CHALLENGES TO HOME PROTECTION IN THE DIGITAL AGE: ENVISIONING HOME 2.0 AND DIGITAL HOME

On June 19 2018, the Dutch PI.lab organized a roundtable to discuss two new concepts: Home 2.0 and digital home, proposed by the VICI team from TILT (Tilburg Institute for Law, Technology, and Society) for better privacy protection in the increasingly digitalized and hyper-connected home environment. Around thirty participants, including academics, law enforcement agents, ICT experts, lawyers and policy-makers, reviewed the weakening home protection in the age of ubiquitous data, and explored the feasibility and configuration of the two concept(ion)s. The majority shared the view of the necessity for re-conceptualizing home as a legal concept, despite some disagreement on how this is best done. This short paper is meant for providing a brief summary of the roundtable discussion with some reflections, and to offer some policy recommendations for improving home and home privacy protection.

The NWO-funded VICI project "Privacy in the 21st century. Finding a new paradigm to protect citizens in the age of ubiquitous data" (2014- 2019), led by Prof. Bert-Jaap Koops, addresses the growing vulnerabilities of citizens in the age of ubiquitous datafication and connectivity. The project aims at re-inventing legal protection of privacy in constitutional law, criminal law and criminal procedure law by finding and applying new conceptual tools. Through comparative legal study, analysis of developments in mobile internet, cloud computing, and surveillance technologies, and theoretic research, the project tries to generate place-independent boundary-marking concepts,[1] which reflect what comes closest to people's personal lives in the post-digital age.[2] In addition to a "mosaic spheres theory" that is being developed by the VICI team, "Home 2.0" and "digital home" are the other two concepts envisioned for re-delineating the boundaries of private life in the law, now that the home becomes more of a hybrid between physical and digital space and our life is characterized by a full integration of virtual and real space.

Home is an important proxy in privacy protection. In most western jurisdictions, home traditionally marks a strictly protected private (home) space (and place), usually delineated by walls, roofs, windows, fences, etc., allowing the best control vis-à-vis the outside world, regulating and restricting others' entry. While the home-as-castle doctrine indicates the strongest privacy protection against external intrusion, the traditional home (Home 1.0) can no longer effectively shield/protect our most intimate private life, due to the fast advances of new technologies. The evaporation of the traditional home is well observed in the carrying around of private life,[3] the extension of private life to (semi)public spaces, the introduction of work and public spheres into home spaces (telework, social networking), shifting of private life into virtual spaces, monitoring of home and home activities from the outside via non-physical intrusion (e.g., thermal imaging, drone camera surveillance, smart metering data) with significantly lower safeguards than for entering the home, etc. The traditional concept of home in law thus encounters increasing difficulties to protect privacy at an equal level as before.

In this context, Prof. Koops presented the two new concepts for the roundtable participants to discuss their conceptual scope, practical possibility and technical configuration to improve legal

[1] "Boundary-marking concepts" are concepts that can function to mark limits of acceptability, reflecting fundamental assumptions about human existence. See R. Brownsword and M. Goodwin, *Law and the Technologies of the Twenty-First Century: Text and Materials*, Cambridge University Press, Cambridge UK/New York 2012, 188-189.
[2] Meaning an era in which the term "digital" has lost its meaning as a distinguishing factor, since digital technologies and the internet are as common to life as water, oxygen and electricity. See Tom Goodwin, The Three Ages of Digital, TECHCRUNCH, http://social.techcrunch.com/2016/06/23/the-three-ages-of-digital/ (last visited Jul 31, 2018).
[3] With digital photos, contracts, diaries, bills and communications stored on mobile devices and on remote-storage services such as clouds.

certainty and legal protection. *Home 2.0* essentially refers to the digitally connected (traditional) Home 1.0 in the context of the Internet of Things (IoT), which implies the home will be more vulnerable to non-physical privacy intrusions. The *digital home* refers to certain networked devices, such as smartphones, and parts of the related cloud ecosystem over which users exercise exclusivity 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. Both concepts can be analyzed from the perspectives of space, boundaries, boundary-markers, legal title, protected values and interests, intrusions and means of enforcement or protection (see the table below). During the meeting, participants discussed in depth whether the two concepts make sense, whether and to what extent they could be realized by technical means such as via privacy by design and by default, and whether and to what extent they could be translated into the law.

Regarding the need for *re-conceptualization*, all participants perceived the aggregating privacy challenges from the age of ubiquitous data, observing that "We have no home in the post-digital age." While some argued that better protection can equally well be achieved via other legal means such as contractual obligations, due care and confidentiality rules, others pointed out that effective privacy protection relies more on social norms rather than legal norms. Participants doubted whether we should primarily protect containers (the home, envelopes, or mobile phones) or contents (private information, personal data), finding this may differ with respect to Home 2.0 and digital home. Conceptually speaking, the concept of digital home received more criticism, regarding, for instance, the applicability of regulatory mechanisms of the analog world to the virtual world, and questioning how to define a protected container when data are ubiquitous and distributed over numerous places. In addition, if home is a place we feel safe in and where we can lower our guard, it is questionable where we may find such a space or place in the digital environment (unless we would opt for a completely disconnected home).

Regarding *technical feasibilities*, it was agreed that both concepts might be realized to a certain extent, though this is not without difficulty. For Home 2.0, it is possible to set up electric, digital borders/boundaries to protect home spaces; however, there might be many of them, and too complicated for ordinary persons to handle by themselves, not to mention mobile devices constantly moving in and out of the home. Thus, standardized industrial security standards are necessary and data protection by design and by default can be of substantial help. The digital home could be achieved in multiple ways, for instance, in the cloud context, by the tagging of data which would give the data context and where the tag could serve as a virtual container. Also, attribute-based technology is possible to authenticate the user and delineate the context. For portable devices such as smartphones, it might be feasible to set up a core area for 'home protection' at the hardware level for exclusive control.

The roundtable discussion brought up three major points for law and-policy makers' further consideration. First, if home is and still will be the center of private (and family) life in the near future, the evaporation of the home must be taken seriously to protect the fundamental values that the home protects, especially in view of its proxy function in dividing the public from the private. As the core unit of communal life and central locus of private life, home evolvement consequent to technology developments must be considered in a systematic way. Second, more practically, future IoT regulation shall focus more on streamlining security and privacy protection standards of connected devices in the home environment to ensure systematic, coherent protection. Third, for regulatory purposes, the concept of Home 2.0 seems a promising concept, extending existing protection of physical boundaries to protection of virtual boundaries, marking which digital devices, spaces and flows should be protected as falling within the 'home'. The concept of digital home might be useful but requires more reflection, since it is yet unclear whether what we want to protect in the digital space is similar to 'home' or rather to some other privacy-related concepts.

CONFIGURATION OF HOME 1.0, HOME 2.0 AND DIGITAL HOME

Dimension	Home 1.0	Home 2.0	Digital home
space	dwelling + curtilage	idem	space defined by…
boundary	wall / roof/ fence	idem / router	logical boundaries
boundary-marker	door / lock / sign	idem / password	logical address
legal title	inhabitant	idem [challenge: ***free***, ***informed*** consent for allowing entry?]	account holder [challenge: ***free***, ***informed*** consent?]
values / interests	privacy, property, peace of mind, family life	idem	idem (or more? or less?)
intrusions	physical (getting in)	digital (surveillance)	a) hacking b) violation of contextual integrity
means of enforcement/protection	locks / social distance / social norms / law	digital security / PbD / contextual integrity [challenge: *lack of social distance*, ***social norms***]	digital security / contract / law? [challenge: lack of **spatial control**, **social norms**, **legal norms]**