstrate the following by a preponderance of the evidence:

> (1) [t]he defendant's connection with the product, such as manufacturer, distributor, or seller; (2) that the design of the product that injured the plaintiff was the same as the design of the product when it left the defendant's possession; (3) that the product failed to perform as safely as an ordinary consumer of that product would have expected; (4) that the design of the product was a proximate cause of the plaintiff's injuries; (5) that the product was used in a manner reasonably foreseeable by the defendant; and (6) the nature and extent of the plaintiff's injuries.[119]

Most smart medical products are so complex that it is legal fiction to assume that consumers have any meaningful consumer expectation, let alone an understanding of how these devices work.[120] To apply this

---

> foreseeable manner, or (2) if, in light of the relevant factors . . . the benefits of the challenged design do not outweigh the risk of danger inherent in the design.

Id. (citing Barker v. Lull Eng'g Co., 573 P.2d 443, 446 (Cal. 1978)).

118. Cruz v. Mathenge, No. B286067, 2019 Cal. App. Unpub. LEXIS 1332, at *36 (Cal. Ct. App. Feb. 26, 2019) (citing *Barker*, 573 P.2d 443).

119. *Id.*

120. *See* Eric Alexander, *Design Claims Fall Under Consumer Expectations Test with an Adequate Warning*, DRUG & DEVICE L. (Jan. 15, 2021), https://www.druganddevicelawblog.com/2021/01/design-claims-fail-under-consumer-expectations-test-with-an-adequate-warning.html [https://perma.cc/VVR5-LCMA].

> A variety of smart devices are available on the market, including deep brain neurostimulators, cochlear implants, defibrillators and pacemakers. There are also numerous health gadgets, apps and wearable technology, designed to monitor vital signs and help us self-manage our chronic conditions. Innovative products still in development include wireless powered wearable smart contact lenses made of biocompatible polymers, which diagnose and treat diabetic retinopathy via automated drug delivery and electrical stimulations.

Karishma Paroha, *Liability Risks Arising from Smart Medical Technology Are Growing*, KENNEDYS (Oct. 28, 2020), https://kennedyslaw.com/thought-leadership/article/liability-risks-arising-from-smart-medical-technology-are-growing/ [https://perma.cc/82MQ-RZ2J].

test for defective design, courts will need to determine what expectations a reasonable consumer would have of a smart home appliance or device.[121] Unless a consumer was a computer programmer, he or she is improbable to have any understanding about the software incorporated in smart products. It is therefore necessary to have expert testimony about consumers' expectations regarding smart home devices.[122]

Due to the complexity of smart home devices, it is unclear how a court will determine what expectations consumers will or should have. Assuming a consumer expectation can be determined, courts will require the smart device to be used in a foreseeable manner.[123] Another issue is whether the consumer expectation test needs to be tailored for the software incorporated in smart devices.

2. Risk/Utility Test for Smart Home Devices

A court applying the risk/utility test will determine whether the manufacturer, distributor, or seller of a smart home device designed it to function under conditions foreseeable for its environment of use.[124] Under such a test, a product's design is defective if the costs of avoiding a particular hazard are foreseeably less than the resulting safety benefits. The risk/utility test is a cost-benefit test that will be more straightforward as a test for defective design versus the traditional consumer expectation test.[125] Courts have espoused the risk/utility test, which weighs the product's risks against its benefits without requiring a showing of an alternative reasonable design. If the product's utility, as designed, outweighs its risks, it is not defective.[126]

---

121. *See* William Judge, Jr. & Nicole D. Walsh, *Medical Device Warnings for Home Use Devices*, MEDMARC (May 7, 2021, 2:00 PM), https://www.medmarc.com/globalassets/news-and-resources/webinars/slides/21-05-medical-device-warnings-home-use-devices.pdf [https://perma.cc/7VVB-57VM].

122. Ryskamp, *supra* note 112.

123. Brent Steinberg, *Autonomous Vehicles*, 1 FLORIDA AUTOMOBILE INSURANCE LAW § 9.2(F)(6)(c) (2022) (highlighting Florida's adoption of the consumer expectation test for product liability claims); *see* Paroha, *supra* note 120.

124. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2, cmt. f (AM. L. INST. 1998) ("To establish a prima facie case of defect, the plaintiff must prove the availability of a technologically feasible and practical alternative design that would have reduced or prevented the plaintiff's harm.").

125. Charlie Wilson et al., *Benefits and Risks of Smart Home Technologies*, 103 ENERGY POL'Y 72, 79 (Apr. 2017). *But see* Robert S. Peck, *The Coming Connected-Products Liability Revolution*, 73 HASTINGS L.J. 1305, 1314 (2022).

126. *See* Ruwantissa Abeyratne, *The Deepwater Horizon Disaster—Some Liability Issues*, 35 TUL. MAR. L.J. 125, 134 (2010) (distinguishing the risk-utility test adopted by several jurisdictions from the reasonable standards test, which considers the adoption of a reasonable alternative design).

3. Risk/Utility with Reasonable Alternative Design Adapted to Smart Home Devices

The *Restatement (Third) of Torts: Products Liability* defines a "design defect" as one that occurs when the foreseeable risks of harm posed by a (smart home) product could have been reduced or avoided by the adoption of a "reasonable alternative design."[127] The requirement of proposing a reasonable alternative design for a defective smart device will be a difficult burden to satisfy for most injured plaintiffs.[128] Plaintiffs must impeach the designs of complex smart home devices that injured them or infringed their privacy, or have their claims dismissed.[129]

In a smart home design defect action, the plaintiff must prove that a design flaw had greater risks than utilities and explain how a specific alternative design would have prevented the smart home device from being unreasonably dangerous. A reasonable alternative design is measured by balancing the overall cost of the design against the "magnitude of the hazard and risk of personal injury, death, and property damage."[130]

The *Restatement (Third)* definition of design defect displaces the *Restatement (Second)* section 402A "consumer expectation" test and the court's "risk/utility test."[131] Section 2 of the *Restatement (Third)*

---

127. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2; *see also* James Beck, *On Alternative Design, Take Two—Negligence*, DRUG & DEVICE L. (Feb. 27, 2017) https://www.druganddevicelawblog.com/2017/02/on-alternative-design-take-two-%E2%88%92-negligence.html [https://perma.cc/7DDR-Z2Y5].

128. *See* Peck, *supra* note 125, at 1322.

> [A] risk-utility approach that incorporates a reasonable alternative design requirement sets too heavy a burden because it requires a plaintiff to both determine the design flaw that caused the collision and develop a safer design that would have worked better. An individual or a business, injured by an AV, even employing an expert, lacks the means by which to accomplish what an automotive company's research and development department evidently could not. Thus, giving way to what might be realistic, the alternative reasonable-design approach cannot work without effectively immunizing the manufacturer, regardless of what corners it may have cut.

Id.

129. *See* Adrian Booth et al., *The Digital Utility: New Opportunities and Challenges*, MCKINSEY & CO. (May 12, 2016), https://www.mckinsey.com/industries/electric-power-and-natural-gas/our-insights/the-digital-utility-new-opportunities-and-challenges [https://perma.cc/ST62-S9EB].

130. Ruddy v. Polaris Indus., No. 3:17-CV-0423, 2022 U.S. Dist. LEXIS 38182, at *40 (M.D. Pa. Mar. 3, 2022). (weighing these factors in determining the reasonableness of an alternative design for a personal watercraft).

131. *Id.* (explaining that a product is defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative

requires plaintiffs to present a reasonable alternative design while demonstrating that there are excessive preventable risks in the smart home product.[132]

4. Failure to Warn or Inadequate Warning for Vulnerabilities in Smart Home Devices

To properly assert a failure to warn claim, a plaintiff must establish that the seller not only knew the smart home product was dangerous, but that a warning could be effectively communicated to consumers how to avoid the peril.[133] A smart home product is defectively designed if "the foreseeable risks of harm posed by the product could have been reduced or avoided by the provision of reasonable instructions or warnings by the seller."[134] A smart home device user may also assert a failure to warn claim if a connected device poses "a risk of injury when used in a reasonably foreseeable manner but is marketed without adequate warnings of that risk."[135]

"A manufacturer must anticipate foreseeable misuse and also consider the particular hazard. When a product presents a serious risk of harm, the manufacturer must warn in a manner likely to catch the user's attention."[136] Smart home device makers are always in the best position to gather data about foreseeable uses and misuses of smart home devices and are therefore the "least-cost avoider" able to take steps to avoid or preclude dangers or risks.[137] Where smart home device manufacturers are not able to redesign around problems, they have a duty to warn consumers about known vulnerabilities.[138]

---

design by the seller or other distributor, or a predecessor in the commercial chain of distribution, and that the omission of the alternative design renders the product not reasonably safe).

132. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2 (requiring the plaintiff to prove a reasonable alternative design as an absolute requirement for liability).

133. Amy L. Stein, *Assuming the Risks of Artificial Intelligence*, 102 B.U. L. REV. 979, 1030–31 (2022).

134. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2.

135. Whaley v. Alaska, No. 4:21-CV-00006-JMK, 2023 U.S. Dist. LEXIS 2979, at *7 (D. Alaska Jan. 6, 2023).

136. Easton v. Chevron Indus., Inc., 602 So. 2d 1032, 1037 ((La. Ct. App. 1992).

137. Nat'l Union Fire Ins. Co. v. Riggs Nat'l Bank, 5 F.3d 554, 557 (D.C. Cir. 1993) (Silberman, J., concurring) ("[A]s between two faultless parties, liability should rest with the one who is best positioned to avoid the loss.").

138. *See* Erin B. Bosman & Julie Y. Park, *Connected Devices Bring New Product Liability Challenges*, MORRISON FOERSTER (Jan. 18, 2018), https://www.sociallyawareblog.com/topics/connected-devices-bring-new-product-liability-challenges_01 [https://perma.cc/R6F7-K9QQ]; Aaron C. Garavaglia, *Smart Homes and Liabilities: A Brave New World*, NAT. L. REV. (Jan. 6, 2021), https://www.natlawreview.com/article/smart-homes-and-liabilities-brave-new-world [https://perma.cc/6389-94BH].

5. Malfunction Theory as a Substitute for a Defect

Plaintiffs in smart home device cases will often find it difficult to identify the defect responsible for a smart home device's failure or malfunction. In some jurisdictions, a plaintiff may establish a prima facie product liability case "even in the absence of proof of a specific defect, by resort to what has been called, variously, the malfunction or general defect theory."[139] For example, in Idaho, plaintiffs can use circumstantial evidence to prove a product defect under the state's "malfunction theory."[140]

The plaintiff's burden of proof would require evidence that: (1) the product malfunctioned; (2) the malfunction occurred during proper use; and (3) the product had not been altered or misused in a manner that probably caused the malfunction to prevail.[141] Plaintiffs in smart home device cases would similarly benefit from using circumstantial evidence of a malfunctioning device, where they could not pinpoint a design defect.[142] In jurisdictions adopting the *Restatement (Third)*, plaintiffs will have an insurmountable burden proving an alternative design or algorithm that would have avoided the peril in a product liability action.

D. Strict Product Liability Extended to Smart Home Devices

Consumers harmed or injured by smart home devices can serve as early responders uncovering smoking gun evidence of a smart device manufacturer's failure to create connected products safe for the foreseeable environment of use.[143] Product liability incentivizes software programmers, designers, and manufacturers to review the safety of their smart home products before releasing them into the

139. 1 LOUIS R. FRUMER ET AL., PRODUCTS LIABILITY § 8.06 (2023); *see, e.g.*, Campbell Soup Co. v. Gates, 889 S.W.2d 750, 753 (Ark. 1994); Mays v. Ciba-Geigy Corp., 661 P.2d 348, 357–58 (Kan. 1983); Rogers v. Johnson & Johnson Prods., Inc., 565 A.2d 751, 754 (Pa. 1989); Sims v. Gen. Motors Corp., 751 P.2d 357, 364 (Wyo. 1988); Siegel v. Mazda Motor Corp., 835 F.2d 1475, 1479 (D.C. Cir. 1987).

140. *See* Andrew Tauber, *Neither the 'Malfunction Theory' nor the Res Ipsa Loquitur Doctrine Excuses a Plaintiff's Failure to Offer Evidence of a Defect*, DRUG & DEVICE L. (June 17, 2021), https://www.druganddevicelawblog.com/2021/06/neither-the-malfunction-theory-nor-the-res-ipsa-loquitur-doctrine-excuses-a-plaintiffs-failure-to-offer-evidence-of-a-defect.html [https://perma.cc/5PWV-UPM7].

141. Black v. DJO Glob., Inc., 488 P.3d 1283, 1287 (Idaho 2021).

142. *See* Sharon M. Peart, *The Malfunction Theory: A Feasible Means to Prove a Defect in Strict Product Liability*, 94 DICK. L. REV. 733, 742 (1990).

143. *See* Adam Green, *'Smart Home' Revolution Tests Legal Liability Regimes*, FIN. TIMES (Nov. 24, 2020), https://www.ft.com/content/e3fc8a83-8bee-4897-b12e-59ed2539b4d2 [https://perma.cc/RA7U-W2U3].

marketplace. Microsoft, for example, has fashioned a new tool for fixing software code bugs called Jigsaw.[144] Nevertheless, security is not a priority for most digital device manufacturers. In fact, a recent empirical study demonstrated that product liability claims relating to IoT devices are extremely rare, "reveal[ing] only two cases where courts have issued decisions pertaining to products liability causes of action and [IoT] cyber-physical device security."[145]

Imposing product liability for defective software will make smart device manufacturers think twice before placing a device or appliance on the market that is ineffectively tested or released with a known cybersecurity defect.[146] The damages in a smart home device products case will be those causally connected to the defectively designed software, which will often include damages for compromised data or the invasion of privacy. Traditional product liability, in contrast, will often involve personal injury or the loss of life.[147]

"A prima facie case of strict product liability requires plaintiff to establish that: (1) the product was placed on the market; (2) there was knowledge that it would be used without inspection for defect; (3) the product proves to be defective; and (4) the defect causes injury to a human."[148] In order for product liability to be extended to smart home devices, the definition of injury would need to be broadened from physical injury to include invasions of privacy, data breaches, or other information-based injuries.

Software defects incorporated into smart home devices may also cause personal injury or death as in conventional product liability

144. Liam Tung, *Sorry, Developers: Microsoft's New Tool Fixes the Bugs in Software Code Written by AI*, ZDNET (Apr. 11, 2022), https://www.zdnet.com/article/sorry-developers-microsofts-new-tool-fixes-the-bugs-in-software-code-written-by-ai/ [https://perma.cc/26YC-RSZZ].

145. J. Royce Fichtner & Troy J. Strader, *Will Products Liability Litigation Help Protect IoT Users from Cyber-Physical Attacks?*, 31 J. INT'L TECH. & INFO. MGMT. 79, 86 (2022).

146. Chen & Urquhart, *supra* note 66, at 100.

> Concurrently, the sheer increased number of connected devices raises concerns about the heightened cybersecurity risks. Vulnerable smart devices without security provisions may become targets of cyberattacks, which pose threats not just to the end-user's security and privacy, but also to the operation of the infrastructural network. There is a concern around the scale of cybersecurity attacks.

Id.

147. *See generally* David Joz, *Latest Smart Home Security Problems and How to Fix Them*, MAKE TECH EASIER (Mar. 16, 2020), https://www.maketecheasier.com/smart-home/latest-smart-home-security-problems-fixes/ [https://perma.cc/QF8K-97T6] (stating that vulnerabilities in smart home devices tend to result in data theft or the invasion of privacy).

148. Rodriguez v. City of Pasadena, No. 20STCV15807, 2022 Cal. Super. LEXIS 68880, at *5 (Cal. Super. Ct. Oct. 25, 2022) (citing Greenman v. Yuba Power Prods., Inc., 59 Cal. 2d 57, 62 (1963)).

litigation, however. "For example, if a smart thermostat in a water heater is programmed to turn off at a certain temperature but a software failure prevents it from activating, water temperature levels could become dangerously hot and consumers could be burned."[149] Product liability in a defective smart home appliance case would be based upon claims that a software manufacturing defect, design defect, or failure to warn of a known danger caused a user or consumer's personal injury, death, or property damage.

Smart home product liability imposes liability on the least cost avoider, which will almost always be a software industry defendant. One court observed that "the policies that underpin product liability (strict liability and even negligence) operate to establish liability on the distributor or seller who places a defective product into the stream of commerce."[150] The principal benefit of asserting strict product liability for plaintiffs in smart home product litigation is that they are not required to prove that the seller was at fault, but only that it sold or marketed a defective connected device causing injuries or death to a consumer.[151]

1. Resolving Legal Lag

Legal lag is the failure of courts and legislatures to update cases and statutes to address the unique demands of rapidly evolving technologies.[152] The failure of courts and legislatures to address defective software, licensing, and information technologies such as "edge computing" is a recent example of legal lag.[153] As software is increasingly deployed in smart home appliances, product liability regimes must also be updated to compensate consumers when software inevitably fails.

149. Andresen et al., *supra* note 103.

150. Palm v. Taurus Int'l Mfg., Inc., No. 3:22-CV-337 DRL-MGG, 2022 U.S. Dist. LEXIS 225898, at *7 (N.D. Ind. Dec. 15, 2022).

151. *See* H. Michael O'Brien, *The Impact of the Smart Home Revolution on the Product Liability and Fire Cause Determinations*, WILSON ELSER (Sept. 12, 2016), www.wilsonelser.com/writable/files/Client_Alerts/product_liability_fire_science_.pdf [https://perma.cc/6E3U-5PT6].

152. Michael L. Rustad & Thomas H. Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDISC. L.J. 77, 77–78 (2003). In 1936, Richard Nixon reflected on the fact that within one generation, automobile liability law became so developed that the size of a comprehensive review grew from a few-page document to an entire encyclopedia. *Id.* at 77.

153. Ezra Dodd Church, *Technological Conservatism: How Information Technology Prevents the Law from Changing*, 83 TEX. L. REV. 561, 581–86 (2004) (explaining how software code and nature of information technologies creates legal lag).

Several recent lawsuits against Amazon relate to its Ring security devices. The first case against Amazon arose out of Alabama, where it was alleged that children were playing basketball at home when a hacker spoke to them through the Ring camera, commenting on their basketball skills and asking them to get closer to the camera.[154]

The children's father alleged common law negligence and invasion of privacy and sought monetary damages.[155] The second case was a class action suit arising out of Mississippi and Texas, where plaintiffs alleged that the security devices and systems were defective due to vulnerabilities enabling hackers to spy on and harass consumers in their homes.[156]

While the plaintiffs in the Mississippi case alleged negligence, breach of contract, intrusion upon seclusion, and public disclosure of private facts, they are unlikely to succeed unless they make a showing of specific harm related to the alleged breach.[157] One federal court stated that the guiding principle of strict liability is that "those entities within a product's distributive chain 'who profit from the sale or distribution of the product to the public, rather than an innocent person injured by it, should bear the financial burden of even an undetectable product defect.'"[158]

Neither courts nor legislatures have addressed the issue of who should be liable when smart devices fail, subsequently causing foreseeable privacy and security issues.[159] As of March 6, 2024, no state or federal court or legislature has issued a single opinion or regulation addressing the liability issues for smart home products such as smart lights, thermostats and other software-driven home products.[160] Tort

---

154. Andresen et al, *supra* note 103.

155. *Id.*

156. *Id.*

157. *Id.*

158. Friedland Fam. Enters. v. Amoroso, 630 So. 2d 1067, 1068 (Fla. 1994) (internal brackets omitted) (quoting N. Mia. Gen. Hosp., Inc. v. Goldberg, 520 So. 2d 650, 651 (Fla. Dist. Ct. App. 1988)).

159. *See* Flynn, *supra* note 109.

> As the market for internet of things devices grows, IoT liability is likely to become a critical issue for both end-users and developers. This could be especially true for end-users of industrial IoT products, who may face the potential for significant damages if an IoT device is compromised by hackers.

Id.

160. Our search of Lexis+ cases, statutes and legislation on January 16, 2023, uncovered no example of a U.S. court or statute addressing the product liability of smart devices. This is an example of legal lag signifying the need for U.S. courts and legislatures to update the law in a rapidly

law has a remarkable ability to evolve social problems in every historical era.[161] Now is the time for tort liability to extend to defective software incorporated in smart home appliances and devices. While cybersecurity has increasingly been emphasized in software product liability litigation, we ought to adopt liability rules to the rapidly evolving smart home industry.[162]

2. Extending European-Style Product Liability to Smart Home Devices

Currently, smart home device manufacturers have the equivalent of a "no liability" zone because of their creative use of warranty disclaimers, caps on damages, and other one-sided contractual provisions.[163] The European Union has adopted a product liability regime that invalidates all of these liability limitations.[164] Across the European Union, case law requires product licenses to have "mandatory terms protecting consumers."[165]

U.S. consumer licensing provisions are unenforceable in Europe because "European courts will strictly scrutinize adhesive license agreements where the dominant party [has] the upper hand" and will

---

evolving smart goods economy. In every historic era, courts and legislatures lag behind technological advances. Rustad & Koenig, *supra* note 152 (recounting Richard Nixon's 1936 observation that in one generation the scope of automotive liability law had expanded from a few pages to an entire encyclopedia); *see* Michael L. Rustad & Maria Vittoria Onufrio, *The Exportability of the Principles of Software: Lost in Translation?*, 2 HASTINGS SCI. & TECH. L.J. 25, 29 (2010). "In the case of software law, there has been a forty-year 'legal lag' between the rises of software as a separate industry and the development of specialized contracting principles." *Id.*

161. Michael L. Rustad, *Torts as Public Wrongs*, 38 PEPP. L. REV. 433, 461–62 (2011).

> The power of the law of torts lies in its ability to adapt to changing social conditions. In the eighteenth century, torts compensated individuals injured by their neighbors. In contrast, in the 1970s and 1980s, mass tort law litigation evolved to compensate the victims of occupational exposure to toxic substances. . . . The inherent flexibility of tort law allows it to mediate social inequities as they arise.

Id.

162. *See* Bob Seeman, *Improving Cybersecurity by Applying Consumer Protection Laws to Software*, NAT'L ASS'N ATT'YS GEN., https://www.naag.org/attorney-general-journal/improving-cybersecurity-by-applying-consumer-protection-laws-to-software/ [https://perma.cc/BHT2-BRW6] (highlighting cybersecurity consumer protection for software); John Koetsier, *Smart Home: Apple Is the Fastest-Growing Connected Device Company*, FORBES (Aug. 31, 2022, 12:00 PM), https://www.forbes.com/sites/johnkoetsier/2022/08/31/smart-home-apple-is-the-fastest-growing-connected-device-company/ [https://perma.cc/96V5-54ZJ]. "The average house in the U.S. now has 20.2 connected devices, according to a new report based on an analysis of 41 million homes and 1.8 billion connected devices," whereas the average European home contains only 17.4 such devices. *Id.*

163. *See* BAO KHAM CHAU ET AL., LIABILITY FOR HOME IOT 2 (2015).

164. *See* 1-12 SOFTWARE LICENSING § 12.12 (2016).

165. *Id.*

strike clauses that "clash with the most favorable mandatory national law" of consumer protection found in the twenty-seven European Union Member States.[166] Extending product liability to smart devices will align U.S. product liability law with the recent update to the European Union's Product Liability Directive.[167]

3. Shielding Smart Home Device Product Liability from Contractual Waivers

The most well-known smart home device manufacturers are creating a no liability zone through one-sided contract clauses that impose the provider's choice of forum and law, eradicate warranties, cap damages, and give theoretical legal rights without meaningful remedies.[168] The software industry's approach has been rushing to market and reallocating the costs of making their products to the consumer and other end users. U.S.-style consumer arbitration agreements, masquerading in the clothing of a contract, systematically strip consumers of any meaningful warranty or remedy. One MIT study concluded that due to the restrictive software licensing agreements of new IoT devices, meaningful liability is eliminated, effectively ending product liability in that market.[169]

---

166. *Id.*; *see also* Jo Best, *Google, Facebook, Twitter Face Lawsuit over 'Illegible, Incomprehensible' Privacy Policies*, ZDNET (Mar. 27, 2014), http://www.zdnet.com/google-facebook-twitter-face-lawsuit-over-illegible-incomprehensible-privacy-policies-7000027780/ [https://perma.cc/52U2-ZVHK] (discussing a lawsuit filed in the French High Court over Google, Facebook, and Twitter's refusal to change unlawful and unfair privacy policy language).

167. *See* EUR. COMM'N, PROPOSAL FOR A DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON LIABILITY FOR DEFECTIVE PRODUCTS (2022), https://single-market-economy.ec.europa.eu/system/files/2022-09/COM_2022_495_1_EN_ACT_part1_v6.pdf [https://perma.cc/9C2X-3KRS].

168. An MIT study confirms that leading smart device manufacturers use end user license agreements (EULAs) to eliminate their liability:

> For example, Nest, a smart appliances vendor, employs a restrictive EULA that disclaim all liabilities for its product's failures. . . . Similar to the EULAs of other IoT devices, Nest's license [is] non-negotiable.
>
> Disclaiming all liabilities has become a disturbing norm across all types of home IoT devices, from Samsung's Smart TV's, to Canary's "complete security system," to Ilumi's smartbulb, to Chillhub's open source refrigerator.

CHAU ET AL., *supra* note 163, at 10.

169. *Id.* at 4.

> Almost all of these devices have restrictive software license agreements that disclaim all liability. Under these agreements, if a malicious user compromise[s] one's Internet-connected oven to start a fire or hack[s] one's Internet-connected washing machine to ruin their clothes, the consumer would have no recourse for compensation. While manufacturers have some need to limit their product liabilities, the breadth and ubiquity of these

CONCLUSION

As smart products displace traditional products on a wider scale, it is necessary to extend product liability to connected devices. This Article proposes a tort reform extending product liability to vulnerabilities in smart home devices that cause consumers to have their personally identifiable data to be lost or otherwise compromised. Such an update of product liability will advance consumer safety while ensuring that all users and bystanders have the same protection when harmed by defective smart devices as by any other product.

Smart product users will have a remedy regardless of whether they were harmed by a defect in the software or the tangible component of the device. The indeterminacy as to liability standards for smart home device manufacturers raises compliance costs and threatens the future of the software industry. Smart device manufacturers, suppliers, distributors, or retailers should be liable if an appliance or device reaches the hands of a consumer and the software fails, causing personal injury, an invasion of privacy, or a data protection lapse. By explicitly updating product liability to include smart home devices, injured consumers will have a remedy against software makers that trade consumer safety for short-term profits.

---

disclaimers could effectively put an end to product liability as Internet-connected products replace their traditional counterparts.

Id.