European Journal of Law and Technology, Vol 12 No.1 (2021)

EJLT European Journal of Law and Technology

# Seeking Legal Boundaries of Digital Home in the IOT Age: A Conceptual Reflection

**Bo Zhao**[1]

## Abstract

Home has a special status in human private life and modern law. Recent technological developments like increasing digitalization, connectivity, smartization, and automation, have made fundamental changes to our home environments and home life. What appears before us now is not only a perpetually digitally connected hybrid home that is totally different than a traditional home, but also, a possible digital home that only exists in virtual spaces and can in many ways function as a traditional physical home.

However, there appears to be no clearly defined (virtual) home boundaries that can function like a traditional proxy to define the boundaries of the digital home in law, continuing to protect the sanctity and inviolability of the home as before, which leads to uncertainty in current law. It has become critically important to find new feasible home boundaries that can separate the digital home from the outside world.

The paper argues that a pure 'digital home' that is geo-location free and device independent can be possible and may exist in the online environment in view of the quick deployment of cloud computing and IoT technologies. This digital home as a virtual container is characterized by mobile, mosaic and individual (private) nature, spreading over the internet, and thus differs much from the modern home configurations.

New home (virtual) boundaries that can play the role of legal proxy include some key security measures used by home occupants (at the moment) to exercise control over the virtual home space (cross-platform, cross-service), such as identification and authentication measures associated with the home occupants' service accounts, as well as encryption, and firewalls under certain conditions. It argues that it is the best to grant 'home protection' to the digital home for the time being under the current legal home

[1] Senior Research Fellow, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University School of Law, the Netherlands (s.b.zhao@uvt.nl). The author would like to thank Dr. Silvia de Conca at TILT for her comments at the Digital Legal Talks 2020, and the journal reviewers' valuable advice. Special thanks to Lucas E. Jones at TILT and my friend Bryce Newell at the University of Oregon School of Journalism and Communication for their suggestions and editorial work to get this paper in the best shape.

protection framework, rather than formally accepting the new home concept which is still immature in view of current technological developments.

**Keywords:** Digital Home, Home Protection, Home Boundaries, Legal Proxy, Geo-Location Free, Device, Independent.

## 1. Introduction

Home has a special status in human private life and modern law. Recent technological developments, namely increasing digitalization, connectivity, smartization, and automation, have made fundamental changes to our home environments and home life. What appears before us now is a perpetually digitally connected, hybrid home that is totally different than a traditional home.

First, the home now contains an extra space, a virtual space, which is set up on home-based networks (wired or wireless) - that we might call HVS (Home Virtual Space) - functioning as the backbone of home activities and management. The hybrid nature of the new home environment has largely blurred the boundaries of the traditional home. Second, the home can be accessed and controlled from the outside (e.g., smart heating and security systems). Third, home occupants can connect to any points on the internet across the world without physically leaving the home, thus *'participating'* in public activities from home. Fourth, many traditional home assets that were kept at home before (such as photo albums and music records) are digitalized and can be moved and stored outside the home, meanwhile a considerable number of new home digital assets and properties have been created and moved, both inbound and outbound through the physical walls of the home.[2]

Not only can *'bricks and mortar'* efficiently protect home occupants and separate the most private aspects of the home from public space, but walls, fences, and doors can also be used as legal proxies to clearly delineate home boundaries to protect the home from physical trespass.[3] However, our digitally connected homes have become rather vulnerable to various network-based intrusions,[4] when the home (as a hybrid of both physical and digital space) can be reached from the outside without obvious physical penetration.

[2] For a detailed discussion of the fundamental changes of home and home life, see a sister paper from the author: Bo Zhao, 'Unravelling Home Protection in the IoT Age' (2020) 21 The Columbia Science and Technology Law Review <https://journals.library.columbia.edu/index.php/stlr/article/view/4876> accessed 25 March 2020.

[3] In the US law, for instance, 'trespass case law reflects the strong default presumption of the home: the slightest overstep or intrusion into home, or even just entry based on false pretences, has been held to be a trespass.' See: Orin S Kerr, 'Norms of Computer Trespass' 116 Columbia Law Review 1150 <https://columbialawreview.org/content/norms-of-computer-trespass/> accessed 14 July 2020.

[4] Virtual intrusions include various hacking events, and, most importantly, widespread capital and government surveillance. For instance, the robust Fourth Amendment home protection of the US constitution may not well adjust to the new digital home environment in the context of law enforcement activities. See: Andrew Guthrie Ferguson, 'The Smart Fourth Amendment' (2017) 102 Cornell Law Review <https://papers.ssrn.com/abstract=2752788> accessed 26 November 2018;

There appears to be no clearly defined (virtual) home boundaries that can function like a traditional proxy to define the boundaries of the home in law, continuing to protect the sanctity and inviolability of the home as before. *'That our walls are dense and deep is of no importance now because the boundaries that define the very experience of home are to be erased.'*[5] The uncertainty in home protection comes from a combination of the following two factors.

Firstly, the fact that the home is a different space and place, a hybrid space, and thus the home boundaries that are well recognized in current law cannot be used to protect the virtual space of home. Secondly, there is conceptual ambiguity with regard to *'digital home'* as the new term gains popularity nowadays. The legal uncertainty as to virtual home boundaries may lead to negative legal consequences in contrast to the current robust legal protection for physical homes in most western jurisdictions as seen in the home castle doctrine.

Consequently, it has become critically important to find feasible home boundaries within legal doctrine that can separate the virtual home from the outside world.[6] Doing this will help clarify the legal uncertainties that exist under current legal frameworks for home protection and upgrade traditional home protection so that it adequately encompasses new home environments.[7] This paper seeks to: a) conceptualize the digital home by reviewing the recent tech-legal developments (mainly the US and EU), b) find feasible virtual boundaries of the digital home that may extend traditional home protection to the extended virtual space, and c) further reflect on the difficulty that contemporary law confronts in coping with the growing conflict between virtuality and physicality, through the lens of the home-protection case.

The paper argues that a pure 'digital home' that is geo-location free and device independent, can be possible, and, may exist in the online environment in view of the quick deployment of cloud computing and IoT technologies. This digital home as a virtual

Andrew Guthrie Ferguson, 'Personal Curtilage: Fourth Amendment Security in Public' (2013) 55 William & Mary Law Review; Orin S Kerr, 'Searches and Seizures in a Digital World' (2005) 119 Harvard Law Review 531; Katherine Strandburg, 'Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change' (2011) 70 Maryland Law Review 614.

[5] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019) 478.

[6] With new technologies introduced into home environment to perform different functions such as health care, there is also the need to mark personal boundaries among home occupants in terms of data flows even inside the home space. See: Alison Burrows, David Coyle and Rachael Gooberman-Hill, 'Privacy, Boundaries and Smart Homes for Health: An Ethnographic Study' (2018) 50 Health & Place 112.

[7] In current trespass law, for instance, it is still difficult to define what is 'digital trespass' in the law enforcement context, e.g., hacking, installing malware, monitoring home devices from the outside (of home), and other aggressive activities against house-held activities. For instance Cook defined digital trespass as 'sending a targeted electronic signal that causes a device to take an action. This action could be sending information back to the government or changing how the device functions for the user.' Hannah Cook, '(Digital) Trespass: What's Old Is New Again' (Social Science Research Network 2017) SSRN Scholarly Paper ID 2923211 1 <https://papers.ssrn.com/abstract=2923211> accessed 15 July 2020.

container is characterized by mobile, mosaic and individual (private) nature, spreading over the internet, and thus differs much from the modern home configurations. New home (virtual) boundaries that can play the role of legal proxy include some key security measures used by home occupants (at the moment) to exercise control over the virtual home space (cross-platform, cross-service), such as identification and authentication measures associated with the home occupants' service accounts, as well as encryption and firewalls under certain conditions.

This paper is both descriptive and reflective. Based on recent publications in the field, I review the most recent tech developments related to the home environment and how they change home life, as well as challenges to the legal protection of home. The paper is reflective because it tries to address one of the most significant challenges: the blurring of home boundaries in the expansion of home space and place to non-physical places and spaces, which makes the current legal protection of home problematic and underinclusive. It is structured as follows.

Section 2 will first briefly explain home and home boundaries in contemporary law. Section 3 discusses how the home and home life have been fundamentally changed by recent technological advances, and why finding new home boundaries for home protection has become critical and difficult. It will discuss two conceptions of digital home and the scope and possible boundaries of each that can be used as proper legal proxies for future home protection. Section 4 will reflect on the concept of the digital home in a larger context and discuss potential ways forward.

## 2. Home and home boundaries in the law

*'Home is our school of intimacy, where we first learn to be human.'* [8] The central role of home in private and family life in modern society is beyond doubt and beyond words. *'The home is many people's greatest property asset and most private place'* [9] Most jurisdictions have established special legal frameworks to protect the home, as well witnessed in the long-standing common law maxim *'My home is my castle',* and the inviolability of the home doctrine in many European constitutions. Home is the centre of private and family life, and thus has received specific, robust protection in most jurisdictions. The sanctity of home is well recognized in common law countries,[10] as is the inviolability of the home in continental European countries.[11]

[8] Zuboff, *The Age of Surveillance Capitalism* 476.

[9] Joshua AT Fairfield, Owned: Property, Privacy, And The New Digital Serfdom (Cambridge University Press 2017) 104.

[10] As observed in the home-castle doctrine. For a full discussion, see: Jonathan Hafetz, 'A Man's Home Is His Castle?': Reflections on the Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries' (2002) 8 William & Mary Journal of Race, Gender, and Social Justice 180–84 <https://scholarship.law.wm.edu/wmjowl/vol8/iss2/2/> accessed 6 August 2019.

[11] Further, the inviolability of home is equally protected under Art. 13 of the German Basic Law, and Art. 50 of the constitutional law of Poland. See respectively: Ivan Škorvánek, 'Privacy Crimes in Poland'

For example, at the constitutional level, the Fourth Amendment of the US Constitution protects the sanctity of home; Article 7 of the European Charter of Fundamental Rights and Article 8(1) of the European Convention on Human Rights (ECHR) both protect the right to respect for private and family life and home. This is essentially because home, as a container and legal proxy, works as the host for a constellation of fundamental values and societal goods, i.e., privacy, safety, liberty, autonomy, security, peace of life, freedom of speech, etc.

Home is systematically protected by multiple legal instruments including contract, privacy, trespass, property, tax, family, land, and mortgage law etc.[12] Despite the important role that the legal concept of  home has played in contemporary law, there has not been a broadly accepted definition of home, often defined as dwelling house or dwelling. The varieties in spatial properties and typologies, as well as different lifestyles of home occupants, have led to different understandings of what is a home and what is not.

Under the contemporary law, a home may refer to not only houses, apartments, and single rooms, but also other residential spaces or places such as caravans, hotel rooms, cabins, bungalows, second homes, mobile homes, etc.[13] US law even includes the external, affiliated spaces of dwelling houses, namely curtilage, as part of home under the Fourth Amendment protection.[14] In most common law jurisdictions, the home refers to dwelling houses, meaning a physical entity with identifiable interior and exterior conditions, and a place of security and privacy.[15]*'It is the act of dwelling then in a place/house that makes it spatial, a home.'*[16]

In essence, the concept *'describes a place where someone dwells, lives or resides'* and *'premises will not ordinarily be a dwelling-house unless the tenant sleeps there.'*[17] In short, the home is *'the place where he lives and to which he returns and which forms the centre of his existence.'* [18] For the European Court of Human Rights (ECtHR), home is an autonomous concept that does not depend on classifications under domestic law; it would

(TILT 2017) 8 <http://www.privacyspaces.org/wp-content/uploads/2016/09/Polish-Substantive-draft.pdf>.

[12] Mostly and best protected under property law for owners to exert exclusive control in societal life via spatial boundary lines, as well explained in Merrill and Smith's boundary approach to property. See: Nicholas Blomley, 'The Boundaries of Property: Complexity, Relationality, and Spatiality' (2016) 50 Law & Society Review 224, 220–230.

[13] See respectively: CoE, 'Guide on Article 8 of the ECHR' (December 2018) 56 at: <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf>.

[14] Andrew Guthrie Ferguson, 'Personal Curtilage: Fourth Amendment Security in Public' (2013) 55 William & Mary Law Review 1287.

[15] Kathy Waghorn, 'Home Invasion' (2009) 6 Home Cultures 261, 2.x.

[16] Kathy Waghorn, 'Home Invasion' 22.

[17] Lord Bingham, *Uratep Ventures Limited v. Collins (Ap)*, paras. 10 & 12.

[18] Lord Millett, *Uratep Ventures Limited v. Collins (Ap)*, para. 31.

depend on the factual circumstances, namely, the existence of sufficient and continuous connections with a habitation to attract the protection of Article 8 of the ECHR.[19]

Despite these varieties, the home is both a physical space and place in terms of territoriality.[20] The home is a spatial space located at a physical (geographical) place, *'spatialized by the boundary'*, [21] with physical boundary lines separating it from the outside. In ordinary life, the ideal home is equally taken as dwellings or houses that are constructed with surrounding walls, roof, windows and doors, as well as extended spaces utilized for living purposes. Home spaces are enclosed and marked by physical structure/construction, and the home place refers to the geolocational and physical relationship of the home to other neighbouring spaces/places.[22] Many would extend, if possible, the home space to adjacent garden areas whose boundary lines both separate and connect the home with the outside. *'The home can be viewed as a boundary separating certain types of activities or information...has historically constituted a key boundary separating virtual as well as physical domains, including the public and the private.'*[23]

As Barth pointed out, boundaries literally *'divide territories on the ground'*,' and more abstractly, *'set limits that mark social groups off from each other'* [24] The concept of boundary is binary, delineating one thing from another, creating different spaces. A boundary in the physical dimension is generally *'operationalized as that which distinguishes geographic regions: Human identity, physical or imaginary borders (e.g., fences, rivers, state lines) to separate spatial territories (e.g., yards, states, countries); and the resulting places are then imbued with local or regional rules, conventions and behavioural expectations.'*[25]

In the context of home protection in contemporary law, home boundaries actually mean three things. First, they refer to the boundary lines that can physically mark/demarcate the

[19] Jana GAJDOŠOVÁ, 'Article 8 of ECHR and Its Impact on English Law' (PhD Thesis, University of East Anglia 2008) 112 <https://ueaeprints.uea.ac.uk/10564/1/Thesis_n069532_ARTICLE_8_ECHR_AND_ITS_IMPACT_ON_ENGLISH_LAW_Jana.Gajdosova.pdf>.article

[20] Following Cresswel, a) space has been seen different from place as a realm without meaning, and as a fact of life, produces the basic coordinates for human life; b) when humans invest meaning in a portion of space and become attached in some way, it becomes a place; and c) basically, place 'is space invested with meaning in the context of power, which happens at all scales and throughout human history. Tim Cresswell, *Place: An Introduction* (John Wiley & Sons 2014) 10 & 12.

[21] Nicholas Blomley, 'The Territory of Property' (2016) 40 Progress in Human Geography 593, 40.

[22] As Cresswell pointed out, (geo)location is not a necessary or sufficient condition of a place. Tim Cresswell, *Place: An Introduction* (John Wiley & Sons 2014) 22.

[23] Stuart Shapiro, 'Places and Spaces: The Historical Interaction of Technology, Home, and Privacy' (1998) 14 The Information Society 275, 275.

[24]Anthony Cohen (ed), 'Boundaries and Connections', *Signifying Identities: Anthropological Perspectives on Boundaries and Contested Identities* (Routledge 2000) 17. (Focusing on social identity boundaries).

[25] Guo Zhang and Elin K Jacob, 'Understanding Boundaries: Physical, Epistemological and Virtual Dimensions' (15 September 2013) <http://informationr.net/ir/18-3/colis/paperC21.html#.X2M1zNRS-pc> accessed 17 September 2020.

home space (a column of space) from external non-home space. This function is primarily performed by the physical construction of home in the sense that walls, windows, fences, roof, and even bars divide the home from the outside space with their physical existence and projection, and are thus regarded as home boundaries themselves.[26] Second, some home boundaries can be physical devices that perform an informational, symbolic function, sending clearly *'framed'* messages to the outside world.[27] Such informational boundaries include various (even low) fences, gates, doors, property marks/signs, border plants, wires, trespassing warning signs, etc., by which outsiders can tell where the home boundaries are located. Further, when the physical boundaries protect the home as barriers and obstacles, the informational ones protect the home by resorting to societal norms that are supported by an *'expectation of robust and automatic pre-legal institutions from respondents, confirming a dominant ethic that condemns boundary crossing.'* [28]

Third, home boundaries in the law mean legally recognized boundary lines and markers that help with clarifying rights and duties between home occupants and others. This can be documented in land and property registration, purchase deeds, and rental contracts that formally recognize and confirm the physical boundaries for establishing rights and duties among involved legal persons (e.g., ownership, user rights, passage rights, etc.). For instance, rental contracts can protect tenants from unnecessary disturbance from property owners.[29] Overall, ownership under property law offers home occupants the strongest protection by granting exclusive control and disposition power.[30] As said above, such legal boundaries (in abstract) are established on the physical boundaries (as legal proxy) to protect the home and home affiliated values.[31]

Yet, when the home has been deeply digitalized and connected, with the increasing deployment of IoT and cloud computing technologies, the home and home life have

[26] Boundary marking is their function secondary to providing safety and security by creating a physical shelter to keep out harm and intrusion; afterwards, other functions were further developed e.g., enlightening, air circulation, decoration, and identity formation. See in general: Judith Flanders, *The Making of Home: The 500-Year Story of How Our Houses Became Homes* (Atlantic Books Ltd 2014).
[27] The two terms are borrowed from Blomley's discussion of property boundaries. According to Blomely's empirical research on property boundaries, everyday property boundaries contain the following key elements: a) being an informational device, b) to send a clearly framed message, and c) with expectation of robust and automatic pre-legal institutions conforming to a dominant ethic that condemns boundary crossing. See: Blomley, 'The Boundaries of Property: Complexity, Relationality, and Spatiality' 234–235. Similarly, Firefield pointed out that physical boundaries matter because they are attached 'with critical information to those particular features of the landscape.' See: Joshua AT Fairfield, *Owned: Property, Privacy, And The New Digital Serfdom* (Cambridge University Press 2017) 136.
[28] See: Blomely, 'The Boundaries of Property: Complexity, Relationality, and Spatiality', 234-235.
[29] The construction of home space, as a legal space, belongs to one of the cultural constructions of space as seen in the public-private divide. See: Paul Berman, 'Legal Jurisdiction and the Deterritorialization of Data' [2018] GW Law Faculty Publications & Other Works 664 <https://scholarship.law.gwu.edu/faculty_publications/1331>.
[30] A difficult problem is that home ownership in the near future can be virtually impossible when the home becomes a data warehouse and service center of rising dominating tech corporate power. See in general: Fairfield, *Owned: Property, Privacy, And The New Digital Serfdom.*
[31] This article only focuses on the first two conceptions of home boundaries.

undergone fundamental changes. Accordingly, traditional home boundaries have gradually collapsed, and the home is turned both outside in and inside out when digitally open to the outside world. As Chen and others revealed *'what should be less disputable is the challenge to boundary management… The boundaries of a smart home are remarkably more fluid as smart devices may – and, sometimes indeed, are designed to – transit information about what is happening inside the home to the remote cloud.'*[32] It is necessary to reconsider: to continue protecting the sanctity and inviolability of home in law, where should we draw new home boundaries when 'the home' can exist in a geo-location free, and device independent manner,[33] spreading anywhere in cyberspace, and thus becoming a space of mobile and mosaic nature.

## 3. Which digital home, which boundary?

### *3.1 Recent home developments and the rise of digital home*

In the IoT age, our traditional home and home life have been changed from physical space to hybrid space (and to mixed reality), and from dwelling to smart living.[34] Such changes can be attributed to the increasing home digitalization, connectedness, smartization, and automation. The new home environment is characterized by the rise of Home Virtual Space (HVS), home automation, and many new digital assets such as digitalized and digital files and documents, and home-generated data. The first striking feature is that the modern home is hyper-connected, in a 24/4 manner, to the outside world via networked networks (the internet and cell tower networks, in future 5 G), in addition to physical openings allowed by windows and doors. HVS at the traditional home spaces can be accessed from the outside via multiple connected networks and the new home environment has been increasingly interacting with the external virtual space,[35] when technical supports are a must for security patch, function improvement, and user data processing. The networked connection in a sense opens the home to the external world, partially changing the home's

[32] Jiahong Chen and others, 'Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption' (2020) 10 International Data Privacy Law 279, 289. The authors focused more on the legal responsibilities and legal status of the stake holders in the smart home context under the European data protection framework, in particular the GDPR. They argued that the fluid nature of home boundaries comes from the original design of smart home to a) transit information from home to the outside, b) dependence of home functions on external events, and c)diminishing of trust at home.

[33] Device independent shall not be taken literally to mean that the future digital home will not rely on hard devices any longer. Rather it means that the future digital home will not be fixed to any specific hard devices, but rather may exist and be accessible anywhere with network accessibility.

[34] See in general: Zhao, Unravelling Home Protection in the IoT Age'.

[35] This article defines virtual spaces as 'computer-moderated, persistent environments through and with which multiple individuals may interact simultaneously' (originally Bartle's definition of virtual world) by networked networks, as an alternative non-physical space, in contrast to the real physical space we live in.' See: Wian Erlank, 'Law and Property in Virtual Worlds', *Research Handbook on the Law of Virtual and Augmented Reality* (Edward Elgar Publishing 2018) 638.

nature from a pure private place to a public one (e.g., accommodating a virtual conference).

A second feature of the new home is the growing number of digital effects (e.g., household data) and other digital properties on the Home Area Networks (HANs).[36] In a broader sense, digital properties, according to Firefield, include four types of property: a) any information or data that is stored electronically, whether stored online in the cloud or on a physical device; b) any online accounts, such as email and communications accounts, social media accounts, shopping accounts, etc., c) domain names, and d) intellectual property, including copyrighted materials, trademarks, and any code one write or own. In the new home environment, digital assets accordingly include: a) digitalized traditional home belongings (e.g., scanned photos, papers, documents and books), b) new digital assets created digitally and belonging to the home (e.g., communication data, HAN data, digital bills, purchased software and applications, book drafts, etc.), and c) similar digitally created asserts that are not home relevant, but entered/kept at home (e.g., work related documents and data, and other data from the outside from various sources). The challenging issue with these digital assets is that they can be easily moved (duplicated and transferred) across the new home environment, and thus the traditional physical barriers may not sufficiently protect them without the introduction of digital 'walls and fences' that will be discussed later.

A third feature is the increasing number of mobile devices (containing multiple functioning apps) that are constantly shifting between home and non-home spaces. They can be taken as, at least for a specific moment, part of the home, when connected to the HAN; while at other times, they are not part of the home physically, when used on external networks as part of a larger IoT system. Smartphones and smart cars are good examples in that home occupant's profile and data can be synchronized between the HAN (anytime) and the operating systems, creating private virtual space even when they are outside home, which potentially extends the 'home space' beyond the traditional (physical) home.

A fourth related feature is that in the digitization process, many previously traditional home belongings and assets are not only accessible from the outside of home, but also can be easily moved (or duplicated) to non-physical home spaces. This includes the digital effects such as digital photos, communication data (duplicated digital copies), e-books, digital currencies, music, family files or records, purchased software, etc. Some of them are carried on portable, connected devices, crossing various spaces and places; others are stored on and accessible from various platforms and servers, thus actually distributed to different geo-locations, even globally.

If this is too abstract, Jaap-Henk Hoepman and Bert-Jaap Koops provided a very good example to understand the future digital home, at least partially: the private digital storage spaces, or cloud storage. Such personal digital storage spaces closely resembles *'the home as a storage environment for private things', and can be taken as 'digital home' at least*

[36] Since HANs have become the backbone of modern home and home life. For a discussion of HANs, see: M Sadiku, M Tembely and S Musa, 'Home Area Networks: A Primer' (2017) <https://doi.org/10.23956/IJARCSSE%2FSV7I5%2F208>.

*part of the 'digital home'.*[37] According to the authors, when out-of-home digital storages function equivalently to traditional in-home storages, especially when remote storages are purely for personal use controlled by special encryption arrangement (at least with the theoretical possibilities to perform as storage in the cloud in a certain way, like encryption in combination with a specific hard device, either a laptop or a tablet, using on-device encryption/decryption).[38] This creates the situation that, very much like the home environment, data stored in the digital home can be accessed by others, on the condition that they have physical access to the environment itself (handing over the device to another for access v. open the door for others to enter the storage space at home).[39]

A last, but most important feature is the fact that HANs gradually start to become the backbone of the future home in terms of home management and organization. This is already reflected in the popular use of smart home technologies such as smart energy solutions (smart locks, smart heating, etc.), security measures (smart locks, security cameras, motion sensors, etc.), and voice-enabled devices (Alexa, Google Next, etc.) for home automation. The organization function based on personal data collecting and profiling can also be used outside the home, further in connected cars and other personal devices in traditionally non-home spaces (also via non-private networks such as public Wi-Fi).

The rise of digital home assets and effects (with a portable mobile nature), the growing use of digital mobile devices (especially smartphones), and the networked openness of the traditional home have important consequences. First, it seems that part of the home (i.e., home components and home activities) has been moved outside the traditional home (hereafter Home 1.0) into cyberspace and can be carried around. Second, in the IoT age in which the internet becomes the backbone of daily life, the traditional home can be accessed any time, from almost anywhere (e.g., in case of smart heating, smart security and virtual meeting). These changes have gradually created a home-like virtual environment, a virtual home experience, or a strong home feeling (or sensitivity). This is mostly the case when one can be deeply immersed into a private virtual space, even when physically at a public space like on a train or bus. This sensitivity or feeling is well captured by the term 'privacy bubbles' that purposely separate virtual space from physical space.[40]

The home sensibility has been largely intensified when one can access multiple online spaces to carry out very private activities that were conducted at home before (e.g., chatting, emailing, banking, entertaining, controlling home heating, gaming, feeding home

[37] Jaap-Henk Hoepman and Bert-Jaap Koops, 'Offering 'Home' Protection to Private Digital Storage Spaces' (2020) 17 SCRIPTed 359.

[38] Hoepman and Koops, 'Offering 'Home' Protection to Private Digital Storage Spaces' 379.

[39] Hoepman and Koops, 'Offering 'Home' Protection to Private Digital Storage Spaces' 380.

[40] Delphine Christin and others, 'Privacy Bubbles: User-Centered Privacy Control for Mobile Content Sharing Applications' in Ioannis Askoxylakis, Henrich C Pöhls and Joachim Posegga (eds), *Information Security Theory and Practice. Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems* (Springer 2012) 71–86. Also 'personal bubble' is not just physical, but also virtual. See: Silvio Carta, 'Your Personal Space Is No Longer Physical – It's a Global Network of Data' (*The Conversation*) <http://theconversation.com/your-personal-space-is-no-longer-physical-its-a-global-network-of-data-97140> accessed 24 July 2020.

pets, etc.) despite the real geo-location. This helps create a virtual private space in which one seems to remain private, given that nowadays ordinary people spend considerable time on cyberspace when they are hyper-connected every minute (especially via mobile phones and other portable devices) in the online world.[41]This is especially the case when we are using a few personal accounts to access multiple online services and functions in the context of cloud computing and IoTs. For instance, Google, Apple, and Microsoft accounts can be used to access not only their services, but also other service provider's services as an identification measure (e.g. logging in Dropbox with a Google account). Many applications such as Firefox can be downloaded and used on different devices (desktops, Laptops, tablets, smart phones, etc.) under the same personal accounts. Personalization and synchronization have made it possible for users to access their online accounts from different physical locations and devices, thus providing more solitude, comfort, control, security and safety that are found at the traditional home.[42]

### *3.2 Which digital home?*

In recent years, digital home has become a rather popular concept in the housing industry and interior design sector, since *'The digital home is a rapidly evolving reality all around us'*.[43] From an industrial perspective, DLNA (Digital Living Network Alliance) defines digital home as *'an electronic network made up of PC and mobile devices that cooperate transparently'*, and needs *'interoperability of the three digital islands within the home: the internet, broadband electronic network and the island of mobile devices'*.[44] For Intel, digital home means *'The vision of a home full of connected, interoperable devices that easily exchange and play content is very partially realized'*.[45] The industrial perspective more reflects the technological developments at the home, but overlooks the rise of the HVS that coexists with the physical space (and place) in parallel. The concept is much used, but lacks a common definition among scholars. Digital home has been approached more as an umbrella concept, without any further comprehensive discussion. For instance, Irion's work discussed personal data processing (transfer and storage in cloud computing)

[41] The *on*life world is featured by, among others, the blurring of the distinction between reality and virtuality, and the offline and online existence. See: The Online Initiative, 'The Onlife Manifesto' in Luciano Floridi (ed), *The Onlife Manifesto: Being Human in a Hyperconnected Era* (Springer International Publishing 2015) <https://doi.org/10.1007/978-3-319-04093-6_2> accessed 14 January 2019.

[42] For instance, the extension of the right to respect for home and private life under Article 8 of the ECHR broadly to non-home places such as business premises in ECtHR case law in the law enforcement context. For instance in the *Levau v. France case*. See: Jana GAJDOŠOVÁ, 'Article 8 of ECHR and Its Impact on English Law' (PhD Thesis, University of East Anglia 2008) 109 <https://ueaeprints.uea.ac.uk/10564/1/Thesis_n069532_ARTICLE_8_ECHR_AND_ITS_IMPACT_ON_ENGLISH_LAW_Jana.Gajdosova.pdf>.

[43]'Intel and the Digital Home' (*Intel*) <https://www.intel.com/content/www/us/en/standards/digital-home-case-study.html> accessed 2 July 2020.

[44] Ignacio González Alonso and others, *Service Robotics within the Digital Home: Applications and Future Prospects* (Springer Science & Business Media 2011) 115.

[45] 'Intel and the Digital Home'.

regarding home device use;[46] Fuente and others define digital home (based on UPnP, Universal Plug and Play) as *'conceived to include all wire and wireless networks, entertainment devices, telephonic systems, home control and many more devices.'*[47]

In view of the current home developments, digital home may mean two things. The first, based on the technological reality discussed above, refers to Home 2.0 in comparison to the traditional, physical home (Home 1.0). It refers to the digitally connected traditional home, containing both the conventional physical space, and the new virtual space that is located within the physical home.[48] Though the home can be connected to and interacted with external networks - such as storing digital assets or other digital artefacts – this concept only covers the virtual spaces created within the traditional home space/place, but not the part outside it. This includes any wired and wireless networks at home: Wi-Fi networks, cable networks, or Bluetooth networks, or a hybrid of all. This digital home exists only within the physical home space, and separated physically by routers (with a specific location/address on connected networks) from external networks.[49]

The concept is similar to the industrial perspective, but focusing more on the hybrid nature of the new home environment, with virtual and physical spaces largely overlapped with each other. It is relatively easy to define the virtual boundaries for legal protection. For instance, home IP addresses that are associated with home physical addresses, although dynamic, can single out the home virtual space/place from other virtual spaces to provide home protection. Another good example is the popular use of geo-fencing technologies to prevent home from invasive online activates at some specific geo-locations;[50] for instance, forbidding unwanted commercial advertisements and political campaigns. This means, when associated with the traditional home addresses and home activities, certain IPs and MAC addresses shall be singled out for special home protection.

[46] Kristina Irion, 'Your Digital Home Is No Longer Your Castle: How Cloud Computing Transforms the (Legal) Relationship between Individuals and Their Personal Records' (Social Science Research Network 2015) SSRN Scholarly Paper ID 2628598 <https://papers.ssrn.com/abstract=2628598> accessed 25 July 2020.

[47] María del Pilar Almudena García Fuente, Javier Ramírez de la Pinta and Adrián López García, 'Interoperability Systems' in Ignacio González Alonso and others (eds), *Service Robotics within the Digital Home: Applications and Future Prospects* (Springer Netherlands 2011) 3 <https://doi.org/10.1007/978-94-007-1491-5_1> accessed 24 September 2020.

[48] For a detailed discussion of Home 2.0, see: Zhao, Unravelling Home Protection in the IoT Age'.

[49] In addition to the broadband connection, another option is to create a wireless HAN based on a mobile phone (or a portable device, as a mobile hotspot or Wi-Fi router) connected to a nearby transmitting tower. For this purpose, Mobile IP (MIP) and MAC address (Media Access Control, burned-in address) are used to allow network access and identification.

[50] For marketing purposes, geofencing can be realized on collection of GPS, cellular data and WiFi data (or their combination) to target ideal customers when they are nearby. See: Sam Selders on July 28 and 2020, 'How Does Geofencing Technology Work?' (*WebFX Blog*, 20 September 2019) <https://www.webfx.com/blog/marketing/how-does-geofencing-technology-work/> accessed 11 August 2020.

The second notion of digital home, which is the focus of this article, refers to a totally virtual space that exists only virtually in cyberspace, regardless of physical locations and boundaries; in short, any spaces in cyberspace that can be found as the equivalent of *'the home'*. According to Koops and others, the digital home contain *'...certain networked devices, such as smartphones, and parts of the related cloud ecosystem over which users exercise exclusive rights to control access, which function as an important means to protect their private life and which can be regarded as an equivalent of home in cyberspace.'*[51] The digital home can be taken as a virtual container (or capsule) in the cyber world, equally functioning as the traditional home that accommodates private life. This concept covers a) the virtual part of Home 2.0 (HVS), and b) other virtual spaces (spheres) that are outside the physical home, but accepted by users as *'home'* or *'an equivalent of the traditional home'*, when performing many of the traditional home functions and providing the home feeling.[52] This conception can be understood from the following aspects.

First, the digital home is independent of a specific physical space and place. Although hardware infrastructure and devices are the pre-condition (physical basis), it exists only virtually, following rules of the virtual world (protocols, codes etc.).[53] The digital home is geo-location free, and can be accessed from multiple physical spaces and places, via multiple digital devices (mobile or static), and almost at any time. It is a virtual container, an overarching virtual space, and a constellation of multiple virtual spaces, in which home-associated activities can happen, digital home assets are stored, and home occupants may come and leave at will. With instant connections established, the user can make *'a temporary defined space that can be used to limit the information coming into and leaving the bubble in the digital domain.'*[54]

Second, the digital home is mobile and mosaic in nature, spreading over multiple places and spaces (in the context of cloud computing and IoT), both physically and virtually. The digital home is accessible from different devices and multiple geo-locations, and runs across multiple service platforms (servers), and exists in various digital forms. This means that a home occupant can seemingly take his home with him anywhere, but actually he is accessing different portions of the home in cyberspace, by using authentication and identification measures (e.g., passwords or trusted devices). This is especially the case when users can use one user account (e.g. a Google account) to access multiple services, devices, and functionalities, with the help of synchronization and personalized services. The constant, gapless shift among cross-platform, cross-device services can really make

[51]'PILab-Brief on Home Protection 2.0 - 180619.Pdf,' 2, accessed July 9, 2020, https://pilab.nl/onewebmedia/PILab-brief%20on%20home%20protection%202.0%20-%20180619.pdf.

[52] Logically, a third notion could be the digital reality home in the gaming context, which can be a duplication of real home. See: Yadin Gilad, Beyond unauthorized access, in: Woodrow Barfield and Marc Jonathan Blitz, *Research Handbook on the Law of Virtual and Augmented Reality* (Edward Elgar Publishing 2018) 355.

[53] In short, 'the software and hardware that make cyberspace as it is'. See: Lawrence Lessig, 'Code Is Law' (*Harvard Magazine*, 1 January 2000) <https://harvardmagazine.com/2000/01/code-is-law-html> accessed 26 July 2020.

[54] Barbara Daskala and loannis Maghiros, 'Digital Territories' (2006) <https://ieeexplore.ieee.org/abstract/document/4199398>.

one feel *'at home'*, which accommodates many home functions such as entertainment, learning, communication, self-reflection, control, even cooking (from distance) etc. Amazon, Google, Microsoft, and Huawei are a few examples of such service providers that make effort to provide cross network, cross platform overarching services (or eco-systems) in the forthcoming IoT age. In this sense, as a private virtual space (container), the digital home can be mobile, carried around by a home occupant to different cyberspaces.

Further, this concept of digital home is not comparable to the traditional home in that it is only an imagined space, a virtual bubble, or a virtual *'container'* by analogy. Technically speaking, the owner of the container does not have a real enclosed space like the traditional home, but have the control over certain structured data either being stored on controlled devices (even partially), or in the clouds (in the general sense), or transferred on the internet (data on the go). Chang, Fletcher and others define container as consisting of: *'...a barrier or set of barriers between its contents entities and the outside world. Each barrier has potential points of entry, either physical or virtual, through which users access the contents within it. The degree of the protection provided by a container is measured by how effectively its barrier prevents unauthorized outside parties (users) from gaining access to its contents through those points of entry'*.[55] The virtual home space is protected by cybersecurity measures and other logical rules (as the boundary and points of entry), which will be discussed in the next section.

Third, in light with this, the digital home will be a very private place/sphere. It is more individual-oriented than the traditional, collective home. Most of the time the digital home is not equally shared among family members as in the way similar to how they share the traditional home space. Most adult members (even a husband and wife) will not share their communication data (e.g., email accounts, passwords, and social network accounts) with each other unless necessary. Usually family members with technical capacity manage a family's cyber space on behalf of the whole family. At present, there is no *'digital home'* in cyberspace that duplicates exactly the traditional home with openly shared space for a family. The truth is that as an imagined virtual space, it is enclosed and protected by using different authentication and identification measures, like user IDs and passwords, biometric measures like fingerprint, and encryptions. Thus, they are not usually shared with other family members like in the traditional home, for which keys are duplicated and shared even with younger kids. Under-aged family members are under stricter control (in terms of formal account registration and tech capacity).

Fourth, the digital home is a forward-looking concept under development, very much open to future technological developments in IoTs and cloud computing. What is discussed above as the digital home at this moment is largely individual account/usage based. Thus, it is dubious for many why the individual account based cyber space/sphere would be called as *'the digital home'* against our common sense about what a modern home shall be like. Looking forward, it is rather possible that the digital home can be developed in future as a full duplication of the traditional home, as a virtual space that contains most home

[55] Benjamin Adida and others, 'The Future of Trespass and Property in Cyberspace' <http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall98-papers/trespass/final.html> accessed 18 April 2018.

functionalities, allowing family members to use their own personal accounts by default. For instance, all Google smart home devices can be collectively managed under one family account that grants different user authorities to different family members to enjoy different home services. It is quite possible that when IoTs and 5G will be fully rolled out, the home (digital home) can be anywhere whenever a natural person is connected to do home-related activities; and by then the digital home is defined by the nature of communication data (either family data or personal data). Another option is that future logging in may only use biometric authentication measures (e.g., facial image, fingerprint, and voice) to access networked services that are characterized by profiling and synchronization, resulting in seamless user experiences.

To summarize, this notion of digital home as a virtual space (a container) differs from the traditional, physical home in its mobile, mosaic nature. It may not be fixed to any specific physical, geo-location, or any specific hardware devices (although can be more associated with a few key devices or networks), distributed over cyberspace. The almost seamless switch among multiple network services in the incoming IoT age (especially ambient computing) has made it possible for individuals to *'take the home'* around, regardless of geo-physical location, and to gain the home feeling (in terms of solitude, functionality, peace, safety and comfort), in addition to the transfer of many home asserts and effects and home activities into virtual spaces.

However, this concept is alien to our common understanding of the modern home that refers to a more fixed spatial space/place as the centre of private life. The affiliation of the resident to the home place and space is exclusively recognized by contemporary law for protection.[56] It is dubious whether a space/place that is geolocation free and mosaic can be really regarded as home by law.

### *3.3 Digital home in a larger context*

Against common sense, however, the mobile and mosaic nature of the digital home was a common feature in home history, and can be even found in some modern communities. In human prehistory, for a very long time, our ancestors (earlier starters) modified different geo-places by building fires and simple structures, probably windbreakers, where they made tools and prepared food, and called them home.[57] The archaeological research of hunters and gathers clearly demonstrates that *'the creation of dwellings (camp) was a central innovation'*, allowing humans to range further, exploiting regions and resources inaccessible, and other activities (e.g., burying the dead); further, with more new sets of connections and meanings created, these temporary dwellings '*became a place of*

[56] For instance, , the European Court of Human Rights only protects home under Article 8 of ECHR when the resident has sufficient and continuous links with a residential place as the factual circumstances. See: GAJDOŠOVÁ, 'Article 8 of ECHR and Its Impact on English Law' 112.

[57] Jerry D Moore, *The Prehistory of Home* (First edition, University of California Press 2012) 28. Note that Moore also notice that home places as '(t)hese sites were places of arrival and return.' (30)

*return*'.[58] It is only when technological developments allowed more food provision and personal belongings (durable goods), the home became affiliated to a specific place (although temporary sometimes).

In human history, home was once only a mobile space - dominantly a personal and intimate sphere, not fixed to a specific geo-location (place), a mobile space that could be created and carried around. Home only became a space fixed to a physical place when our ancestors had too much stuff, and sedentism gradually developed even in the absence of agriculture.[59] In modern society, hunters and gatherers of non-sedentary communities, such as Eskimos and African tribes, move their homes to different geo-locations for food supply and other societal activities; for which the home is not anchored to a specific geo-location (place), but to a much larger geographical scope. In both cases, the home is a portable, mobile space. Historically speaking, the prototype of our modern home is only a product of the industrial revolution, and our basic home structure has not much changed since the late 1800s.

Our *'homes and how we live in them is the result of the violent intrusion of science, welfare laws and the industrial and economic needs of the late nineteenth century'*[60] Shapiro observed that home space in the colonial period America had extended far beyond home place with the advances of communication technologies by then.[61] Specifically, newspapers and mail *'created the potential for a new kind of permeability'*, and *'private information originating within the home could become accessible to a wider audience as the private space of sealed letters extended through public places*.*'* [62]

In the information age, as analyzed above, the home has been under significant changes consequent to fast deployment of IoT and ambient computing technologies. The recent trend, namely the mosaic and mobile nature of the digital home, has been reflected in contemporary law development. As Strandburg noted recently, the Fourth Amendment home protection needs to find ways to adapt to the technosocial extension of the Home (and home protection) due to the social significance of new social media and cloud computing, when, for example, one may not know exactly where their home documents (as bits and bytes) are physically stored.[63] And *'these technologies are potentially the technosocial extensions of our homes and offices and like hotel rooms and cartilages, need Fourth Amendment protection'*.[64] The US Supreme Court's ruling in the landmark case Reily (with regard to cell phone search and seizure) reveals some changes in the concept of the modern home: *'a phone not only contains in digital form many sensitive records previously*

[58] Moore *The Prehistory of Home* 41.

[59] Moore *The Prehistory of Home* 51–52.

[60] Alexandra Deschamps-Sonsino, *Smarter Homes: How Technology Will Change Your Home Life* (Apress 2018) XVI.

[61] Shapiro, Places and Spaces: The Historical Interaction of Technology, Home, and Privacy' 278–230.

[62] Shapiro, Places and Spaces: The Historical Interaction of Technology, Home, and Privacy' 278–230..

[63] Katherine Strandburg, 'Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change' (2011) 70 Maryland Law Review 614, 654–655.

[64] Strandburg, 'Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change' 659.

*found in the home; it also contains a broad array of private information never found in a home in any form - unless the phone is.'*[65] Most recently, due to the mobile nature of many home effects (moving into public spaces), Ferguson proposed the concept of personal curtilage (in contrast to traditional curtilage) for a personal to claim protection under the US Constitution Fourth Amendment for his own personal space in public spaces to adjust the home protection to the digitalized world.[66]

Italian law is rather sensitive to impacts of new technologies on home protection. Art. 615 (the provisions of hacking and accessory offences of informatic and telematic systems) of the Italian criminal law (1993) is positioned in the section on inviolability of the home to punish hacking a computer system.[67] For Italian legislators, the informatic or telematic system presents *'a virtual expansion of the area of respect due to the affected subject, guaranteed by art. 14 of the Constitution [i.e., inviolability of the home]...'*;[68] The Italian Supreme Court, according to Felicioni, defined *'informatic home'* in the context of criminalization of hacking as: *'...ideal space pertaining to the person to which the protection of the privacy [riservatezza] of the individual sphere guaranteed by art. 14 Constitution [i.e., protection of the home] can be related. Cyberspace as a virtual place is comparable to the physical domestic place provided it is equipped with security measures (for instance, passwords) that express the will of the rights holder to exercise his ius excludendi alios'*.[69] As Koops pointed out, art. 615 *'has been closely modelled on the trespass provision of art. 614, carries the same sanctions for hacking as for violation of the home'*, but regardless of where they are (informatic or telematic systems).[70]

Apparently, the expansion of the concept of home (space) into the virtual world/cyberspace makes the intended legal protection partially adjustable to home's *'new'* mobile and mosaic nature. However, this causes confusion when the home has been conventionally prototyped in contemporary law as more or less fixed to specific places, as seen in the criticisms against the Italian concept of informatic home. Since the criminalization of unlawful access to computers is independent of the place of the computers and protects computers regardless of their content (supra), and moreover also

[65] *Riley v California 573 US ___ (2014)* 21. (Italicized by the author.) Today, many refugees who fled their home in war time do regard their smartphones as their home in a foreign country which keep their most precious things, family photos and past memories. See Elisabeth Eide, 'Mobile Flight: Refugees and the Importance of Cell Phones' (2020) 10 Nordic Journal of Migration Research 67..

[66] Ferguson, 'Personal Curtilage: Fourth Amendment Security in Public' 1327–1340.

[67]*Art. 615-ter.* [Unlawful access to computers (hacking) and some crimes accessory to hacking]. See: Bert-Jaap Koops, 'Privacy-Related Crimes in Italian Law' (Social Science Research Network 2016) TILT working paper series ID 2877668 16 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2877668> accessed 14 December 2017. The earlier formation of the concept of informatic and telematic systems have not been clearly defined in Italian law, but they cover the most scope of the common definition of cyberspace (both in terms of hardware and software), not pinpointing the spatial and locational features of different sub-spheres.

[68] Koops, 'Privacy-Related Crimes in Italian Law'. (Italicized by the author.)

[69] Ct: Bert-JaapKoops, 'Criminal Investigation and Privacy in Italian Law' (TILT 2016) 16 <https://ssrn.com/abstract=2888422> accessed 3 January 2018.

[70] Koops, 'Criminal Investigation and Privacy in Italian Law'.

includes computers with a public function (para. 3) that seem the opposite of 'home computers', the notion of informatic home has serious flaws, and the placement in the section on inviolability of the home has been criticized as a fundamental error.[71] As Iovene and Flor commented: *'while the 'informatic home' seems a good candidate for that, it is not sufficiently precise, since the home serves the interest of the ius excludendi alios from a pre-eminently personal or intimate sphere, while computer systems involve a broader range of activities in which people express their personalities, also in developing social relations online or in other 'informatic' spaces.'*[72]

The criticism of insufficient accuracy of the informatic home as a legal concept comes from the contrast between the traditional (physical) home space and the seemingly limitless informatic home. The criticism is to the point, but only partially right. First, in the digitally connected traditional home (Home 2.0), many current household activities are no longer of private nature even within the physical structure of home when teleworking and social networking become a routine. Second, even the digital home (informatic home) that is spreading outside the traditional home space, there is the possibility to find some virtual boundaries to offer continued home protection in the virtual world. Though still open and provisional, some of the security measures can at least partially play the role of traditional walls, fences and windows as boundary markers and legal proxy for home protection in the law.

### *3.4 Which boundaries: physical, hybrid or virtual?*

As the above criticisms against informatic home reveals, a big problem with the second concept of digital home is how to practically separate the home space from non-home space in the virtual world (cyberspace). For the first concept, Home 2.0, this is not difficult because of the close connection/affiliation of the added HVS to the traditional physical home. New HVS can mostly be identified and separated by home IPs (or other similar network addresses for the location purpose) that are usually attached to a physical home address, thus it is a practical solution for contemporary law to use them as the proxy for home protection. A good example on this point is the popular geo-fencing practice that *'is the process of defining virtual fences or perimeters around a real-world physical location using geofencing software which is a common part of RTLS (Real-time Location System)'* [73] In practice, Home 2.0 can be protected by establishing virtual fences or perimeters by law to forbid targeted virtual penetrations without home occupant's consent, or lawful grounds (e.g., contractual obligations of service providers). This shall at least exclude unwanted online commercial advertising and political campaigns, and may bar intrusion of

[71] Koops, 'Privacy-Related Crimes in Italian Law' 19.

[72] Koops , 'Privacy-Related Crimes in Italian Law' 21–22. (Italicized by the author.)

[73] See: Jan Kostak, 'Main Applications of Geofencing Technology and Software' (*Sewio RTLS*) <https://www.sewio.net/geofencing-technology-and-applications/> accessed 11 August 2020.

law enforcement agencies even in criminal investigation activities (except with a warrant or the like).[74]

However, for the second notion, the digital home that has no specific physical territorial identify (a position or geo-location in the physical world), and is of mobile and mosaic nature (with data distributed over multiple geo-locations and service platforms), shall be clearly separated from open/public spaces in cyberspace. Virtual boundaries are not new in cyberspace in terms of territoriality and regulation. A well-known example is China's *'famous'* Great Firewall that establishes a *'clear'* virtual boundary to protect China's cyber sovereignty; a big intranet, and mostly one-dimensional.[75] Geo-blocking technologies have been popularly used in e-commerce for *'blocking'* visitors and data flows from certain geo-locations, or for different treatment, for purposes of copyright protection and financial services. The point is that, though different from physical walls, virtual (digital) walls have already been implemented with available technological means, successful or not. Essentially, it is about finding feasible boundaries for systematically structured bits and bytes, deciding who has control of personal data in terms of access, transfer, storage and making profits.

As for the digital home (as a virtual container), virtual boundaries shall function both as barriers and points of entry in analogy. Barriers can protect the private space from unwanted intrusion and surveillance, and equally separate the home space from public space outside, while points of entry through the barrier server as network-based openings into the container. Further, both the barriers and points of entry shall play the role to signal/notify home boundary lines to visitors (by allowing or disallowing entry).[76] In the following, the digital walls (barriers) and points of entry will be discussed respectively for the second concept of digital home. The Table below highlights some basic configurations in home boundary settings of the traditional home (Home 1.0), Home 2.0 and the digital home.[77]

[74] Technically this will require either home owner's control of the accessing gate of HANs, or internet service provider's filtering of data flows to the home IPs. Since the first is almost too difficult and thus impossible in practice, ISPs will take over more responsibilities. But this may lead to other issues, such as ISP's role and the openness of the internet. They shall be further discussed no doubt when this paper only focuses on the concept and boundaries of the digital home now.

[75] By using multiple blocking and filtering techniques, and especially controlling a few servers under the possession of state-owned-enterprises (SOEs). See: Chris Hoffman, 'How the 'Great Firewall of China' Works to Censor China's Internet' (*How-To Geek*) <https://www.howtogeek.com/162092/htg-explains-how-the-great-firewall-of-china-works/> accessed 27 July 2020.

[76] Adida and others, 'The Future of Trespass and Property in Cyberspace' .

[77] It is based on the configuration table discussed by prof. Koops on a previous PiLab conference. See: 'PILab-Brief on Home Protection 2.0 - 180619.Pdf' <https://pilab.nl/onewebmedia/PILab-brief%20on%20home%20protection%202.0%20-%20180619.pdf> accessed 9 July 2020.

**Configurations of Home 1.0, Home 2.0 and Digital Home**

| Dimensio n | Home 1.0<br>traditional home | Home 2.0<br>Home 1.0 + HVS | Digital home |
|---|---|---|---|
| space | dwelling + curtilage | dwelling/ curtilage + home virtual spaces | virtual space, a constellation of cross-platform and cross-service spaces |
| boundary | wall/roof/fence/window/ door/ditch | *idem* + router | logical boundaries with points of entry on multiple devices, networks and services |
| boundary marker | door/lock/property sign | *idem* + password/other security measures/geo-fencing | Accounts + passwords/other authentication and identification instruments/ Encryption/VPNs/geo fencing |
| legal title | inhabitant/occupant | *idem* + account holder (network services) | account holder (multiple network services)/ clients/ subscriber/ coder/ data subject or data owner(?) |
| values/ interests | privacy, property, solitude, peace of mind, family life, security, autonomy, freedom of speech | *idem* + the right to be connected (to access home)/ personal data | *idem* + connectivity/data portability/interoperationality (for cross-platform & cross account services) |

| | | | |
|---|---|---|---|
| intrusions | physical intrusion (entering and remaining) | *idem* + digital (surveillance/hacking) | *Idem* (hardware)+ digital/virtual |
| means of enforcement/ protection | locks/social distance/social norms/law | *idem* + digital security/PbD/contextual integrity/Code or internet protocols/ service contracts +new emerging cyber social norms (self muting of non-speakers in online conferences) | data protection law/security law/IP law/ mandatory contractual clauses/network protocols + new emerging cyber societal norms |

First, like doors and gates, the digital home must have points of entry. The digital home as a virtual container only has *'software points of entry but no physical ones, as there may be no physical manifestation of a particular virtual container'*.[78] Points of entry can exist at many places in computer networks such as TCP/IP ports, and UDP ports,[79] and further in an IoT system (with increasing numbers of entry points added to be secured by strong passwords or certificates).[80] For digital home occupants, this involves multiple security measures including passwords and various authentication/identification measures. They can prevent unwanted penetration of private virtual spaces, and equally authorize entry.

For instance, credentials check and verifications separate legitimate users from illegitimate users when entrance to online services is required. If passwords are not personal or identical enough, in case being stolen and forged, other authentication measures such as bio-identifiers (e.g., fingerprint, face, iris, voice, etc.) can be used.[81] Another example is account configuration in social network services that allows user's accounts to be public, semi-public or private, controlling points of entry in a systematic way. These measures

[78] Adida and others, 'The Future of Trespass and Property in Cyberspace' .

[79] Adida and others, 'The Future of Trespass and Property in Cyberspace' .

[80] 'IoT Security Issues: Top 10 Challenges' (*IBM Developer*, 26 March 2020) <https://developer.ibm.com/technologies/iot/articles/iot-top-10-iot-security-challenges/> accessed 17 September 2020.

[81] For primary bio-identifiers, see: Stan Z Li and Anil Jain (eds), 'Primary Biometric Identifier', *Encyclopedia of Biometrics* (Springer US 2009) <https://doi.org/10.1007/978-0-387-73003-5_746> accessed 30 September 2020.

shall clearly separate public, open spaces from private ones (including the digital home). *'When a limit or restriction does not require authentication, access is still open to all'*,[82] and *'access that bypasses an authentication gate should, under proper circumstances, be deemed an unauthorized trespass'*.[83]

As Kerr pointed out, however, terms of use that set conditions for accessing like age limit or consent for using cookies cannot be taken as controlling authorization; and thus violating terms of use should not render the access a trespass.[84] Whatever an authentication requirement is, it *'creates a technical barrier to access by others. It carves out a virtual private space within the website or service that requires proper authentication to gain access'*.'[85] Authentication is the key to construct the concept of the digital home. But the authentication requirement is not sufficient to guard the digital home *per se*. In reality, we still encounter phishing and spamming in emails nowadays when communicating with others even with a secured email account; we may *'consent'* to receive emails from unknown persons, because our doors and windows need to open to the outside world, to allow permeability of the home.[86]

Second, similar to physical home barriers like walls, fences, bars and roofs, the digital home has virtual barriers to prevent unauthorized entry into the virtual container, establishing virtual boundaries. A popular digital tool, which is more equivalent to *'bricks and mortar'*, is encryption. Encryption *'allows us to end relevant and often-sensitive information over the internet and through electronic means without unauthorized people seeing it'*.[87] Thus encryption, as a bedrock of online security for everything from computer games to VOIP phone calls and video chats, works in a way similar to physical walls and fences, blocking unauthorized visitors from protected space (both data in storage and on the go), while allowing others in with a proper decryption key. Further, host-based firewalls that run on an individual device or private network, and thus differ from network-based firewalls,[88] are another important tool for home protection. If they are complex enough to incorporate antivirus software and intrusion prevention software capacities, they can be very effective in fending off most types of malware incidents and stopping the spread of malware

[82] Kerr, 'Norms of Computer Trespass' 1164.

[83] Kerr, 'Norms of Computer Trespass' 1161.

[84] Kerr, 'Norms of Computer Trespass' 1166. Using Cookies (except persistent login Cookies) CAPTCHA, and blocking IPs are not closing the space in Kerr's reasoning; partially because IPs are dynamic and bypassing them are not illegal when a website is still open to other users. Kerr, 'Norms of Computer Trespass' 1167-1169.

[85] Kerr, 'Norms of Computer Trespass' 1171.

[86] Shapiro, 'Places and Spaces: The Historical Interaction of Technology, Home, and Privacy' 76.

[87] Not that not all encryption tools are available to individual users.
See: 'What Are the Different Types of Encryption? | HP® Tech Takes' <https://store.hp.com/us/en/tech-takes/what-are-different-types-of-encryption> accessed 30 September 2020.

[88] The first is installed on the gateway computers (or devices) of LANs, WANs and intranets, acting as walls and fences *in gated residential communities*; while the second more like walls and fences of privately owned homes.

infections.[89] VPNs (virtual private network) can also protect online private spaces (and thus the digital home), by hiding IP addresses and encrypting all the data one sends or receives, offering online anonymity and privacy.[90] Another example is encrypted routers (with VPNs) as an efficient way to protect all connected devices and personal data from third party snooping, secure home network against attacks, hacking and spying, and unlock the internet (circumvent geo-restrictions and blocks).[91]

However, their deployment is a complex issue. For instance, firewalls can be implemented as hardware, software, or both. As a network security system, they monitor and control outbound and inbound network traffic, establishing a barrier between a trusted network and untrusted external network. In the IoT context, recent firewall techs can function in the traditional wall manner to keep out most visitors, unless they use physical force or have the right key. For instance, the Data Capture Unit is designed for the IoT environment as 'a physical connection that creates a cast-iron gateway', which is '*only one-way and doesn't allow for a reciprocal stream of data*'; it *'allows safe data extraction',* and '*Connections like wireless updates are necessary for any product can only be triggered for the inside*'. [92] Further, network IDS/IPS (intrusion detection and prevention systems) can perform detection and analysis of network traffic moving across in a more detailed way; IDS tools alert attacks while IPS systems further block harmful traffic.[93] An IPS is put directly behind a network firewall, *'adding another layer of analysis that removes dangerous contents from the data flow'*, and an IDS functions within the internal network.[94]

Thus, the problem with firewalls for the digital home is that they are not all mobile and have to be installed either on a hard device, or together with other software, thus difficult to be incorporated as a critical element of the mobile digital home. For the concept Home 2.0, this makes perfect sense in that the firewalls installed at HANs work like traditional walls at the home. But for the digital home spreading over the internet, firewalls can be a difficult component due to the mosaic and mobile nature of the private home space. Firewalls that allow data flow by default do not function like the traditional walls that block most unauthorized entry. Also firewalls function more like a combination of both traditional walls and doors (plus locks), since they need to allow data flows inbound and outbound in the context of packet filtering and stateful inspection, as well as in the proxy service methods (which hide the true IPs of the private networks devices from malicious

[89] 'Host-Based Firewall' (*The IT Law Wiki*) <https://itlaw.wikia.org/wiki/Host-based_firewall> accessed 27 July 2020.

[90] 'What Is a VPN? | Virtual Private Networks Explained | Norton' <https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html> accessed 30 September 2020.

[91]See: https://restoreprivacy.com/privacy-tools/

[92] See: People at Siemens, 'Why Building a Wall Is the Best Cyber Security Solution' (*Medium*, 31 May 2019) <https://medium.com/peopleatsiemens/why-building-a-wall-is-the-best-cyber-security-solution-812581333f90> accessed 30 September 2020.

[93]'Cyber Security Tools' (*EDUCBA*, 1 January 2020) <https://www.educba.com/cyber-security-tools/> accessed 19 August 2020.

[94] 'Cyber Security Tools'.

adversaries).[95] The analogy between the physical walls and virtual walls may not work that well in this context due to the fact that cyberspace is in nature a space totally different from the physical world. Thus, whether the analogy of the digital home may match the traditional home is an issue to be further discussed.

Both door-like and wall-like technological tools can generally separate the home space from other spaces, creating *'digital home'* that is under the occupier's control. Without authorization/permission, others cannot enter the inside; otherwise the entry is virtual trespassing. As Cook pointed out (in the search and seizure context), *'once the government moves to the private level of the device and has the device return information that was not being shared, the government has stepped off the highway and onto the private property (for instance, the hard drive).'*[96] Apparently the use of identification and authentication measures, and other security measures (e.g., encryptions and VPNs) can help establish virtual boundaries - similar to doors, bars, fences, walls, and roofs. They may send clear signals to visitors that they are not welcome, unless acquiring the owner's authorization. However, unlike physical walls, doors and roofs, they are not necessarily arranged together at one location or on one device by the digital home occupier.

Third, in the IoT age individuals will need special types of virtual boundary lines for protection against dominating intrusive ISPs (Internet Service Providers), as the digital home becomes increasingly dependent on them. Unlike the traditional home, most digital homes exist on *'rented'* virtual spaces that are provided by ISPs, and home occupants are actually *'virtual tenants'* protected by *'rental contracts'*. For instance, internet intermediaries like Google, Facebook and Twitter hold a large amount of service accounts and personal data when operating with a data-driven business model. Technically speaking, they may access all user's data in a 24/7 manner, with or without home occupant's consent; and they will process a considerable amount of home-generated data on their distant servers outside the home.[97] The same applies to both the digital home and Home 2.0, which are totally under the control of ISPs. A digital trespass may happen when an app developer/service provider may use their customer's bandwidth to send copies of its software to other customers (as a distribution network). In this context, the company actually acts beyond the customer's authorization and conducts digital/cyber trespass into the user's personal space (digital home). In this context, proper boundary lines are strongly needed, because *'owners should be protected from entities that are given an inch, but take*

[95] See: 'Security and Resilience of Smart Home Environments' 188 <https://www.enisa.europa.eu/publications/security-resilience-good-practices> accessed 29 April 2019.

[96] Cook, '(Digital) Trespass: What's Old Is New Again' 7–8. According to *State v. Riley,* digital trespassing takes the following form: using one piece of technology, a computer or more specialized device such as a stingray, to make use of the resources of another piece of technology, in terms of 'approaching' or 'making use of any resources of a computer.' See: Cook, '(Digital) Trespass: What's Old Is New Again' 6.

[97]But the presence of strangers with listening ears and talking tongues is new in traditional home environment if one looks into home history. At the private home in the Rome time, home servants (not treated as equal home members) presented before masters, even when they conducted the most intimate home activities, having sex.

*a mile'*.[98] Passwords and encryption measures cannot fully protect an individual's data when prevailing service providers take aggressive steps to maximize their harvest from data processing. To avoid abuse of personal data and mass surveillance which are the reality of today's data driven economy, clear home virtual boundaries must be established to help home residents to regain control of the home.

## 4. Feasibility and implications

The core issue for home boundary making in cyberspace is to set up limitations or restrictions for data flows for the digital container, so that an individual can exercise sufficient control over one's virtual space. Cyberspace is imbued with virtual boundaries. However, these boundaries are invisible and *'actually spatial metaphors rather than physical demarcations'*,[99] even though *'the infrastructure of computers, wires, fibers, Wi-Fi and protocols distinguish distinct units in the digital environment just as walls and fences do in the physical world'*.[100] As discussed above, encryptions, VPNs, firewalls, various identification and authentication methods, etc. can to different degrees protect the digital home from virtual intrusions. Thus a further issue to consider is to assess the feasibility of the discussed measures, testing whether they can: a) act as boundary markers, separating home from non-home virtual spaces, and signalling the boundary lines to visitors, and b) be available as a proper legal proxy to protect the new digital home.

The mosaic and mobile nature of the digital home means that it is both location free and container independent, spreading over multiple devices and virtual spaces. In this sense, encryptions, firewalls and VPNs that are mostly device based or network based (on HANs or other non-home networks), cannot be carried freely around by a home occupant as a built-in element of the digital home. The current practice is that a home occupant may access the digital home via a few key devices or networks, so that the firewalls, encryptions and VPNs may function as walls and fences to protect the digital home. But in this case their functions are more like the walls and fences in a gated community, or a residential complex, blocking most unwanted visitors, as an extra security layer to protect the people living inside. Thus, they are not marking out home boundaries. Portability would be a crucial factor to qualify any home components due to home's mosaic and mobile nature.

A further point is that though encryption and VPN technologies can secure end-to-end communications, they cannot mark the boundary lines in a traditionally visible manner. They actually help conceal the digital home (contents) from public surveillance and scrutiny, including browsing history, IP addresses and locations, streaming location, connected devices, and web activities. The established communication tunnels or blended, unreadable bytes and bites function more as high walls and fences hiding home residents behind, when data packets are travelling across networks. This is more like the prehistory

[98] Fairfield, *Owned: Property, Privacy, And The New Digital Serfdom* 122.

[99] 'Understanding Boundaries: Physical, Epistemological and Virtual Dimensions' .

[100] 'Understanding Boundaries: Physical, Epistemological and Virtual Dimensions'

mobile home in that hunters and gatherers stored their foods and tools, as well as other supplies, at different places for future use, by hiding them, not by building strong walls and fences.

Thus, what really counts as walls and doors (in the general sense) of the portable, mosaic virtual space (as one's virtual home) is only the portable security measures that are: a) at the application layer and under user's direct control, and b) non-device, non-location based. At this moment, this would be our personal (service) accounts secured by passwords or other identification and authentication methods, such as one's Google account, Firefox account, etc. Thus, in terms of feasibility, only some security software - especially those with a good interface design, installed across platforms and devices - becomes essential for the digital home occupants for setting up walls and barriers. For instance, for users of the popular Chinese social networking app Wechat, its security measures (include encryptions, firewalls, and security and privacy configurations) are the walls of the digital home.[101]

The seamless user experience and rich functionalities (as a private, controlled space, across multiple platforms, services and devices) likely creates a portable private space (a container, or capsule), accommodating different private life/home activities under one user account that is more like the traditional home (as the centre of private life). In case the software may incorporate encryptions and firewalls to function on different devices, they can be accepted as virtual walls. *'Given that these clear barriers must involve a username-password dialog, a certificate request, a denied connection, or strong encryption, the user can hardly be confused as to which parts of cyberspace are private!*.'[102] In case users have the technical capacity to exercise sufficient control, such as shutting down user account/space and authorizing or disallowing access, the digital home functions more like the traditional home. Mostly this happens at the application layer where the user has more control.

The signalling function is performed more in a binary manner, either granting entry or not. It is better explained in the practice of AdBlock and other advertisement-blocking apps, when used on a synchronized Firefox account on different devices. Even when a user visits a website that is open to all visitors, the add-on will block wanted, intrusive commercial advertisements and protect his private space from intrusive data collection and exchanges. But this will not work in a cross-platform manner, if the user does not synchronize the function. At this point, there could be a case of trespass if the visited website ignores the warning of no tracking by cookies and other means.

Different from traditional home boundary markers (and points of entry) - such as locks, doors, fences, and walls - virtual boundary lines are almost invisible to home occupants

[101] Wechat, unlike Facebook and Twitter, incorporates mini apps (from other service providers) within itself (apps within app) and thus performs most daily life functions including marketing, booking, personal banking, news media, social networking, documents transfers, gaming, and online streaming. See: Julianna Wu, 'Mini Programs: The Apps inside Apps That Make WeChat so Powerful' (*South China Morning Post*, 27 February 2019) <https://www.scmp.com/abacus/who-what/what/article/3028262/mini-programs-apps-inside-apps-make-wechat-so-powerful> accessed 30 September 2020.

[102] Adida and others, 'The Future of Trespass and Property in Cyberspace' .

and difficult to manage. To protect the digital home by law, it is important to assess if the above home boundaries (i.e. authentication and identification methods like passwords, encryptions, VPNs, and firewalls under user's direct control) can be used as the right legal proxy to separate the digital home from the external cyberspace. Clearly, to access a person's private space (personal accounts in specific) by breaking or circumventing the authentication and identification measures is trespassing. Circumventing other securities tools - including encryptions and VPNs that the users directly use to protect their private virtual spaces (the personal container) - is no doubt an intrusion. Because an encryption key *'defines two realms: the data encrypted with that key, which can be considered inside the container, and data not encrypted with the key, which can be considered outside the container'*.[103]

The same is to the use of firewalls for virtual home protection which indicates the home occupants' intention, on the condition that they are installed on the major devices (i.e. mobile phones and laptops under the user's direct control) which are used for accessing the digital home. This is because as a concept under development, the digital home is still not totally location-and-device independent yet. But with the fast roll out of cloud computing and IoTs, private life can soon become less and less device-and-location independent, and the digital home more mobile and mosaic. This may mean that one day we may do return to the prehistory time to have a fully mobile home, a virtual container or capsule, to carry with us.  By then concealing the home can be more important than blocking it and we need to reconsider the functions of 'walls, fences and doors' that are the security measures of the physical world.

## 5. Can the digital future be our home?[104]

The preceding sections focused on a conceptual analysis of the digital home as a virtual container, a private virtual space that is of mosaic and mobile nature and that is protected by different security measures. Currently, only a few available security measures can function as a digital home's virtual boundaries (as legal proxy) for home protection under law, including user accounts and passwords (most feasible now) and other authentication and identification measures (to be further developed), VPNS, firewalls, and encryption measures (feasible under certain conditions as illustrated above). Thus, at the conceptual level, the digital home may exist in a cross-networks, cross-platform, and cross-services manner, but the concept is still immature in view of new home developments in cloud computing and networking technologies.

First, whether the analogy of home between the virtual private space (in cyberspace) and the traditional, physical home space may work is questionable. Conceptually speaking, the traditional home concept will not work for the digital home in terms of most physical functionalities, including sleeping, feeding, breeding, space sharing, developing intimate relationships, etc. These protected, private activities are absent in digital home

[103] Adida and others, 'The Future of Trespass and Property in Cyberspace' .

[104] Zuboff, *The Age of Surveillance Capitalism* 11.

environments that only duplicate or/and extend some functions of the traditional home (the most individual part) into cyberspace. Also, the previous analysis demonstrates that there are no exact (digital) walls, fences, and doors in the virtual world matching their physical counterparts. Walls and doors only exist in a metaphorical sense for the digital home to allow or disallow entry (both as barriers and points of entry).

Second, in line with this, any attempt to use physicality-based rules to regulate and govern part of cyberspace has limitations, as is evident in the effort to find feasible virtual home boundaries for upgrading legal protection. While the gradual shift of a considerable part of current home life to an increasingly digitally connected world is apparently real, using the term *'digital home'* can be partially misleading. Even if the new digital home's mobile and mosaic nature can be traced back to the prehistory of home development and found in modern Nordic communities, virtual home life cannot be equal to and replace traditional physical life. The digital home is not the same as the physical home because virtuality will never replace physicality in human private life. [105] Further, the geo-location and device independency of the digital home does not mean insignificance of physicality, but just the fact that the digital home will not depend on and be limited to any specific digital devices or geo-locations as the traditional home is.

Third, but most importantly, the gradual blurring or collapsing of boundaries in daily life due to deepening digitalization and connectedness have created new challenges to the modern law. The strong need for delineating new home boundaries for legal protection in modern law to protect home life and important home related values is only an indication of similar challenges for modern law concerning border control in the Online world and smart environments that infer our future or even current behaviours.[106] This includes the blurring of the borders between online and offline, as well as those between private, social and public contexts. How the modern law may deal with such boundary issues, when it used to rely on physical proxies such as walls and roofs in the home protection case, is quite challenging when there is the equally strong need for clear virtual boundaries and when traditional, physically based laws (concepts and rules) are difficult to apply to the virtual world even by analogy.[107]

Last, in view of the above, it is rather questionable, at this moment, to define and protect the digital home in a more systematic, formal manner by law. An essential reason is that the digital home is still in its earliest stages and consists of only a small part of current home life, even though the new practice has created significant implications for home protection by law (e.g., the blurring home boundaries in an increasing hybrid of virtual and physical spaces). As the above analysis demonstrated, digital home practices and technological

[105] For instance, compare a real pet dog with a digital pet dog (either as software or a combination of hardware and software). But it is not deniable that a digital pet dog can be coded to act in many different ways that are not available to a real pet dog.

[106] See: Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing 2015) 79.

[107] One such example would be the growing claim of state borders and sovereignty in cyberspace.

developments are yet not mature enough to establish workable, clear-cut home boundaries between home and non-home spaces—similar to the legal proxy we now use in the current legal framework in which physical boundaries like walls, fences, and roofs separate home from the outside world.

Looking forward, it is best to find ways to strengthen the current protection of the new *'home space'* outside our traditional physical home, but to still maintain the current legal mechanism to protect the physical home and related home data (collected and stored in the traditional home), without formally recognizing and defining the digital home.

Currently, there are a few options to protect *'the digital home'*. A practical, technical solution is to follow the recommendations from the research of Koops and Hoepman to protect the digital home (space) that can be clear cut in the technical sense from the outside with the suggested special technical means to create a more home like cyber environment with strict control by the owners. A second (legal) solution is to only grant such spaces strengthened and distinct legal protection, namely the home protection, but without equating such spaces to the *'home'* under law. This will provide legal certainty and coherence when most of our daily life still exit in the physical home space, meanwhile offering stronger protection than the weak protection over many home assets that are not in the traditional physical home any longer.