THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XXI STLR.ORG FALL 2019

UNRAVELING HOME PROTECTION IN THE IOT AGE: SMART LIVING, MIXED REALITY, AND HOME 2.0

Bo Zhao*

Walls, windows, roofs, and fences cannot protect our home from virtual invasions and other non-physical intrusions. Neither can the current legal framework of home protection continue to safeguard the sanctity of home in a data-driven environment. Due to critical changes in household infrastructure and lifestyle, contemporary law has gradually become disconnected from the reality of the digital home, providing less protection than it did in the pre-digital age. This is partially because contemporary law has not properly addressed the complications, including a) the rise of digital and hybrid spaces and digital assets in the traditional physical home; b) the fast expansion of home (private) life into multiple spaces and places independent of geo-location; c) the lack of clear home boundaries in the digital world, as compared to boundaries previously marked by physical walls, fences, windows, etc.; d) the new power dynamics between home residents (now the data source) and devices and services providers (now increasingly in control of the home); e) the growing significance of home data protection in addition to physical privacy; f) the changing perception of home in the Internet of Things (IoT) age that is becoming more detached from home's geo-location and physical features; and g) weak enforcement jurisdiction in view of the

* Senior research fellow at Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University Law School, the Netherlands. The author would like to thank Prof. Bert-Jaap Koops (TILT), Prof. Pierce Robin (TILT), and Prof. Bryce Clayton Newell (School of Information Science, University of Kentucky) for their valuable comments and advice. Many thanks to Columbia Science and Technology Law Review Articles Editor Joshua Taylor for helping me through managing many minor, detailed issues and providing valuable suggestions, as well as Dr. Yang FENG (Zhejiang University Law School) for his encouragement and support. The research of this paper was only made possible by a grant from the Netherlands Organization for Sentience Research (NWO), project number 453-14-004.

complicated industrial supply chain, growing cross-border data flows, and untamed foreign tech powers.

This paper argues that contemporary law needs to develop a better conceptual framework to adjust to the fundamental changes as outlined. It argues that the inviolability of the home and home protection should cover not only the home's physical space, but also its virtual and hybrid space, helping residents regain their control of home. This can be achieved, the paper suggests, by adopting a new concept "Home 2.0," an upgrade of the traditional home ("Home 1.0"), and by re-emphasizing the physicality of the new home environment to better anchor the current home protection legal framework.

I. INTRODUCTION

In recent years, litigation against smart home products and service providers has been on the rise. On August 16, 2018, the U.S. Seventh Circuit Court ruled in *Naperville Smart Meter Awareness v. City of Naperville* that smart meter data was regulated by the Fourth Amendment, but that the Amendment did not protect the data in this case, warning that the outcome could be different had the data been collected more frequently or shared with law enforcement officials.

[1]Because smart meters collect data at high frequencies (every fifteen minutes) and such data can reveal intimate details inside the home unavailable to government without a physical search, the residents had a reasonable expectation of privacy in the data, and

1. Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527–29 (7th Cir. 2018).

the government's access to such data could be regarded as a search.[2] The court distinguished between smart meters and analog meters in household data collection and opined that the "ever-accelerating pace of technological development carries serious privacy implications," as illustrated by the smart meters in this case.[3] The court ruled that residents of Naperville had little choice to decide whether to adopt smart meters and that they did "not assume the risk of near constant monitoring by choosing to have electricity in [their] home[s]."[4] However, the court eventually found that the search was reasonable after balancing the intrusion on Fourth Amendment rights against the government interests in cost reduction, provision of cheaper power, encouragement of energy efficiency and improvement of grid stability.[5]

On Oct. 8 2018, the U.S. District Court for the District of New Jersey dismissed an eight-count class action against three smart TV makers (Samsung, LG and Sony), alleging that smart TVs continuously monitored and tracked consumers' viewing habits, recorded their voices, and transmitted this information to defendants' servers, after which the information was shared with third-party advertisers and content providers.[6] In the United States, an Amazon Echo smart speaker was able to provide crucial evidence in a double murder case, and Amazon was ordered to produce any recordings made by the speaker, as well as any information identifying cellular devices that had been paired with that speaker.[7] Police have already requested that Google-owned company Dropcam turn over footage from cameras inside people's homes, and Fitbit data has been used in court against defendants multiple times. [8] Further, as former Director of National Intelligence James

---

2. *Id.* at 526. In *Kyllo*, the U.S. Supreme Court held that the thermal scanning of a residential house by law enforcement constituted a search, as the technology was not routinely used by the public. Kyllo v. United States, 533 U.S. 27, 40 (2001).

3. *Naperville*, 900 F.3d at 527.

4. *Id.*

5. *Id.* at 528–29.

6. Jadzia Pierce, *New Jersey District Judge Dismisses All Counts Against Smart TVs*, INSIDE PRIVACY (Oct. 8, 2018), https://www.insideprivacy.com/data-privacy/new-jersey-district-judge-dismisses-all-counts-against-smart-tvs/.

7. Anthony Cuthbertson, *Amazon Ordered to Give Alexa Evidence in Double Murder Case*, INDEPENDENT (Nov. 14, 2018, 10:13 PM), https://www.independent.co.uk/life-style/gadgets-and-tech/news/amazon-echo-alexa-evidence-murder-case-a8633551.html. For similar cases, see also Kayla Epstein, *Police Think Amazon's Alexa May Have Information on a Fatal Stabbing Case*, WASH. POST (Nov. 8, 2019), https://www.washingtonpost.com/technology/2019/11/02/police-think-amazons-alexa-may-have-information-fatal-stabbing-case/.

8. Sean Adl-Tabatabai, *Government Admits They Will Use Smart Home Devices for Spying*, NEWS PUNCH (Feb. 10, 2016), https://newspunch.com/government-admits-they-will-use-smart-home-devices-for-spying/.

Clapper, revealed, U.S. intelligence agencies might use various smart home devices to monitor "targets and possibly the masses."[9]

In addition to these U.S. cases, new types of technology-related home intrusion are not uncommon in other parts of the world. These intrusions include police hacking of home computers,[10] manipulation of home webcams from a far distance,[11] child online harassment and stalking (ending with suicide),[12] misuse/abuse of sensitive data collected from sex toys used in the home,[13] smart refrigerators engaging in spam, and DDoS attacks.[14] Another growing significant concern comes from nonconsensual sharing of sensitive data collected from the home by smart devices and service providers with third parties for purposes unknown to home residents, such as targeted advertising, recruiting, or profiling for the housing market. What is perhaps more worrying is the proliferation of home surveillance (sensurveillance) in a 24/7 manner consequent to ubiquitous computing and the non-stop virtual presence of service and device providers in the IoT age. Home residents are essentially

---

9. Trevor Timm, *The Government Just Admitted It Will Use Smart Home Devices for Spying*, GUARDIAN (Feb. 9, 2016, 3:29 PM), https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government.

10. For acquiring digital evidence, some jurisdictions, including the Netherlands, have granted law enforcement agencies the power to hack home computers for criminal investigations of suspects or others with whom they are associated, although cross-border hacking is not allowed in general. *See* Janene Pieters, *New Law Allows Dutch Police to Hack Suspects*, NL TIMES (June 27, 2018, 4:10 PM), https://nltimes.nl/2018/06/27/new-law-allows-dutch-police-hack-suspects. For a discussion of police hacking laws in some representative jurisdictions, see Ivan Škorvánek et al., *"My Computer Is My Castle": New Privacy Frameworks to Regulate Police Hacking*, (Neth. Org. for Sci. Res., Working Paper No. 453–14–004, 2019), https://papers.ssrn.com/abstract=3348711.

11. Margi Murphy, *Woman Shocked After Pervert Hacker Took Control of Her Webcam and Asked Her to 'Suck my D***'*, SUN (Oct. 6, 2017, 10:35 AM), https://www.thesun.co.uk/tech/4624800/hamer-webcam-hacked-tells-woman-rude-words/.

12. Michelle Dean, *The Story of Amanda Todd*, NEW YORKER (Oct. 18, 2012), https://www.newyorker.com/culture/culture-desk/the-story-of-amanda-todd.

13. *See, e.g.*, Nicole Bogart, *Canadian Sex Toy Maker Settles $4M Lawsuit Claiming We-Vibe Tracked Private Data*, GLOBAL NEWS, (Mar. 14, 2017, 12:11 PM), https://globalnews.ca/news/3308543/we-vibe-privacy-lawsuit-settlement/.

14. Sarah Murray, *When Fridges Attack: Why Hackers Could Target the Grid*, FINANCIAL TIMES (Oct. 17, 2018), https://www.ft.com/content/2c17ff5e-4f02-11e8-ac41-759eee1efb74; *Fridge Sends Spam Emails*, BBC NEWS (Jan. 17, 2014), http://www.bbc.com/news/technology-25780908.

"gambling with their privacy"[15] when they invite smart technologies into their home, turning their home into a data factory.[16]

These are all non-physical intrusions and invasions that harm residents without physical penetration of the home, often without their knowledge. These incidents are the result of significant developments in the home environment, from the "third round" of electrification[17] to the more recent proliferation of various smart home and home automation technologies.[18] Characterized by *digitalization*, *connectedness, smartization,* and *automation* in the context of IoTs, our home and home life have been changed in fundamental ways: from physical space to hybrid space and mixed reality,[19] from a solely private space to half-public space, and from dwelling to smart living. A fundamental change is that the Home Virtual Space (HVS) has become the center and backbone of home life in terms of home organization, management, and maintenance,[20] with a considerable part of home life shifted into virtual space. This has created not only new functionalities and services, but also new household infrastructure. These changes lead to growing technical complexity, diminishing control by home residents, and numerous security vulnerabilities and privacy breaches, raising the question of how we may sufficiently protect the modern home in this fundamentally changed environment.

---

15. Feng Zhao, *Will Smart Home Tech Make Us Care More About Privacy?*, TECHCRUNCH (June 3, 2018, 9:30 AM), http://social.techcrunch.com/2018/06/03/will-smart-home-tech-make-us-care-more-about-privacy/.

16. Justin McGuirk, *Honeywell, I'm Home! The Internet of Things and the New Domestic Landscape*, E-FLUX J. (Apr. 2015), https://www.e-flux.com/journal/64/60855/honeywell-i-m-home-the-internet-of-things-and-the-new-domestic-landscape/.

17. The previous rounds of electrification were brought about by lighting, power and heating. *See* Inge Røpke et al., *Information and Communication Technologies – A New Round of Household Electrification*, 38 ENERGY POL'Y 1764 (2010).

18. In this paper, smart home is defined in the ICT context, although the concept can be dated back to 1930s America when electricity consumption came into the household. *See* Sarah J. Darby, *Smart Technology in the Home: Time for More Clarity*, 46 BUILDING RES. & INFO. 140, 142 (2018).

19. For simplicity and avoiding complicating further discussion, "place" in this Article refers to location in daily language, having a "concrete form," and maintaining a "relationship to humans and the human capacity to produce and consume meaning". TIM CRESSWELL, PLACE: AN INTRODUCTION 132–33 (2nd ed. 2014). "Space" is defined as "a backdrop against which human behavior is played out." PHIL HUBBARD ET AL., KEY THINKERS ON SPACE AND PLACE 4 (Phil Hubbard et al. eds., 1st ed. 2004). Place and space have always been connected together; as Cresswell explained, "[s]pace is a more abstract concept than place," and "[w]hen humans invest meaning in a portion of space and then become attached to it in some way . . . it becomes a place." CRESSWELL, *supra*, at 15–16.

20. The concept of Home Virtual Space (HVS) will be further defined in Section II (B).

Walls, windows, roofs, and fences cannot protect our home from virtual invasions and other non-physical intrusions;[21] neither can the current legal framework of home protection continue to safeguard the sanctity of the home in a data-driven environment. Due to critical changes in household infrastructure and lifestyle, contemporary law has become gradually disconnected from the reality of the digital home, providing *less protection* than it did in the pre-digital age. This is partially because current law has not properly addressed certain complications, including: a) the rise of digital and hybrid spaces and digital assets in the traditional physical home; b) the fast expansion of home (private) life into multiple spaces and places independent of geo-location; c) the lack of clear home boundaries in the digital world, as compared to boundaries previously marked by physical walls, fences, windows, etc.; d) the new power dynamics between home residents (now the data source) and devices and services providers (now increasingly in control of the home); e) the growing significance of home data protection in addition to physical privacy; f) the changing perception of home in the Internet of Things (IoT) age that is becoming more detached from home's geo-location and physical features; and g) weak enforcement jurisdiction in view of the complicated industrial supply chain, growing cross-border data flows, and untamed foreign tech powers.

This paper argues that contemporary law needs to develop a better conceptual framework to adjust to the fundamental home environmental changes as briefly outlined above. It argues that the inviolability of the home and home protection should cover not only the home's physical space, but also its virtual and hybrid space, helping residents regain their control of home. This can be achieved, the paper suggests, by adopting a new concept "Home 2.0," an upgrade of the traditional home ("Home 1.0"), and by re-emphasizing the physicality of the new home environment to better anchor the current home protection legal framework. It argues that, in contrast to other approaches, this new concept can best prevent the traditional concept of the home from becoming even more elusive, so that it will not lose legal relevance and significance as a legal proxy in protecting many home-associated critical values and interests, including privacy, autonomy, dignity, liberty, freedom of expression, solidarity, and peace.

This paper is structured as follows. Sections II will first briefly introduce the significance of the home and home protection in

---

21. For example, law enforcement agencies can make tech-enabled observations to collect information, using technologies such as thermal scanning or flying drones. For a discussion of observing the home from the outside in some jurisdictions, see Bert-Jaap Koops et al., *The Reasonableness of Remaining Unobserved: A Comparative Analysis of Visual Surveillance and Voyeurism in Criminal Law*, 43 L. & SOC. INQUIRY 1210 (2018).

contemporary law. Then it will discuss in detail the fundamental changes in the modern home environment and home life due to the proliferation of smart home and IoT technologies, which result in residents gradually losing control of the home. It further analyzes why contemporary law has not yet provided sufficient protection, causing, in fact, decreased privacy protection in the home in the context of growing non-physical intrusions. Section III will examine some key conceptual approaches to improve legal protection of the home to adjust to new digital realities, analyzing their pros and cons. Section IV further proposes that a new concept, "Home 2.0," can bridge the deepening regulatory gap between physicality and virtuality in the contemporary legal framework by re-emphasizing the physicality of modern home—in particular the meaningful connections between the Home Virtual Space (HVS) and home physical space—to best protect the home.

II. CHANGING HOME ENVIRONMENT AND DIMINISHING HOME PROTECTION

A. Sanctity of the Home and Home Protections

In western liberal society, our homes have been the center of private life and personal development. "The home is many people's greatest property asset and most private place."[22] Home is the primary source of what is known colloquially as "personal space." As Fox rightly analyzed, the significance of the home can be well explained in four value-types:

"Home as *a physical structure* offers material shelter; home as *a territory* offers security, control, a locus in space, permanence and continuity and privacy; home *as a centre for self-identity* offers a reflection of one's ideas and values, and acts as an indicator of personal status; and home as *a social and cultural unit* acts as the locus for relationships with family and friends, and as a centre of activities."[23]

Home has been recognized in the positive law as providing a kind of sanctuary or "moral nexus between liberty, privacy, and freedom of association."[24]Due to the central status of the home in private life, contemporary law has developed a sophisticated system

---

22. JOSHUA A. T. FAIRFIELD, OWNED: PROPERTY, PRIVACY, AND THE NEW DIGITAL SERFDOM 104 (2017). This Article follows Barros' approach to define home as "any type of permanent dwelling, whether rented or owned, and whether occupied by one person or by a family or group of any sort." D. Benjamin Barros, *Home as a Legal Concept*, 46 SANTA CLARA L. REV. 255, 258 (2006).

23. Lorna Fox, *The Meaning of Home: A Chimerical Concept or a Legal Challenge?*, 29 J.L. & SOC'Y 580, 590–91 (2002).

24. Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957, 991 (1982).

to protect the home's space and place as best characterized in the castle doctrine in common law countries.[25] The castle doctrine is "one of the oldest and most deeply rooted principles in Anglo-American jurisprudence" and "part of the fabric of the Fourth Amendment to the Constitution."[26] "The [U.S.] Supreme Court's decisions… have allotted great weight to home privacy within the Fourth Amendment," and "the Fourth Amendment… was arguably crafted around the castle doctrine itself."[27] Article 8 of the European Convention of Human Rights (ECHR) protects the right to respect for one's home and correspondence, and the European Court of Human Rights (ECtHR) has developed a rich body of case law for home protection.[28] Article 7 of the European Charter of Fundamental Rights recognizes "the right to respect for his or her private and family life, home and communications."[29] Further, in general, the home has been granted special protection in contemporary law. According to Barros, "the pervasiveness of the special treatment of homes in these contexts suggests the existence of a strong cultural consensus that homes are uniquely important when issues of security, liberty and privacy are at stake."[30] For instance, the concept of the home "occupies a sacred place in U.S. legal and cultural traditions."[31] The home has been particularly protected under constitutional law, tort law, property law, family law, tax law,[32] criminal law,[33] civil law, and contract law.[34] Even Article 8 of the ECHR acknowledges the importance of the home environment by protecting the individual against

---

25. For a discussion of the home castle doctrine, see Catherine L. Carpenter, *Of the Enemy Within, the Castle Doctrine, and Self-Defense*, 86 MARQ. L. REV. 653 (2003).

26. Jonathan L. Hafetz, *"A Man's Home is His Castle?": Reflections on the Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries*, 8 WM. & MARY J. WOMEN & L. 175, 175 (2002).

27. Tyler Anderson, Note, *Balancing the Scales: Reinstating Home Privacy Without Violence in Indiana*, 88 IND. L.J. 361, 367 (2013).

28. For a discussion of case law on home protection, see Eur. Ct. H.R., *Guide on Article 8 of the European Convention on Human Rights*, at 73–88 (Aug. 31, 2019), https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf [hereinafter Eur. Ct. H.R., *Guide on Article 8*].

29. Charter of the Fundamental Rights of the European Union, 2000 O.J. (C 364/10).

30. Barros, *supra* note 22, at 257.

31. Megan J. Ballard, *Legal Protections for Home Dwellers: Caulking the Cracks to Preserve Occupancy*, 56 SYRACUSE L. REV. 277, 279 (2006).

32. "Tax rules and government-backed mortgages provide incentives for home ownership." *Id.* at 279.

33. In most jurisdictions, criminal law protects the home by criminalizing trespass and burglary and by the requirement for a warrant in the search and seizure context.

34. In the context of a rental contract and associated tenant rights. For a detailed discussion of ways the law protects the tenant's personal interest in the home, see Barros, *supra* note22, at 282–90.

environmental pollution, above a certain threshold, that affects an individual's well-being and ability to enjoy the home.[35]

Though it is difficult to overstate the everyday importance of the home in law,[36] it is equally difficult to define what a home *is* under the law. Undoubtedly, however, home "is the place where [a person] lives and to which he returns, and which forms the center of his existence."[37] Whether the home space has been used for "dwelling" is an essential element or criterion in the legal definition of the home. Home is, as Shapiro put it, "a shelter of some sort that serves as the customary dwelling place of one or more persons," and can take various forms "from a mud hut to a Bedouin tent to a houseboat to a palace."[38] The traditional, classic home, usually understood as one's dwelling place, consists of physical infrastructure, such as walls, roofs, windows, curtains, and doors, and in some circumstances may include gardens and yards (or "curtilage") directly connected to the dwelling. Its physical existence not only creates the physical space to accommodate private activities and fend off physical intrusion, but also marks and separates the home as a space from the outside. The home is the most private space and place, and home activities are private activities; thus, the home is the clearest denominator in the public-private divide in modern societal life and law.[39] "[T]o the extent that a boundary between public and private existed, it corresponded to the boundary of the home."[40]

The physicality of the home allowed contemporary law to define and anchor home protection within comparatively clear physical boundaries. Home boundaries in law can be defined by physical boundaries of home space and place marked by walls, windows, curtains, roofs, fences, etc., and in turn by related legal concepts as seen in property law (ownership) and contract law (usership) that are mostly based on those physical boundaries. However, the home environment, both space and place, can change and evolve with technological developments over time, and thus the physical demarcations that separate the home from the outside have not been fixed.[41] In Shapiro's classic work on the interplay between

---

35. Eur. Ct. H.R., *Guide on Article 8*, *supra* note 28, at 85.

36. Fox, *supra* note 23, at 581.

37. Uratemp Ventures Ltd v. Collins [2001] UKHL 43 [31], [2002] 1 AC 301 (HL) 310 (appeal taken from Eng.).

38. Stuart Shapiro, *Places and Spaces: The Historical Interaction of Technology, Home, and Privacy*, 14 INFO. SOC'Y 275, 275 (1998).

39. *See* Barros, *supra* note 22, at 272 ("The evolution of home, in a sense, separated the family and its private life from the larger community."); Shapiro, *supra* note 38, at 275 ("But the home has served and continues to serve as a key locus for distinguishing between the public and the private.").

40. Shapiro, *supra* note 38, at 277.

41. In this paper, "home development" refers to the process of the home environment growing and changing to become more advanced in terms of

technology and home protection, he explained the impact of technology on home boundaries and the control of information flow to and from the home.[42] He addressed in great detail how the past century of technological developments—including the telegraph, the telephone, the internet, and telework—have changed the home environment and home life, separating the home space from the non-home place until the late 1990s. Notably, "they bring portions of the outside world into the home, but they also bring parts of the home into the outside world."[43] Shapiro argued that "different technologies, including structural elements, have affected and reflected over time the boundaries represented by the home" and that "that boundary has helped shape the construction of privacy in the West."[44] However, with the advent of smart home technology and IoTs, the modern home environment has undergone even more fundamental changes.[45]

The rise of the Home Virtual Space (HVS) and its co-existence with traditional physical space in the home has fundamentally changed the home environment and home life. *Home and home life exist not only in a physical space and place, but also in a virtual place and space and the interactions between the virtual and physical.* Yet contemporary law and its underlying rationales are mostly based on protection of the home in the physical nature of the home environment.[46] Contemporary law has hardly considered, *in a systematic manner***,** how to protect the HVS and its critical role in modern home life, especially given the increase in virtual intrusions and digital threats, causing home residents to start to lose control of their home through interference and surveillance.

The following section will illustrate in detail the fundamental changes in the modern home environment due to increasing digitalization, connectedness, smartization and automation. Section C will discuss big changes in home life from physical dwelling to smart living and the impacts of technical complexity on home occupants who are gradually losing control of their homes. Section D then analyses residents' diminishing privacy and protection at home due to these fundamental changes in the home environment—

---

meeting residents' different needs (for instance, the introduction of electricity and gas for lighting and cooking).

42. Shapiro, *supra* note 38, at 278–84.

43. *Id.* at 282.

44. *Id.* at 275.

45. Shapiro observed that "[w]ith the ruling in *Katz* [*v. United States*, 389 U.S. 347 (1967)], the home . . . was effectively extended into electronic space. The boundary of the home was fully acknowledged as being virtual as well as physical." *Id.* at 280.

46. *See* Zhao, *supra* note 16.

in particular, the permanent presence of digital service providers at home and the lack of clear home boundaries.

B. From Hybrid Space to Mixed Reality

The proliferation of the internet and mobile information and communications technology (ICT) in all corners of private life has created the reality of an "onlife" world,[47] and has made the contemporary home "a mixed zone," "a space into which individuals, families, publics and markets assume common residency."[48] In the post-digital age, life at home has gone far beyond physical dwelling, "transcend[ing] materiality and spatial locality via digital networks."[49] The physical home has expanded into the digital landscape via, for instance, social networking tools.[50] We also live in so-called "digital real estate," possessing digital property (such as photos) "transcending time and space and reaching others beyond existing concrete social circles."[51] We have reached a new stage of home development beyond physical boundaries; home residents may experience and reside in multiple spaces and places at the same time, collapsing the traditional boundary of the public and private and thus challenging traditional home protection rules and norms. This stage of development, up until the arrival of IoT and home automation, has been driven mainly by connectedness and digitalization.[52]

Evolving digitalization at home has resulted in increased personal data, digital property (both assets and data), and virtual existence. Growing connectedness further facilitates the separation of home space and place, information flow (both inwards and

---

47. "Onlife" refers to the fact that we are assembling the online world into our lifeworld, thus living in a new life environment characterized by the blurring of the distinction between reality and virtuality and between human, machine, and nature; the reversal from information scarcity to information abundance; and the shift from the primacy of entities to the primacy of interactions. *See* THE ONLIFE INITIATIVE, *The Onlife Manifesto*, *in* THE ONLINE MANIFESTO: BEING HUMAN IN A HYPERCONNECTED ERA 7 (Luciano Floridi ed., 2015).

48. Evelyn Honeywill, *The Coming Home of Postindustrial Society*, *in* REIMAGINING HOME IN THE 21ST CENTURY 150, 153 (Justine Lloyd & Ellie Vasta eds., 2017).

49. *Id.*

50. According to Justin McGuirk, traditional walls in the contemporary home support physical structures, "providing us with shelter, security and solitude," but nowadays walls via social networking tools, "also denote virtual conduits into which we invite the public, on which we 'post', 'share' and consume aspects of one another and our societies." *Id.*

51. *Id.*

52. Brennen and Kreiss, distinguishing between digitalization and digitization, refer to digitalization as "the way in which many domains of social life are restructured around digital communication and media infrastructures." Scott Brennen & Daniel Kreiss, *Digitalization and Digitization*, CULTURE DIGITALLY (Sept. 8, 2014), http://culturedigitally.org/2014/09/digitalization-and-digitization/ [https://perma.cc/U32D-FVRX].

outwards), and shifting home boundaries, much of which Shapiro predicted decades ago.[53] The arrival of IoT and the "smart home"—an application of IoT in the household—has further added smartization and automation to home environment, enhancing and supplementing home connectedness and digitalization. The home environment has encountered considerable changes, in that very soon the concept of home as "physical dwelling" will be replaced by "smart living." The long-term impacts of this change should not be underestimated, and may fairly be compared to the introduction of electricity, landline phones, and televisions into home environment.[54] Despite the lack of a common definition, "smart homes" can be defined as homes equipped with a range of inter-connected sensors, systems, and devices that can be automated, monitored and controlled through, for instance, a computer or smartphone from both inside and outside the home.[55]

Still at a nascent stage in their development, smart homes can result from unintentionally integrating new technologies with the traditional home environment, intentionally integrating new technologies (from the beginning),[56] or a home that is "smart by design." The most popular smart home assets at this moment include the following categories:[57] security assets (such as smart doors and windows); home automation appliances (such as vacuum cleaners, and smart heating and lighting); smart energy devices (such as thermostats and smart meters.); and smart home entertainment devices (such as smart TVs, smart projectors, and smart radios). The other two important categories are human-machine interface (such as the smartphone, remote control handset, personal digital assistant devices),[58] and home network devices (such as a router, bridge, repeater, modern, gateway and power-line). In addition, many digital devices that are not fixed at home but often connected to Home Area Networks (HANs) and devices at the physical home space and place are equally important, and can be regarded as part

---

53. *See* Shapiro, *supra* note 38, at 280–83.

54. These are only similar in the sense that the latter two connect the home to the outside world, but they do so with very different functionalities and roles in home life.

55. DAVID BARNARD-WILLS ET. AL., ENISA, THREAT LANDSCAPE AND GOOD PRACTICE GUIDE FOR SMART HOME AND CONVERGED MEDIA 5 (2015), https://www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence [https://perma.cc/N6P2-PC5K].

56. *See* W. Keith Edwards & Rebecca E. Grinter, *At Home with Ubiquitous Computing: Seven Challenges*, *in* UBICOMP 2001: UBIQUITOUS COMPUTING 256, 257 (Gregory D. Abowd, Barry Brumitt, & Steven Shafer eds., 2001).

57. For a detailed overview of smart home assets, see BARNARD-WILLS ET. AL., *supra* note 55, at 10–11.

58. Home occupants can be interacting with smart home devices when they are not consciously using them, especially when some devices (in particular sensors) are low profile and not visible to users**.** *See id.* at 41.

of smart home assets, including portable devices (smartphones, tablets, etc.) and connected smart cars.[59]

Smart home systems can perform different functions and achieve multiple ends. They can help home residents achieve better control over the home (including security,[60] efficiency, energy control,[61] comfort, healthcare,[62] and plant and pet monitoring); support personal lifestyle;[63] enhance self-sufficiency, health care and household management; and stimulate social life. Residents can virtually "enter" the home from a distance and do things at home via home automation; *vice versa*, they can "leave" home and do things outside the home without physically leaving the home. Many smart home devices can be used in ways beyond their designated purposes when combined with other devices. For example, analyzing data from smart meters can detect burglars based on unusual electricity consumption.

The smart home environment is still under rapid development. Home devices can be deployed in different ways with different security and privacy risks. In general, smart homes can be organized in four basic ways: (1) a fully decentralized model; (2) a model of local connectivity without connections to cloud services and a central gateway; (3) a centralized model based around a central hub or gateway of some form; or (4) a combination of the above three models. At this moment, a more popular and reliable approach is a centralized system built on a central hub or gateway. For instance, a central software system (located on a home-based device) coordinates all home devices and their services to provide added value and more complex services. This is the popular solution of

---

59. Another conceptual option is to include distant devices connected to smart devices and networks at home as part of a larger concept of "smart home" or "digital home" transcending physical boundaries. This will be discussed in Section II (C).

60. Not only can smart security devices provide security, but networked homes can also provide collective services via public platforms for local authorities and utility providers, including emergency telemedicine service, natural disaster assistance, time-sensitive information delivery from law enforcement, and social support from local government. *See* Muhammad Raisul Alam et al., *A Review of Smart Homes—Past, Present, and Future*, 42 IEEE TRANSACTIONS ON SYS., MAN & CYBERNETICS, PART C (APPLICATIONS & REVS.) 1190, 1200 (2012).

61. *See* Jean-Nicolas Louis et al., *Environmental Impacts and Benefits of Smart Home Automation: Life Cycle Assessment of Home Energy Management System*, 48 IFAC-PAPERSONLINE 880, 880–85 (2015), https://doi.org/10.1016/j.ifacol.2015.05.158.

62. This includes healthcare for aging and disabled people, as well as remote monitoring of patients. *See* Alam et al., *supra* note 60, at 1200.

63. This includes "green living." *See* Sarah Mennicken, Jo Vermeulen & Elaine M. Huang, *From Today's Augmented Houses to Tomorrow's Smart Homes: New Directions for Home Automation Research*, *in* PROCEEDINGS OF THE 2014 ACM INTERNATIONAL JOINT CONFERENCE ON PERVASIVE AND UBIQUITOUS COMPUTING 105, 108 (2014), http://doi.acm.org/10.1145/2632048.2636076.

current market players including Amazon, Google, and Apple, offering central gateways/services to coordinate different devices (and services) from other service/device providers. This can be a much safer approach with a centralized HAN and secured network security management from the service provider. But in reality, users often combine a centralized structure and sporadically installed smart devices that are not connected to the centralized HAN. For instance, smart cars and smart meters may not be integrated into a centralized system. This mixed structure is a market reality due to the different range of services and to the requests of service providers.[64] The viability of the smart home is flailing, in large part because the smart home is expensive and complicated to install and because it does not function cohesively (due to problems of interoperability and post-sale maintenance such as software updates).[65]

In the new home environment, the most apparent, fundamental changes include the rise of the Home Virtual Space (HVS), the co-existence of both physical and virtual spaces (including Ambient Intelligent Space), and the creation of "mixed realities" from their increasing interaction. [66] The rise of HVS is a distinctive feature of the new home environment. The new home reality consists of the co-existence of virtual space and physical space at the same home geo-location (place) and space, with the HVS' *virtual and limitless* connection to the outside, and physical space with *limited, physical* connections. HVS has not been defined in the specific context of home development, nor does a commonly accepted definition of HVS exist among scholars. Drawing insights from the works of Chaffee and Fayard on virtual space,[67] HVS can refer to material infrastructure, including connected network devices, smart devices, and software, either installed in the traditional home or soon to be

---

64. They may want to have networked services separate from those provided by Google, Amazon, etc.

65. Stacey Higginbotham, *The Smart Home's Problem Is Its Best Product Is Terrible and Made by a Bankrupt Company*, FORTUNE (Oct. 16, 2015), http://fortune.com/2015/10/16/smart-home-problems/ [https://web.archive.org/web/20191025024452/https://fortune.com/2015/10/16/smart-home-problems/].

66. Some scholars may separate Virtual Space from the Ambient Intelligent Space conceptually. *See* Carol Saunders et al., *Virtual Space and Place: Theory and Test*, 35 MIS QUARTERLY 1079 (2011); Mohammadali Heidari Jozam et al., *VR-Smart Home: Prototyping of a User Centered Design System*, *in* INTERNET OF THINGS, SMART SPACES, AND NEXT GENERATION NETWORKING 107, 108 (Sergey Andreev, Sergey Balandin & Yevgeni Koucheryavy eds., 2012).

67. *See* Eric C. Chaffee, *Securities Regulation in Virtual Space*, 74 WASH. & LEE L. REV. 1387, 1394–95 (2018); Anne-Laure Fayard, *Space Matters, But How? Physical Space, Virtual Space, and Place*, *in* MATERIALITY AND ORGANIZING: SOCIAL INTERACTION IN A TECHNOLOGICAL WORLD 177 (Paul M. Leonardi, Bonnie A Nardi & Jannis Kallinikos eds., 2012).

built into the home.[68] HVS can also refer to the software-generated virtual environment that exists in the home's traditional physical space, including entities such as connected video game systems (e.g., Xbox or Wii), HANs (wired or wireless), social networking environments (via mobile apps), information/data flows, and virtual property such as virtual currency and virtual belongings.

On this point, Brey's distinction between two types of virtual entities, *simulations* and *ontological reproductions*, can help understand the nature of the HVS. Simulations refer to virtual versions of real-world entities with perceptual or functional value similar to the real world equivalent, but having no pragmatic worth or effect.[69] Ontological reproductions are computer imitations of real-world entities that have nearly the same value or programmatic effects as their counterparts, and thus bear real-world significance that extends beyond their virtual environment (thus with similar real-world value to their physical counterparts). Many virtual entities can be just as "real" as their physical counterparts and have real pragmatic significance. One can quickly understand this difference by comparing a virtual beer with a virtual chess game. In this sense, the current HVS can equally contain two types of virtual entities: virtual simulations such as virtual games and other virtual objects (valuable only in the virtual environment), and ontological reproductions with real-world pragmatic significance such as digital and digitalized documents, digital currency, and log data.

The co-existence of the HVS and the physical space of the home and their interactions give birth to what is called *hybrid spaces*. The newly added technological devices are new assets establishing the physical conditions for the HVS, accommodating information-related activities including social networking, online shopping, teleworking, and telelearning. The "Ambient Intelligent Space" refers to an environment that is equipped with computers and sensors to adapt to user activities through an automated form of awareness.[70] Thus, the HVS "depends on real-world spatial fixity - the points of accessing the physicality and materiality of wires," but exercises "independence" in that it is not confined and defined by physical boundaries.[71]

---

68. They can be interpreted as part of the HVS because they are made and installed for creating such a space, if not for other purposes at home.

69. One can argue, on the other hand, that even a virtual beer has its own value in a virtual game environment (though not in the physical world). This is the reason why many players buy or exchange arms in virtual war games to gain competitive advantage.

70. Erfaneh Allameh et al., *The Role of Smart Home in Smart Real Estate*, 5 J. EUR. REAL EST. RES. 156, 159 (2012).

71. *See* Robert M. Kitchin, *Towards Geographies of Cyberspace*, 22 PROGRESS IN HUM. GEOGRAPHY 385, 387 (1998).

Further, the HVS occupies both a physical location (i.e., the home place and space) and a designated virtual location (the assigned IP address or home network address, depending on the setup). The HVS can be guarded by network passwords or codes that are known to home residents or authorized users.

Further, the HVS can be *a reflection, demonstration, and/or mirror* of the traditional physical home. The traditional physical home can be measured, analyzed and managed in virtual space by means of human-machine interfaces such as smartphone apps, tablets or home hubs. Though the HVS may not currently be a precise copy of a physical home, it does engage with and integrate some physical assets. The HVS collects data and uses this data to interact with the physical home to improve home security, comfort and efficiency. For instance, smart robot cleaners that map home space may then share the data with other smart home devices.[72] Home-generated data (and data processing) is the essential building block of the HVS, and contributes to "surveillance capitalism".[73] There is also a perceptual aspect of the HVS. According to Saunders et al. what exists in virtual space for people is both *perceptual space* and *cognitive space* in the user's mind, although the space in virtual worlds mimics physical space. Virtual worlds are not physically three-dimensional, and they only appear three-dimensional in the mental representations of users.[74] The HVS is likely to be constructed as a replication of the real home environment: "not only are they like real-world spaces but they are also often in the image of real-world spaces."[75] Whatever the nature of HVS is, "in today's world, digital and physical environments are increasingly mixed, offering us a hybrid space in which to interact."[76] Home physical and virtual spaces are closely interwoven, and their boundaries are merging and being redefined, at least in the context of how residents and other people connect to and interact with each other and the outside world in the new home environment.[77]

Due to the rapid development of smart home technologies, the interaction of the HVS with physical space at home has further created "mixed reality."[78] In this new phase, physical and digital

---

72. Mapping data (with home assets identified and assigned names) can also be shared with and used by other smart devices within the HANs. *See* James Vincent, *Google Wants to Improve Your Smart Home with iRobot's Room Maps*, VERGE (Oct. 31, 2018, 9:00 AM), https://www.theverge.com/2018/10/31/18041876/google-irobot-smart-home-spatial-data-mapping-collaboration.

73. *See* Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 78 (2015).

74. Saunders et al., *supra* note 66, at 1081.

75. Kitchin, *supra* note 71, at 395.

76. Fayard, *supra* note 67, at 192.

77. *Id.* at 177–78.

78. This is especially the case with entities such as experimental virtual reality contact lenses, brainwave controllers, and full sensory interfaces, and, in the

objects and entities co-exist and interact with each other at a higher level in real time, with a continuum ranging from a completely real and natural environment, to a completely virtual environment in the traditional physical home space/place. Though mixed reality can broadly mean all stages of data-enriched real or virtual environments, mixed reality augments real places, people and things with rich virtual experiences.[79] According to Fairfield, "the central element of Mixed Reality is the tying of data to an anchor in the real world, be it a person, geographic location, or structure."[80] "Mixed Reality applications enrich the real world with virtual data through the use of technology," and "sit at the midpoint of the RV continuum. They are grounded in real objects and space but augment those objects or places with computer-generated data."[81] In the new home hybrid spaces, "interaction and activity flow across physical and virtual spaces."[82]

One can experience partially mixed reality in museums. Some museums that previously provided on-site audio guides now offer virtual information to visitors, connecting them to virtual spaces and times via hyper-linking capacity, interactivity, and multimedia capabilities. Other examples include the well-known Pokémon Go game and the use of Google Glass.[83] "People move at ease between physical reality, the two-dimensional cyberspace, and virtual reality cyberspace. They carry cyberspace in their pockets, they wear it, and they live with it in their homes."[84] The HVS thus largely enriches the physical space of the home with extra virtual dimensions and hyperlinked information, as well as home automation.[85] Home

---

future, direct nervous system links. These make it difficult or even impossible to distinguish between cyberspace behavior and physical behavior, and between real, not real, and virtually real. *See* Gilad Yadin, *Virtual Reality Exceptionalism*, 20 VAND. J. ENT. & TECH. L. 839, 879 (2018). In this article, hybrid space and mixed reality refer to the same phenomenon of the coexistence and interaction of the HVS and home physical space, but mixed reality refers more to mixed human perceptions of the home environment as "reality."

79. Joshua A.T. Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, 27 BERKELEY TECH. L.J. 55 (2011).

80. *Id.* at 63.

81. *Id.* at 73–74.

82. Jannis Kallinikos et al., *The Challenge of Materiality: Origins, Scope, and Prospects*, *in* MATERIALITY AND ORGANIZING: SOCIAL INTERACTION IN A TECHNOLOGICAL WORLD 3, 16 (Paul M. Leonardi et al. eds., 2012).

83. Some may call Pokémon Go augmented reality. *See* Larry Greenemeier, *Is Pokémon GO Really Augmented Reality?*, SCI. AM. (July 13, 2016), https://www.scientificamerican.com/article/is-pokemon-go-really-augmented-reality/.

84. Yadin, *supra* note 78, at 879.

85. For a detailed discussion of home automation systems, see Alexandre Demeure et al., *Building and Using Home Automation Systems: A Field Study*, *in* END-USER DEVELOPMENT 5TH INTERNATIONAL SYMPOSIUM, IS-EUD 2015 MADRID, SPAIN, MAY 26–29, 2015 PROCEEDINGS 125 (Paloma Díaz et al. eds., 2015).

automation is another important element for considering technological complexity, adding another layer of already complex human-environment interaction via installing various automated functions such as smart heating and smart coffee makers. The technical complexity of home automation results in residents' diminishing control over the home, which will be further analyzed in the next section.

C. Growing Complexity and Losing Control: From Physical Dwelling to Smart Living

Overall, escalating digitalization, connectedness, smartization, and automation have significantly changed our home environment, and have consequently transformed our home life from *dwelling in physical space* to *smart living in mixed reality*. A number of significant changes in the household and home life require our attention in analyzing the efficacy of the current law on protection of the home.

The first fundamental change is that the HVS has now become the center of home life in terms of organization, management, and maintenance, with a considerable part of home life shifted to virtual space. The concept of "me-time" in the U.S.,[86] which exists largely at the cost of sacrificing other activities or multi-tasking at home,[87] now oftentimes means smartphone time in the living room, at the dining room table,[88] or in bed. Residents can be physically in the home but virtually active outside the home. Life in cyberspace is about participating without even leaving home.[89] Second, the increasing connectivity of the home environment to the outside has blurred the previously clear boundaries of the public-private divide, leading to what is so-called the "*private/public home*."[90] The home is no longer a private closed environment, and "where to draw the line between public (or corporate) and personal information" becomes an important issue.[91] Third, social relationships and interactions have changed in a similar fashion within the home. Digital interconnections have supplemented or replaced many common family activities, such as increased smartphone use even while dining

---

86. *How People Really Use Mobile*, HARV. BUS. REV. (Jan. 2013), https://hbr.org/2013/01/how-people-really-use-mobile.

87. *See* Lynne Hamill, *Changing Times: Home Life and Domestic Habit*, *in* THE CONNECTED HOME: THE FUTURE OF DOMESTIC LIFE 29, 31–33 (Richard Harper ed., 2011).

88. *6 Tech Habits Changing the American Home*, BARNA GROUP (Apr. 18, 2017), https://www.barna.com/research/6-tech-habits-changing-american-home/.

89. LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 287 (2006).

90. Andreas Jacobsson, Martin Boldt & Bengt Carlsson, *A Risk Analysis of a Smart Home Automation System*, 56 FUTURE GENERATION COMPUTER SYS. 719, 720 (2016).

91. *Id.* at 731.

and watching TV together.[92] Even at home, people can have intense, "constant and ubiquitous link[s]" with persons who are not family members.[93] People who can manage multiple digital devices and home networks have more bargaining power when they are more needed by other home residents.

Fourth, digital assets, *e.g.*, digital photos, files, documents, and currency, like the non-digital parallels, are increasingly counted as essential parts of home property. This has been accompanied by the growing significance of home-generated data for both residents and for service providers. The proliferation of smart, connected products has "turn[ed] the home into a prime data collection node."[94] In a sense, home-generated data will constitute critical building blocks for the new generation of "home"; they will not only keep the home functioning, but will also serve as a digital archive. Such data can be stored at a home-located database (hard drive), through service provider's storage, or through third-party storage (via cloud services). A growing, serious concern is the further processing of home-generated data from ubiquitous computing and home automation; for instance, considering their data richness, where should such data be processed? How should it be used? And by whom? Fifth, home smartization and automation have shaped home behaviors,[95] and have created the capacity for home monitoring of children and home surveillance by law enforcement agencies.[96]

A final, but significant, change in the home environment is the strong digital corporate "presence" in each corner of our home. These digital corporations help build our smart home, and, therefore, their strong presence is justified in providing continuous services as our unseen "roommates." [97] In the pre-digital era, homebuilders left residents alone after finishing their work. They needed to make an appointment when they wanted to come back to conduct repair work, and our home was under the residents' control. However, digital homebuilders never *virtually* leave, and intrude when they need to update software and implement security patches,

---

92. Kirsten Gram-Hanssen & Sarah J. Darby, *"Home Is Where the Smart Is"? Evaluating Smart Home Research and Approaches Against the Concept of Home*, 37 ENERGY RES. & SOC. SCI. 94, 98 (2018).

93. Stefana Broadbent & Claire Lobet-Maris, *Towards a Grey Ecology*, *in* THE ONLIFE MANIFESTO: BEING HUMAN IN A HYPERCONNECTED ERA 111, 120 (Luciano Floridi ed., 2015).

94. McGuirk, *supra* note 16.

95. Behavior changes when search engines are used as the "domestic mind" in the modern home. *See* Richard Harper, *From Smart Home to Connected Home*, *in* THE CONNECTED HOME: THE FUTURE OF DOMESTIC LIFE 3, 6 (Richard Harper ed., 2011).

96. For a discussion of surveillance by police via compromising home devices, see Škorvánek et al., *supra* note 10.

97. Sophia Maalsen & Jathan Sadowski, *The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance*, 17 SURVEILLANCE & SOC'Y 118, 119 (2019).

or transfer home-generated data to servers—even to servers in foreign countries. The omnipresence of digital homebuilders also includes social networking service providers such as Facebook that are trying to develop their own smart home systems to extend services to the home environment.[98] Their presence is ubiquitous, and residents cannot deny them access, essentially meaning that residents agree to keep their back garden door open to welcome service providers to conduct repair work at any time. The home thus has other members in the virtual sense, who exist within the home having the same physical presence as residents. This creates a risk that the adoption of Smart Home Technologies (SHTs) is opening up unwanted data flows between the home and the outside world.[99] Unavoidable data flows combined with technological complexity means unavoidable growing interference of private corporations in private home space.

Home residents that lack professional knowledge and security awareness in the complex, often hybrid smart home environment are the vulnerable party in the new user-service provider relationship. Consent is a well-known problem in service contracts, as users either tend to consent to data collection and processing in vague terms, or they do not bother reading contractual clauses at all before accepting services. Consent in reality sets up the legal boundaries for the HAN. Home residents cannot see the virtual boundaries of the smart home and have no effective control of this "layer" of the home, in contrast to its physical components, i.e., windows, walls, roofs and fences.[100] Physical assets and boundaries have increasingly been replaced by protocols and algorithms in the virtual world that residents cannot not control, relegating them to the will of digital giants.[101]

Home users have eventually lost control of their own homes, becoming data generators or data carriers for service providers. Zygmunt Bauman defined this as "the commodification of the self," characterizing homes as "leaky data boxes."[102] At this point, the home "becomes an extension of our immaterial labor," producing metrics similar to that produced by wearable tech, monitoring and measuring us.[103] As datafication and data commodification of the home environment are widespread phenomena, there is a strong risk

---

98. Michael Calore, *Facebook Made You a Smart-Home Device, and There's a Camera on It*, WIRED (Oct. 8, 2018, 9:00 AM), https://www.wired.com/story/facebook-portal-smart-home-device/.

99. Gram-Hanssen & Darby, *supra* note 92, at 97.

100. Zhao, *supra* note 16.

101. *See, e.g.*, Natasha Lomas, *Critical Flaw IDed in ZigBee Smart Home Devices*, TECHCRUNCH (Aug. 7, 2015, 9:02 AM), http://social.techcrunch.com/2015/08/07/critical-flaw-ided-in-zigbee-smart-home-devices/.

102. FAIRFIELD, *supra* note22, at 110.

103. McGuirk, *supra* note 16.

that residents may take their current weak position for granted. They must redefine their relationship to providers to regain control, a goal that is critical to personal development and privacy.[104] In general, loss of control is largely due to technological complexity and advances out of residents' reach, including the presence of very sophisticated HAN structures (with mesh network and legacy devices) and absence of human-machine interfaces. Residents cannot figure out how exactly smart home systems work and where security vulnerabilities are. This loss of control may explain why many people are reluctant to introduce smart devices into their homes, or why others simply have blind trust in smart home services.[105]

D. Diminishing Privacy and Home Protection

As illustrated above, digitalization, connectedness, smartization and automation have changed the home from a traditional physical space and place, to a hybrid space, and finally to a mixed reality in the IoT age. Accordingly, our home life has been transformed from mere "dwelling" to smart living with altered home behaviors. These changes—mostly associated with the rise of HVS, mixed reality, data transfer and processing, and weakening home control—have led to considerable privacy and security risks and threats to the home, testing and contesting the current legal framework for home protection.

The European Union Agency for Cybersecurity (ENISA)'s threat landscape 2014 report on smart homes and converged media provides a detailed, still-valid picture of different threats imposed by these technological developments. These include physical attacks; unintentional damage (accidental); disasters (natural environmental); damages or loss of IT assets; failure or malfunctions; eavesdropping or interception or hijacking; nefarious activity and abuse; and legal threats (violation of laws or regulations, failure to meet contractual requirements, and unauthorized use of copyrighted material). A majority of the vulnerabilities emerge from business models, economic incentives, different ownership and administration models, and pervasive and persistent insecurity.[106] These vulnerabilities lead to significant risk of harm in smart homes, creating opportunities for potential cybercrime, privacy invasion,

---

104. "The notion of the home and what it entails has been fundamental to the construction of conceptions of privacy over time." Shapiro, *supra* note 38, at 275.

105. Control can concern protection from outside intrusion, automation of various functions and services, autonomy and independence within home, or response to information from outside the home. *See* Charlie Wilson, Tom Hargreaves & Richard Hauxwell-Baldwin, *Smart Homes and Their Users: A Systematic Analysis and Key Challenges*, 19 PERS. & UBIQUITOUS COMPUTING 463, 473 (2015).

106. BARNARD-WILLS ET. AL., *supra* note 55, at 39–42.

and data breaches[107] through, for instance, function creep and social sorting.[108] Threat agents include numerous corporations with commercial interests in home data collection such as data miners and advertisers (with threats derived from use and abuse of intentionally shared or unintentionally leaked information from smart homes), and technology vendors and service providers (with threats derived from errors in "design, installation, administration, maintenance of devices and systems," as well as legacy devices and failed service). Other threat agents include cyber criminals (financial criminals and content pirates), traditional criminals, hacktivists, terrorists and nation states (law enforcement, espionage, cyber warfare, intelligent services). [109]

These threats make the new generation of the home, especially the spatial-virtual space, vulnerable, even when walls and fences can block physical intrusions from the outside. The cases discussed in the beginning of this paper represent home surveillance by service providers, either of a public or private nature. As many have already noted, smart home devices can be deployed as useful tools for invasive surveillance by state authorities,[110] by service providers for commercial profits, by hackers for profits and ill intentions, and even by family members for control and monitoring, resulting in pervasive privacy invasion. Virtual home invasions are a new threat that can be more serious than physical invasions due to the quality and quantity of personal data collected from home environment. All home-collected data (log data, metadata, and communication data) are virtually personal data, attributable to residents, that serve to further data profiling. Home-generated data are very rich in volume, variety and quality and reveal even the most private parts of home life (sexual activities, intimate relationships, financial status, health conditions, etc.). Illegal or non-consensual processing even outside of the home space can thus be interpreted as serious home invasions.

Thus, in the IoT age, to "protect the home" is to protect both the physical home space and the new HVS and home-generated data. In this respect, the current law has not developed sufficient protection in the major areas most in need of upgrade.

---

107. *Id.* at 41–42.

108. "Social sorting" means that people are assigned different categories, worth or risk in a way that has significant impact on their life chances. *Id.* at 43. "Function creep" constitutes "a certain instrument being used for something other than [its] intended purpose." *See* Dick Dekkers, *Privacy or Security? - "Function Creep" Kills Your Privacy*, DIGIDENTITY (Sept. 2, 2016), https://www.digidentity.eu/en/article/Function-creep-kills-your-privacy/.

109. BARNARD-WILLS ET. AL., *supra* note 55, at 35–37.

110. We are now in the golden age of surveillance, in which intelligence and law enforcement agencies are "going dark" for identification, monitoring, location tracking, or gaining access to networks or user credentials. *See* Timm, *supra* note 10.

First, traditional criminal law cannot sufficiently protect home residents from *virtual trespass*, including spam, computer viruses, malware, and home device hacking. In the earlier ages of cyberspace, spam, viruses and malware were the major forms of virtual trespass of home computers. At present, with cyber trespass law in force, these forms are largely mitigated; however, incidents like the famous WannaCry ransomware attack demonstrate that they still sometimes pose considerable threats to the community.[111] Cyber trespass law "has always been the constraint on private parties."[112] Today, another type of virtual trespass happens more frequently, often without our awareness. With more companies interacting with or controlling our home devices, while some of them only operate "to the extent to get the job done," "many others don't ask, or go well beyond the resource use necessary for the task at hand." [113] Some companies install software for user-designated purposes but not always in the user's interests; others may secretly install unrequested software for other purposes, like mining Bitcoin on a home resident's computer, portable device, or other home devices. Further, hacking into the system and re-programming devices to run desired software, so-called "generative functionality," opens up a wider range of threats, including monitoring network traffic; controlling other devices; and extracting information stored in the system, including sensitive personal data and media content.[114] Threats also include external functions such as hosting malware or illegal websites, operating as part of a botnet, or sending spam emails.[115]

Most western jurisdictions criminalize physical invasion or entry of a home without the residents' consent, through prohibitions on trespass, burglary, and home theft. As Yadin's recent research revealed, broad unauthorized access provisions are the backbone of the US CFAA (Computer Fraud and Abuse Act of 1986), U.S. state-level computer misuse legislation, and computer hacking laws worldwide by way of the 2001 Council of Europe Convention on Cybercrime.[116] Hacking legislation can be vague, and cyber stalking and cyber harassment laws are ineffective in many jurisdictions (at least in the U.S.).[117] When hacking activities are conducted by hackers from foreign jurisdictions, access to digital evidence and judicial cooperation is problematic, even when the incurred damage

---

111. *See* Timothy B. Lee, *The WannaCry Ransomware Attack Was Temporarily Halted. But It's Not Over Yet.*, VOX (May 15, 2017, 4:20 PM), https://www.vox.com/new-money/2017/5/15/15641196/wannacry-ransomware-windows-xp.

112. FAIRFIELD, *supra* note22, at 121.

113. *Id.* at 120.

114. BARNARD-WILLS ET. AL., *supra* note 55, at 42.

115. *Id.*

116. Yadin, *supra* note 78, at 851.

117. *Id.* at 851–55.

is serious. Mutual Legal Assistance (MLA) procedures may render the process of acquiring digital evidence (not limited to hacking) very time-consuming.[118] Even recent developments in private and public partnerships (PPP) have not improved efficacy of cyber regulation, although the growing engagement of industry has obvious advantages in cybercrime investigation.[119]Additionally, traditional criminal laws that punish trespass cannot be fully applied to hacking activities because of the different nature of "entering": while physical trespass requires the crossing of a spatial boundary and the presence of a human body in a specific area of home, virtual trespass only requires entry into the HVS without physical presence, which is usually unknown until harm is detected. The same can be said for cyber stalking and cyber harassment in the home environment, for which laws originating from the physical are not easily applied to virtual space and cross-border harm.

Second, the contemporary legal framework cannot provide sufficient protection for the new generation of homes against state intrusions, especially in the context of criminal investigation (i.e., search and seizure and police hacking) and intelligence agency activities. Recognizing what former FBI Director James Comey termed "going dark,"[120] legislators in many western countries have used domestic law to set limits on police hacking powers, recognizing their potential intrusiveness.[121] "Hacking by law enforcement is a relatively new phenomenon in the context of the long-standing conflict between security and privacy" (at least in the EU), and "access to encrypted and other data through such hacking techniques brings significant investigative benefits."[122] There should

---

118. As RAND's research demonstrates, irreducible complexities and time-consuming elements always exist in MLA procedures when extraterritorial digital evidence is involved. *See* MICHAEL J. D. VERMEER, DULANI WOODS & BRIAN A. JACKSON, RAND CORP., IDENTIFYING LAW ENFORCEMENT NEEDS FOR ACCESS TO DIGITAL EVIDENCE IN REMOTE DATA CENTERS 9–10 (2018) (ebook), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2240/RAND_RR2240.pdf.

119. *See* Thomas J. Holt, *Regulating Cybercrime Through Law Enforcement and Industry Mechanisms*, 679 ANNALS AM. ACAD. POL. & SOC. SCI. 140, 148 (2018).

120. "Going dark refers to the phenomenon by which government agencies have a legal right to access particular communications but lack the technical ability to do so, often because technology companies have deployed strong encryption to shield the information." Susan Hennessey, *Lawful Hacking and the Case for a Strategic Approach to "Going Dark"*, BROOKINGS (Oct. 7, 2016), https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark [https://perma.cc/7RN9-SR9M].

121. *See* Škorvánek et al., *supra* note 11, at 12–28.

122. MIRJA GUTHEIL ET AL., EUR. PARLIAMENT, LEGAL FRAMEWORKS FOR HACKING BY LAW ENFORCEMENT: IDENTIFICATION, EVALUATION AND COMPARISON OF PRACTICES 8 (2017), http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.

be sufficient protection of the home in this gray area of constitutional law. However, current research shows that even though constitutional law and criminal law offer robust protection of home life in many constitutional jurisdictions, their relevance to police hacking activities is "limited and partial."[123] Legal protections stemming from the sanctity of the home are more relevant in cases when computers within the home are used to monitor the home environment,[124] but are less relevant when data stored on the computer is the target of the investigation. In Dutch and German law, for instance, the protection of the home does not appear to be a *directly* relevant standard of protection in the case of covert remote searches.[125] Other potential measures "requiring technology vendors and service providers to bypass the security of their own products and services," and requiring "systematic weakening of encryption through the mandated introduction of backdoors and/or weakened standards for encryption" risk infringement of the fundamental right to privacy and infringement of network security.[126]

In the search and seizure context, for instance, the Fourth Amendment of the U.S. Constitution requires a search warrant in the case of physical entry into a home by law enforcement agencies. However, this area of law has not been developed to provide sufficient protection for homes in the IoT environment. As Christopher Slobogin asserted, "[w]ithout a proper recognition by the [Supreme] Court of how the Fourth Amendment protects digital privacy, virtual access by law enforcement threatens the security of citizens in their houses and digital effects."[127] Stefan Ducich advocated that Fourth Amendment privacy protection should be based on exclusion, presuming "an objective unreasonableness in any warrantless penetration by the state into the smart home," rather than a physical trespass approach that fails to account for the potentially remote nature of government incursions.[128] In Europe, Article 8 of the European Charter of Human Rights protects the rights of respect for private life, family life and home, with strong case law developed by the ECtHR.[129] However, none of these provisions explicitly extends protection of the home to police

123. Škorvánek et al., *supra* note 10, at 53.
124. *Id.* at 53–54.
125. *Id.* at 57.
126. GUTHEIL ET AL., *supra* note 122, at 8–9.
127. Stefan Ducich, *These Walls Can Talk! Securing Digital Privacy in the Smart Home Under the Fourth Amendment*, 16 DUKE L. & TECH. REV. 278, 291 (2018) (citing Christopher Slogobin, *A Defense of Privacy as the Central Value Protected by the Fourth Amendment's Prohibition on Unreasonable Searches*, 48 TEX. TECH. L. REV. 143, 161 (2015)).
128. *Id.* at 278, 298.
129. Eur. Ct. H.R., *Guide on Article 8*, *supra* note 28, at 73–87.

hacking or other categories of remote or virtual entry,[130] and the Court has yet to rule on their application to virtual space and digital assets. Still, to address challenges from previous ICT development, the Court has extended physical home protection, even in a rather broad manner, to cover non-traditional home spaces. Perhaps somewhat radically, the court recognizes that homes are not limited to traditional residences, but include caravans and other unfixed abodes (such as cabins or bungalows stationed on land), an individual's business premises (such as the office of a member of a profession, a newspaper's premises, a notary's practice, or a university professor's office), the branches or other business premises of a company, or possibly even training centers and venues for sports events and competitions and their annexes (like a hotel room in the case of away events).[131]

The third-party doctrine in common law privacy protection may not be valid in the new digital home environment, when home-generated data transferred to a third-party device and service providers may have great impact on the life of residents.[132] U.S. legal scholars have argued for extending Fourth Amendment protection to internet communications, for the sake of discrete transmission or interpersonal privacy protection.[133] The information that a person knowingly exposes to the public, even in his own home or office, is usually not subject to Fourth Amendment protection.[134]

Third, invasions of HVS can happen both outside the home space and at any time, and thus largely run short of effective legal constraints. Home-generated data can be transferred to or accessed by third parties in possession of network services and device providers under vague contractual clauses. Thus, data controllers and processors can understand what happened in a home environment without physically entering the home space. As

---

130. *Id.*

131. *Id.* at 74. In so extending protection, the Court has adapted to the shifting of private life and home-associated assets (like digital photos and bills) to other virtual places and spaces that need equal privacy protection.

132. Under third-party doctrine, "a person loses Fourth Amendment protection—i.e., does not have a reasonable expectation of privacy—to any communications that the person voluntary discloses to another." Monu Singh Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 2 (2013). For a discussion on the pitfalls of the third-party doctrine, see Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 622 (2011).

133. Protection is, however, more or less implicated in Smith v. Maryland, 442 U.S. 735, 743–44 (1979). *See* Bedi, *supra* note 132, at 8.

134. Katz v. United States, 389 U.S. 347, 351 (1967). But the third-party exception to the privacy doctrine should not be overstated. The Supreme Court has sometimes found that information shared with third parties is still subject to Fourth Amendment protection. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2221–23 (2018) (finding that cell-site location information is subject to Fourth Amendment protection).

"function creep" shows, smart home data have "predictive value for applications including market segmentation, risk classification, assessments of insurability, and policing and crime control."[135] Even knowing what devices a consumer owns at home can constitute a serious privacy violation.[136] Privacy harm, in terms of data misuse or abuse, is far outside of the awareness of residents. The threat of harm exists most when the same company whose services or devices a resident uses in the home conducts data profiling and commoditizing. In this regard, protection is traditionally granted by privacy and data processing clauses in a consumer contract; in reality, however, this is largely compromised by "the fallacy of consent."[137] As illustrated above, physical ownership of smart devices cannot prevent the further, continued control of these devices by their producers and by service providers. Operating systems (OS) and smart home software generate a similar problem of access and control by providing for updates and maintenance by default.[138] It is clear that property rights that once granted an owner the strongest degree of control based on physical possession fail to do so in the digital world.[139]

Fourth, co-control of the home environment through smart home devices, depending on the network setup, is problematic. Recent data protection regulations will not provide the desired level of home protection, as home-generated data will travel beyond the physical boundaries of the home and will end up in the hands of third parties.[140] "Aggressive IP laws, restrictive contractual provisions and technological locks"—the latter of which include end-user license agreements (EULA) and digital rights management (DRM)—have deprived residents of control over the digital goods

---

135. BARNARD-WILLS ET. AL., *supra* note 55, at 43.

136. NOAH APTHORPE ET AL., A SMART HOME IS NO CASTLE: PRIVACY VULNERABILITIES OF ENCRYPTED IOT TRAFFIC 2 (2017), https://arxiv.org/pdf/1705.06805.pdf [https://perma.cc/7GAU-894Y].

137. Colin O'Malley, *Zuckerberg's Testimony and the Fallacy of Consent*, LUCID PRIVACY GROUP (Apr. 11, 2018), https://lucidprivacy.io/zuckerbergs-testimony-and-the-fallacy-of-consent-55e9eb8839aa.

138. A similar problem happens with other smart devices, such as smart toys. *See* Esther Keymolen & Simone Van der Hof, *Can I Still Trust You, My Dear Doll? A Philosophical and Legal Exploration of Smart Toys and Trust*, 4 J. CYBER POL'Y 143, 150–51 (2019).

139. Consider, for example, the difference between owning a paper book and a digital book purchased from Amazon: Kindle content is licensed, not sold.

140. Take the most stringent data protection legislation – the European General Data Protection Regulation (GDPR). The law is widely criticized for its vague, unenforceable basic definitions of personal data, consent, controllers and processors. *See, e.g.*, Nadezhda Purtova, *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, 10 L., INNOVATION & TECH. 40, 75–78 (2018).

they buy.[141] At the present stage, the home is still "independent" from the HVS and digital assets, as they are largely affixed and supplementary to the basic functioning of the home. However, in the near future, they are likely to become built-in features at the backbone of home functioning and organization, as seen in some automated industrial sectors. When this occurs, the relationship between the home and service providers will undergo an even more fundamental change, as residents lose ownership control.

Fifth, diminishing control over the home environment in the face of increasing interference from both state and corporate powers triggers further concerns regarding the status of the fundamental values underlying home protection, including peace, privacy, security, autonomy, self-development, freedom of expression, and family life. As discussed, one of the core rationales behind protecting the inviolability of the home is to secure residents' prevailing territorial control against unwanted intrusions; this is not sufficiently achieved under the current legal framework. Failure to protect this control critically threatens other home-protected values, like privacy and autonomy. Within the new home environment, strong licensing laws associated with smart devices and services protect "a small coterie of powerful private actors" and limit our autonomy through EULA and DRM.[142] What is more worrying is the introduction of automated and AI technologies into the home environment,[143] as autonomy and independence in the home is surrendered in the face of technological control.[144] Smart home systems will soon make decisions or act as proxies for their owners.[145] It will be no surprise if a resident's Google Home or Amazon Alexa starts to doubt or correct shopping decisions at home based on the data collected from the home environment and related sources.

Furthermore, definitions of liability, accountability, and trespass should be reconsidered for the sake of home protection in changed home environments. Liability and accountability are particularly difficult, given the involvement of automation technology and complex data flow management. In the case of any data breaches,

---

141. AARON PERZANOWSKI & JASON SCHULTZ, THE END OF OWNERSHIP: PERSONAL PROPERTY IN THE DIGITAL ECONOMY 4 (Laura DeNardis & Michael Zimmer eds., 1st ed. 2016).

142. *Id.* at 11.

143. "Fine grained, sub-conscious and personalized levels of algorithmic persuasion may have significant effects on the cognitive autonomy of individuals and their right to form opinions and take independent decisions." COUNCIL OF EUR., DECLARATION BY THE COMMITTEE OF MINISTERS ON THE MANIPULATIVE CAPABILITIES OF ALGORITHMIC PROCESSES (2019), https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168092dd4b.

144. Charlie Wilson, Tom Hargreaves & Richard Hauxwell-Baldwin, *Benefits and Risks of Smart Home Technologies*, 103 ENERGY POL'Y 72, 82 (2017).

145. BARNARD-WILLS ET. AL., *supra* note 55, at 49.

privacy invasion, and technology-related incidents within the home, it becomes difficult to identify the source of the problem and to attribute responsibility to the responsible actors. In the smart home environment, liability and accountability are not clearly allocated among products and service providers.[146] Additional consent problems arise with respect to guests within the home when residents allow them to access HANs. Anytime they are near the same HAN in the future (nowadays mostly dependent on Wi-Fi), they will gain access by default unless the HAN manager changes the password; they can thereby access the resident's home virtually without entering it physically. In this case, permission to access the HVS may only be intended to allow for a single entry, and thus whether subsequently entering the home in this way is a "trespass" should be legally reconsidered. Current law may need to redefine device and service providers' legal status when they have almost permanent presence in the home. This definition must reflect what legal role we assign to providers—do we conceptualize them as guests, landlords, permanent builders or maintainers, or mere delivery men?

III. UPGRADING AND RECONCEPTUALIZING HOME PROTECTION

In this changed home environment, a "bright line" rule for protecting the home only insofar as it exists at the doorstep of physical residence is insufficient to protect the traditional locus of privacy from technological encroachment in a networked world, in which technology and social behavior are co-evolving. [147] As Ducich observed, though property plays a constructive role as a means of articulating what is secured by the Fourth Amendment, the traditional means for home protection based on physical trespass (and physical boundaries) is inappropriate in a smart world. [148] Strandburg rightly pointed out that "a future is nearly upon us that will make it impossible to preserve the privacy even of traditional Fourth Amendment bastions, such as the home, without considering the intervened effects of technological and social change." [149]

---

146. The vague, intertwined notion of responsibility for cybersecurity in smart homes provides a good example. Most smart home devices are fixed function devices; thus, once deployed, they cannot be upgraded to add security fixes unless the device manufacturer provides an upgrade. End users cannot buy security software from a third party. Though security responsibility falls on the original equipment manufacturers (OEMs) that build the devices, they push off the responsibility to the operating system (OS) vendor, arguing that the OS is responsible for the security of the device. Alan Grau, *Security for the Smart Home – Who is Responsible?*, ICON LABS, https://www.iconlabs.com/prod/security-smart-home-%E2%80%93-who-responsible (last visited Apr. 30, 2019).

147. Strandburg, *supra* note 132, at 621.

148. Ducich, *supra* note 127, at 294.

149. Strandburg, *supra* note132, at 619.

There is a strong need for certainty and predictability regarding this point of law. Thus, though many may criticize Justice Scalia's re-emphasis on the importance of property in privacy jurisprudence in *Jones*, we may understand this approach as "re-anchoring" Fourth Amendment privacy protection in the physical world to "survive modern dependence on smart technologies."[150]

As we have seen, "home" is not a fixed term. Some jurisdictions have extended the traditional "home protection" to various non-home places. As discussed, the ECtHR has extended home privacy protection to many traditional non-home spaces/places, such as business premises, hotel rooms, a company's registered office, branches, and even legal persons; such extension acknowledges that many very "private" activities that used to happen solely in the home now also occur in other places.[151] So far, however, courts protect only the physical space of the home, but not any parts of the affiliated HVS. Although the court of Justice of European Union (CJEU) opposed ECtHR's broad understanding of the concept of the home, it has finally extended the right to respect for the home to measures taken by state authorities in the business premises of companies.[152] In an exceptional but less relevant case, the CJEU recognized the legitimate interest of a resident's use of CCTV installed at home to monitor and protect the property, health and life of the home owners; however, it ultimately concluded that the fact that the CCTV was also monitoring a nearby public space excluded its monitoring from being "a purely personal or household activity."[153] Similarly, the U.S. Supreme Court has extended the protection of the Fourth Amendment, for which the home is undoubtedly the quintessential arena, to residences other than permanent homes, and to an individual's office.[154]

Neither the CJEU nor the U.S. Supreme Court has yet offered sufficient protection for the changed home environment against escalating non-physical intrusions and invasions. They have not fully extended the concept of the "sanctity of the home" to cover both the home's physical and virtual spaces. In the digital world, the notion of inviolability (and the castle doctrine) is not complete without including protecting the hybrid space of the home. In *United States v.*

---

150. Ducich, *supra* note 127, at 294.

151. *See* Eur. Ct. H.R., *Guide on Article 8*, *supra* note 28, at 74–75. The Eur. Ct. H.R. ruled in *Niemietz v. Germany* that "it may not always be possible to draw precise distinctions, since activities which are related to a profession or business may well be conducted from a person's private residence and activities which are not so related may well be carried on in an office or commercial premises." Niemietz v. Germany, 251 Eur. Ct. H.R. (ser. A) at 30 (1992).

152. STEVE PEERS ET AL., THE EU CHARTER OF FUNDAMENTAL RIGHTS: A COMMENTARY 154 (2014).

153. Case C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů, 2014 EUR-Lex 2428 ¶ 36 (Dec. 11, 2014).

154. Strandburg, *supra* note 132, at 650–52.

White, for instance, the Supreme Court narrowly held that "a government informant could permissibly wear a wire to transmit conversations to police agents," even when "the conversations took place in the defendant's home."[155] However, "this led a number of states to take more protective positions. . .under their state constitutional provisions," as Strandburg pointed out, in particular "requiring a warrant for electronic monitoring of conversations with an informant or undercover agent" for in-home conversations.[156] Though an informant or undercover agent can wear a wire under the court's case law, what she can do in a suspect's home "is circumscribed by the scope of that individual's consent to the informant's presence".[157] Another example is tracking a person's geo-location inside the home. This is certainly an intrusion when one's cellphone location data is acquired,[158] but many jurisdictions do not specify safeguards on location tracking in police actions in the home context.[159]

Further, recent research also shows that when police hack targeted data stored on a home computer or access a user's computer behavior, constitutional home protection in many jurisdictions "appears to be less relevant as the standard of protection".[160] In contrast, the home as a legal proxy provides very strong protection where a penetrated computer is hacked as a tool by police to monitor behaviors in the physical home, such as by turning on the microphone or the webcam.[161] Data within the home thus lacks the equivalent constitutional protection given to traditional home assets (such as diaries and personal documents) in the search and seizure context.[162] It is questionable why a personal computer, *as a home digital asset and a part of the HAN*, is not entitled to equivalent protection within the home; why it cannot be more protected within the home than it is in other places, and what the underlying rationale for the differentiated legal treatment is. When people bring computers and other digital devices into their home, their expectation of better protection than they would receive at

155. *Id.* at 653.

156. *Id.*

157. *Id.* at 654.

158. *See* Bert-Jaap Koops, Bryce Clayton Newell & Ivan Škorvánek, *Location Tracking by Police: The Regulation of 'Tireless and Absolute Surveillance'*, 9 U.C. IRVINE L. REV. 635, 687 (2018) (citing Filippo Raffaele Dinacci, *Localizzazione Attraverso celle Telefoniche*, *in* LE INDAGINI ATIPICHE 369 (Adolfo Scalfati ed., 2014)).

159. *Id.*

160. Škorvánek et al., *supra* note 10, at 55.

161. *Id.* at 54–55.

162. "[T]he home remains the pinnacle of Fourth Amendment protection under both the property and privacy paradigms." Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 145 YALE L.J. 946, 950 (2016).

public places, such as in coffee shops and airport halls, should not be dismissed.

A more worrisome problem comes from the hidden but ubiquitous presence of network services and devices providers that need to connect with the home to organize the HAN and maintain services, thereby continuously monitoring the home. "The time is fast approaching when it will be impossible to understand what happens at home without understanding the way in which home environment is intertwined with the digital world and hence with third party servers."[163] Once devices are present, residents cannot prohibit interference for maintenance and security reasons. They are largely unaware of how (and where) their home-generated data are stored and processed, or whether they are sent to unwanted third parties.[164] Even worse, as Fairfield argues, residents enter "the new digital serfdom,"[165] in which (1) present contractual obligations cannot hold data abusers accountable, especially when they exist in foreign jurisdictions; and (2) property law and IP licensing systems cannot properly protect our digital home assets (data) or even hard devices from abuse or misuse. As for new digital assets (including both devices and software) at home, current copyright law and IP licensing rules have gradually eroded the owner's control, thereby contributing to loss of control of the home. [166] As for home-generated data, contractual data protection and privacy clauses cannot play an equally strong role as can physical walls in fending off unintended collection and processing. "Home as locus-of-information-generation must trump home as means-of-information-protection," and "[w]e must find rules that protect the information-generative functions of homes by protecting the information they produce," because the *ability* to gather information does not imply the *right* to gather that information.[167] We must consider (1) when home-generated data should be protected at home "by default"; and (2) whether such data should be equally protected when it exists outside the physical home.

Under the current legal framework, the increasing network connection of the home with the outside world turns the virtual part of the home into the weakest point of modern home protection law,

---

163. Strandburg, *supra* note 132, at 657.

164. For instance, Amazon's smart home device Echo reportedly wrongly picked up the owner's private conversation and sent it to a random contact. *See* Gary Horcher, *Woman Says Her Amazon Device Recorded Private Conversation, Sent It Out to Random Contact*, KIRO 7 (May 25, 2018, 9:29 PM), https://www.kiro7.com/news/local/woman-says-her-amazon-device-recorded-private-conversation-sent-it-out-to-random-contact/755507974.

165. FAIRFIELD, *supra* note 22.

166. As Fairfield eloquently points out, IP licensing and property law have eaten up ownership and property rights in the digital world and trapped us in digital serfdom. *Id.* at 4–5.

167. *Id.* at 129-130.

as there are no firm, clearly established boundaries and instruments for its protection. In general, the current legal framework has not yet recognized the HVS as a "formal" part of the home that merits equal protection. Scholars have proposed different approaches to adjust the law to the new generation of the home, as characterized by deepening connectedness, smartization, digitalization and automation.

First, Fairfield takes a systematic approach. He suggests returning in part to the traditional concept of property (with full ownership and strong user rights),[168] and reducing the overreach of the current intellectual property rights. He argues that this will foster "growth of theories of actual old-fashioned ownership interests in intangible property of all sorts," and develop "a freestanding theory of information-based property."[169] However, extending property rights to personal data and personal information is currently problematic. In practice, without continuous professional help—in particular service and maintenance support—residents cannot manage and run increasingly sophisticated smart devices and services in the home environment. Further, the proposed legal changes would fundamentally overhaul the whole data-driven economy and its related power structure; and would not be feasible in the near future. Further, stronger property protection may sometimes be effective, but "all information is not property"; "propertizing" information is hard, and using property to provide additional downstream control for data is dangerous.[170] It is also notable that property rights, at present, are not the true baseline of home protection under many circumstances, even in the physical world. For instance, tenants and other home visitors can be well protected under the home-castle doctrine against unwanted external intrusion without full property rights.

Second, Ferguson and others suggest interpretation or reconceptualization of the concept of "curtilage." They propose extending Fourth Amendment protection of curtilage beyond the exterior walls of the house to cell phones and cell site location information (CSLI) under the concept of "digital curtilage" or "informational curtilage." As a traditional legal concept in common law, curtilage was used to protect surrounding areas of the home and activities that may technically fall outside of it.[171] Curtilage covers

---

168. To free smart and digital property ownership from interference, Fairfield argues to have for new recognized rights to hack (tinker), to sell, to run, and to ban. *See id.* at 186–235.

169. *Id.* at 243.

170. *Id.* at 159–60.

171. Andrew Guthrie Ferguson, *The Smart Fourth Amendment*, 102 CORNELL L. REV. 547, 609 (2017). For a more detailed discussion of curtilage in common law history and theory, see Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283, 1307–27 (2013)

"an area … immediately surrounding [a] house … which we have held enjoys protection as part of the home itself,"[172] and secures the area from outside interference or observation.[173] For Keffer, this means that "the CSLI data becomes the *digital* curtilage of the cell phone, or an effect of my effect (i.e., a cell phone's CSLI data as an effect of an effect or digital papers created by an effect)."[174] For Ferguson, curtilage is a mature legal framework that addresses the definitional and security questions proposed by IoTs.[175] Digital curtilage protects stored data and certain communications signals that are closely associated with stored data, with the effect that they have been marked out and claimed as secure and are used to promote personal autonomy, family, self-expression, and association.[176] Ferguson's proposal expands the traditional curtilage from physical home areas to "all of the constitutionally protected interests… and focuses on the informational content not the particular physical space."[177]Ferguson further proposes to take "informational curtilage" as a global theory in the context of the IoT to replace "the physical intrusion/trespass test and the reasonable expectation of privacy test currently in use".[178]

This approach is valuable and offers a practical way to incorporate the digital reality, but not without risk. It has a conceptual problem in the context of *home* protection, as curtilage may be used to protect digital data and signals that exist outside the traditional home space and place. If the protected data and signals physically exist within the traditional home space, then they are already part of the traditional home and should not need to be understood as "curtilage." Further, if this new property concept covers data and signals outside the traditional home, such as mobile phone data in public spaces, then curtilage is interpreted in *such* a broad way that it strays too far from its original meaning. Such an extension radically expands the understanding of the "home" in most communities. As Ferguson himself points out, "The protection of curtilage exists not because curtilage looks like a home, or is bounded by the walls of the home, but because *it provides a space to act like a home*."[179]

(arguing for a theory of personal curtilage in public under the Fourth Amendment to protect personal space).

172. Florida v. Jardines, 569 U.S. 1, 5–6 (2013).

173. *See* United States v. Romano, 388 F. Supp. 101, 104 n.4 (E.D. Pa. 1975).

174. Scott Keffer, *Too Big to Surveil: The Fourth Amendment Illuminated by 'Modern Lights' and Shadowed by* Obsta Principiis *in a Post-*Carpenter *World Concerned with Privacy*, 28 INFO. & COMM. TECH. L. 161, 181 (2019).

175. Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. L. REV. 805, 809 (2016).

176. *Id.* at 809–10.

177. Ferguson, *supra* note 173, at 618.

178. *Id.* at 617.

179. Ferguson, *supra* note 177, at 859 (emphasis added).

On this point, first, the key issue is the distinction between "home protection" and "the home." Digital data and signals that are not generated in or that do not exist in the physical home space can sometimes be granted "home protection" if necessary; however, they are not part of "the home," and are not necessarily protected *as* though they are the home, even under the concept of "curtilage." In contrast, assets inside and data generated *within* the physical home are part of the modern home —in particular, part of the HVS—and thus always merit full "home protection." Even further, in U.S. Supreme Court case law, curtilage was oftentimes treated as part of "the home," as evidenced in the famous case *Florida v. Jardines.* Justice Scalia ruled that "[t]he officers were gathering information in an area belonging to Jardines and immediately surrounding his house in the curtilage of the house, which we have held *enjoys protection as part of the home itself*."[180] An interpretation of curtilage that expands "the home" into all digital scenarios has deviated too far from its original meaning and attendant association with the home and home area. This broad interpretation will certainly dilute the legal justification for strong home protection.

In a similar vein, one may propose to use a new term "digital home" to cover all digital devices (as physical containers) and virtual spaces (including data and/or networks) that need equal "home protection" because of their significance in privacy and security protection. This approach could broadly cover mobile appliances (such as smartphones, tablets, computers, etc.), cloud services, and even social networking services. In reality, it covers three essential elements. First, it includes the entities that are already in the physical space and place of the home. Second, it may include mobile entities connected to the traditional home or to a virtual extension of home at all times, even if they are not physically present. For instance, smartphones and smart cars are not always at home but can always be virtually connected to the HVS.[181] Third, it may include entities that have nothing to do with the traditional home, but are so important that they should be granted "home protection" regardless, in order to protect private life. On the face of it, this approach is promising because it recognizes the digital reality that smartphones and cloud spaces often contain the most private and sensitive information. However, as this approach is disconnected from the physical reality of "the home", it will harm the constitutional right to home protection. Human life is, and will continue to be, mostly based in the physical world, although a considerable part may shift to virtual spaces. In most cases, people

180. Florida v. Jardines, 569 U.S. 1, 5–6 (2013) (emphasis added).

181. Nowadays, smartphones have many functionalities and can contain, in digital form, many sensitive records previously found in the home, as well as a broad array of private information never found in a home in any form. *See* Riley v. California, 573 U.S. 373, 396–97 (2014).

still live in their physical homes and store most of their valuables in the traditional, physical home, even in digital forms.[182] Granting home protection to cloud spaces and smartphones (when not at home) will diminish the legal concept of the sanctity and integrity of home, a concept that has a strong legal tradition and that has played a critical role in protecting individuals against unwanted interference. In sum, to regain control and protection of the modern home, it is important to distinguish the much-demanded "home protection" from the concept of "the home."

As the ECtHR's extension of home protection already indicates, extending "home protection" to non-home spaces like business premises may both dilute the level of protection for privacy and other important values and obstruct the original meaning of "the home" as a legal concept. As a matter of fact, a reasonable person will *not* expect the same level of privacy protection in business premises (even in her own office) and other non-home places as she would in her own home. This is simply because she will expect a need to regulate her behavior in a setting outside of the private home environment.[183] Privacy and private life in non-home places and spaces, including personal data, should be subject to legal instruments like confidentiality law and contract law. The concept of the "digital home" thus does award different levels of home protection according to the geo-locations of protected data and devices. In reality, however, there is a difference between home and non-home spaces, and a *reasonable person* should understand that devices and data are in different environments when in the home or workspace.[184]

Last and most importantly, physical locations can dramatically impact virtual spaces. Meaningful connections between a physical space and the associated virtual space always exist. Even today, a physical location may be the decisive factor in identifying the nature of the associated virtual space and data. In terms of legal privacy and security protection, HVS should be better protected than the virtual space in a public pub or coffee shop with semi-public Wi-Fi networks. Here, no one can offer a person legal "home protection",

---

182. It is clearly reasonable to keep the most valuable, important digital documents and information at home computer (or storage) due to the strong legal/physical protection of home than in one's office or other non-home places.

183. They will engage in the proper role-playing to adhere to "main theme" of a social setting. *See* Bo Zhao, *Exposure and Concealment in Digitalized Public Spaces*, *in* PRIVACY IN PUBLIC SPACE: CONCEPTUAL AND REGULATORY CHALLENGES 139 (Tjerk Timan et al. eds. 2017).

184. As a common law fiction, the term "reasonable person" refers to a hypothetical person who exercises average care, skill, and judgment in conduct and serves as a comparative standard for determining liability. The fiction has played a critical role in many different aspects of private law, criminal law, and even public law. *See* Mayo Moran, *The Reasonable Person: A Conceptual Biography*, 14 LEWIS & CLARK L. REV. 1233 (2010).

even if she is accessing data present at or downloaded from her HVS via a laptop. The nature of the physical space and place is more decisive a factor than the nature of the protected digital contents in defining due legal protection. Another example can be found in the context of police hacking. Many may argue that in practice, police have difficulty determining the exact point where hacking happens inside a home. Technically speaking, however, many IP addresses are associated with specific private homes and can be well distinguished from non-private IP addresses with geo-location data.[185] Thus, the geo-location of a physical entry point (e.g., a home IP address) can be a determine whether a virtual space is located in "the home," in the sense that entering or leaving that entry point means leaving or leaving the HVS.

IV. HOME 2.0: RE-EMPHASIZING HOME PHYSICALITY

A more moderate, applicable concept of home protection is *Home 2.0*. More extensive than the traditional home, it encompasses both the traditional physical space and the newly developed HVS, based on physical home boundaries. Home 2.0 can recognizes the new home environment by anchoring the HVS in the traditional physicality of the home and thus in traditional home protection law. This requires that in addition to the traditional home protection that contemporary law provides, the law also protects virtual spaces co-existing within the physical space of home. This best coordinates the two different spaces by anchoring the new HVS to the traditional home's location in the physical world. Thus, Home 2.0 covers all entities, both physical and virtual, existing within the traditional home already protected by the current law—namely, the space, place, and things within the four walls of a dwelling house, as well as the home curtilage. Home 2.0 does not extend its boundaries to virtual spaces *outside* the traditional physical home space and place, such as clouds or servers of services providers. The virtual space of the home (networking, whether wireless or wired) should be dependent on HAN(s) (whether accessible from the outside or not), and thus have a *physical address* at the HAN(s). Therefore, although the Wi-Fi signal from a resident's neighbor is strong, and the resident

185. Tracking a person's IP address using simple tracking tools may lead straight to her front door, and police may legally acquire specific information from ISPs. *See How Your IP Address Could Lead Anyone to Your Front Door*, WHAT IS MY IP ADDRESS, https://whatismyipaddress.com/find-me (last visited Nov. 25, 2019). Most home IP addresses are fixed for a period of months or even years, although ISPs are supposed to ensure they are dynamic. As such, a physical location is often connected to an assigned home IP address. *See How Long Does an IP Address Stay Attached to a Home or Business?*, EL TORO, https://www.eltoro.com/how-long-does-an-ip-address-stay-attached-to-a-home-or-business/ (last visited Nov. 25, 2019).

may thereby access their HAN, it is not part of the resident's home virtual space.

The Home 2.0 concept has a few key legal implications. First, law enforcement agents should be expected to acquire a warrant or permission for the purpose of search and seizure, regardless of whether their entry into the home is physical or virtual. Devices and digital assets, whether or not they are smart, automated, or networked, should all equally be protected under the legal standard of "home protection," as long as they are within the physical home or connected to HANs within the physical home space. Second, data generated at home will not be protected *as part of the home* once they "leave the physical home." This will avoid radical expansion of the scope of "the home", which may dilute the legal sanctity of the home as discussed in the previous Section. Virtual boundaries of the home currently defined under contract law between residents and device providers (via contractual data and privacy protection clauses) should be stricter; home-generated data unnecessary for HVS maintenance and operation should not be collected, transferred and further processed outside of the home space, especially by unknown, unconsented third parties. Third, all data flowing outside of the home should be tagged as "home data" and should deserve a special kind of "home protection," meaning that a warrant should be needed for access even if they are in the storage of service providers. In addition, such data should not be shared with non-contractual third parties as sensitive home data, unless necessary or with further consent from data subjects on a case-by-case basis. While the data has left the home space and place and is thus no longer part of "the home," it still merits *home protection*. Fourth, technically speaking, this also means that any smart devices and network devices deployed at home should be legally separated from non-home devices and services, so that they meet higher privacy protection standards (e.g., Security by Design, or other higher industrial standards). More specifically, smart home devices and services providers should "design [and build] their products [and services] around the customer's ability to control their own data."[186]

Thus, a further, feasible step to upgrade home protection would be to assign each home a fixed virtual address (static IP address) to label the HVS, demarcating it from other non-home places and spaces for special legal protection. Geo-fenced IoT devices are a telling example. A special software program can create virtual boundaries using GPS or other means to define a geographical area. Geo-fencing technology thus can tie a device to physical geography, so that the geo-fenced devices or apps may function only within certain GPS parameters.[187] For instance, Yik Yak, a collegiate gossip

186. Zhao, *supra* note 16.

187. FAIRFIELD, *supra* note 22, at 71.

app, offered to geo-fence the app off from any institution that requested it, so that if a user entered the geo-fenced area, the app would stop working.[188] In this sense, geo-fencing technology can be used to protect the home by creating protected home areas based on GPS parameters.

One of the biggest advantages of the Home 2.0 approach is that it best reflects and adapts to the largely changed home environment, a hybrid space characterized by mixed reality, with information associated with physical assets and physical assets connected to virtual space. The concept will not eliminate the traditional home protection proxy, home physical assets and spaces, but will instead effectively combine them with the new HVS. If the current law does not provide sufficient protection for the HVS and mixed reality, home as a legal concept and the related concept of "home protection" cannot protect an important part of the modern home with ever-growing significance. Further, another advantage of this approach lies in the legal certainty and predictability that it provides. The traditional home concept would continue to exist —which remains a reality of life—and the law would protect the added HVS and its interaction with the physical home space. Thus Home 2.0 can revitalize home protection in the IoT age by both recognizing the new HVS as *a formal part of the home* under the current legal framework, and by retaining the traditional home concept and strong home protection traditions with continuous legal certainty and predictability at an uncertain time, when numerous new technologies are revolutionizing our home and home life.

188. *Id.*