Editorial

One of the most ancient legal principles is that of the separation between the private and the public domain.[1] Historically, the public domain was subject to the rule of the king and the private domain fell under the rule of the father of the family (*pater familias*). In ancient Greek philosophy, a distinction was made between the home (*oikos*) and the public domain (*polis*). The word privacy itself stems from Latin – *privare* means taking something out of the public domain, and is thus the exact opposite of *publicare*, taking something from the private into the public domain. The right to privacy is consequently linked with the act of withdrawing matters from the public sphere.

Slowly but surely, the private domain has been formulated not so much in terms of spheres, but in terms of land and ownership. In Medieval times, the private domain was linked to the ownership over land and the buildings on it. Typically, these would be feudal lords who owned large properties. They ruled over private lands, while the king reigned over the public domain.

With increased prosperity, it became increasingly common for everyone to own a home. Private lordship was democratised and anyone could claim a small private kingdom. 'My home is my castle', as the English proverb goes, echoing the idea of a place fortified against the outside world.

Importantly, the democratised private domain was a mirror situation of the old feudal lord in terms of ownership. The feudal lord owned all the property on his land and the people working on his land were considered serfs. Similarly, in the home of the private individual, the objects such as chairs, tables, cutlery and curtains, are his property. In addition, like the feudal lord, the male breadwinner of the family was considered to have dominion over the other family members, until not so long ago.

Here, of course, also lies an important limitation of the protection of the private domain in modern times. The sanctity of the home cannot only be lifted when people are suspected of endangering public safety or undermining public interests, but also when family members infringe upon each other's basic rights. The government has a right, and even a duty, to ensure that public morality is also applied in the private domain.

Recent developments signal a second important limitation of the sanctity of the home. Not only are the people living on the property of an owner no longer subjected to his absolute reign, the objects increasingly fall beyond his powers too. This especially holds true for the introduction of smart devices in the home. Those devices, like a smart meter, a smart refrigerator and a smart television, are connected to the web and can

DOI: 10.21552/edpl/2017/3/3

1 See for a historical perspective on privacy the excellent book series edited by Aries and Duby <http://www.hup.harvard.edu/collection.php?cpk=1094> accessed 10 October 2017.

be steered and controlled by a third party via the internet. This questions the scope of the protection of the home.

This question becomes urgent when connected to the responsibility over these objects and a number of technological developments, such as the growth of the so-called 'Mirai-botnet'. Different from traditional botnets, this one feasts mainly on devices such as remote cameras, routers and other smart devices that are part of the Internet of Things (IoT). While computers and smart phones are often protected both by the software developer and the consumer, this does not hold true for most devices connected through the IoT; they are either left unprotected or shielded by weak security measures and standard passwords like '4321', which are often not altered by consumers.[2] Consequently, these devices can be easily compromised, making them the ideal hosts for botnets. As is well-known, botnets can be used to a number of ends, such as DDoS attacks, click-fraud, ransomware and spreading fake news, perhaps even compromising democratic elections.

The question becomes, who is responsible for the attacks conducted through the use of IoT devices in the homes of individuals? Is it the manufacturer of the hardware, the software developer, the service provider promoting its use or the individual itself? Do we make the individual responsible for the actions conducted through the devices in his home or not? If we do, that means that the individual has a legal obligation to secure the devices, for start by changing passwords and by taking a number of other basic security measures. If he does not do so to a reasonable extent and illegal actions are conducted through the devices in his home, he could be held accountable for them.

It is questionable whether citizens are really up to the rat-race with criminals in the ping-pong game between security measures and circumvention tactics. But even if they would, the fact remains that these devices are really not comparable to a chair or a table. The smart meter is given to us by the energy supplier: is that device really ours or is it the device of the supplier placed in our homes? Do we carry responsibility for its security design? In addition, many of the smart devices that we do voluntarily take into our homes, such as a smart refrigerator, are so complex that we cannot really control them. They can act on our input, but can we reasonably be accountable for the actions conducted through such devices?

Another solution might be to make others responsible for the smart devices in our homes, but this may raise equally thorny issues. Suppose there is malware placed on such an IoT device, which is used as part of a botnet for malicious undertakings, does the provider or software developer have the right to enter that device via the internet to remove the malware or should this be seen as an infringement of our home through virtual means?

2 Elisa Bertino and Nayeem Islam, 'Botnets and Internet of Things Security' (2017) 50(2) Computer.

Still, I think it might be interesting to analyse in how far we can develop a more hybrid conceptualisation of the right to the protection of the home. Already, a number of scholars have argued that in the public domain, our privacy should be better protected. Our private lives increasingly take place on our laptops, smartphones and iPads, they signal. Why should there be fewer limitations for the police to enter my smartphone when I'm in the public domain than when the police want to enter my home?[3]

Similarly to this more hybrid conception of the public domain, we could develop a more hybrid conception of the home. Let's call it the porous home and the porous house right. Can we develop a conception in which the integrity and sanctity of the home is maintained, while the objects not under our full control are excluded from the right to the protection of the home? I think a good starting point for such complex situations of control and territory might be to draw an analogy with embassies. Contrary to popular belief, the embassy located at a certain country does not necessarily fall under the territorial jurisdiction of the sending country.

Still, there are limits to the authority the receiving country can exercise over the embassy. Article 22 of the Vienna Convention on Diplomatic Relationships specifies:

> 1. The premises of the mission shall be inviolable. The agents of the receiving State may not enter them, except with the consent of the head of the mission.
> 2. The receiving State is under a special duty to take all appropriate steps to protect the premises of the mission against any intrusion or damage and to prevent any disturbance of the peace of the mission or impairment of its dignity.
> 3. The premises of the mission, their furnishings and other property thereon and the means of transport of the mission shall be immune from search, requisition, attachment or execution.

There are three important elements in this article: the right to enter the property, the protection of the property against unlawful intrusion and the transport from and to the property. If we take this as a starting point, we could say that the owner of the home (the receiver) has the duty not to enter the software of the IoT device in his home without the consent of the supplier (the sender). Still, the receiver has the obligation to ensure that the device is not damaged or compromised by third parties in the physical sense. The digital transport of data from and to the device, however, falls under the responsibility of the sender. If illegal actions are committed by or through the use of the IoT device, it is the responsibility of the sender.

This is of course only a starting point of the discussion. We live in times when fundamental legal principles are challenged and old ways of dealing with legal issues no longer work. That is also the theme of this issue. In essence, it regards the limits and boundaries of data protection law as we know it. Professor Broeders, in his foreword,

3 See for example the project of Prof Koops to reinvent privacy protection in the public domain <https://www.tilburguniversity.edu/nl/webwijs/show/e.j.koops.htm> accessed 10 October 2017.

suggest that the use of Big Data analytics in national security and law enforcement shows that the traditional focus of data protection law on gathering personal data and to a lesser extent the use of data no longer works: it is the analysis of the data that should (also) be regulated. Professor Van Eijk argues, in his foreword, that we should prepare for and work on the post-GDPR (General Data Protection Regulation) era. This would, according to him, require a tilting process: from privacy and data protection as a fundamental right, to a horizontal approach in which competition, consumer and other areas of law play an important role.

The limits of the data protection framework are also at the core of the Articles section. *Fanny Coudert* discusses the new Europol Regulation and suggests that it fails to acknowledge the risks created by the new environment and fails to identify and to address the challenges ahead. This is a missed opportunity for the EU legislator to devise a new way to implement data protection safeguards. In their article, *Nico van Eijk*, *Chris Jay Hoofnagle* and *Emilie Kannekens* suggest that EU data protection law can learn from the American approach, for example by relying more on rules about unfair commercial practices. *Rob van den Hoven van Genderen* discusses the developments known as Artificial Intelligence (AI) and concludes that the GDPR uses outdated terminology. Due to the non-technological orientation and the hinge on conventional directions of thinking, the GDPR will not be sufficient to protect personal data in the age of AI, he argues. Finally, *Frederik Zuiderveen Borgesius*, *Sanne Kruikemeier*, *Sophie Boerman* and *Natali Helberger* discuss the regulation of tracking walls and take-it-or-leave-it-choices under the European data protection framework. They point to elements for improvement in the rules following from the GDPR and the proposed e-Privacy Regulation and suggest that a partial or complete ban of tracking walls should be considered.

As always, special mention should be made of the Reports section, coordinated by Marc Cole, which is one of the elements that make EdpL stand out. *Andra Giurgiu* and *Miguel Recio* have contributed to our GDPR Implementation Series, describing the implementation process in Luxembourg and Spain respectively. *Dominic Broy* has written a report about one of the most important recent developments, namely the proposal to regulate the flow of non-personal data. *Christina Etteldorf* discusses a court case about data retention in Germany and *Teresa Quintel* analyses an important matter in the United Kingdom before the Investigatory Powers Tribunal. Finally, Christina Etteldorf has been invited to describe an important case in Canada, in which the Supreme Court exercised authority over Google. In the case note section, Maja Brkan and Tijmen Wisman have once again managed to bring together four case comments by leading experts. *Irene Kamara* discusses the Opinion of Advocate General Kokott of the Court of Justice on the concept of personal data, *Hielke Hijmans* discusses the Opinion of the Court of Justice on the Draft Agreement of the Transfer of Passenger Name Records (PNR), *Nicolas Blanc* discusses the hearing in the *Schrems II* case and *Diana Dimitrova* discusses the Court of Justice ruling in the *Rigas satiksme* case concerning the scope and limits of data protection. Finally, *Alessandro Mantelero*, as editor of the book review section, discusses the book *The Aisles Have Eyes* written by the

famous Joseph Turow and *Gianclaudio Malgieri* engages with *Data Protection and Privacy: (In)visibilities and Infrastructures*, which is part of the series of books that appears each year after the Computer, Privacy and Data Protection (CPDP) conference.

For those interested in writing an article, report, case note or book review, please e-mail our executive editor, Nelly Stratieva at <stratieva@lexxion.eu>. Upcoming deadlines:

- EdpL 2017/4: 15 October 2017 (Young Scholars Award 2017);
- EdpL 2018/1: 1 January 2018.

We hope you will enjoy reading EdpL's third edition of 2017!

Bart van der Sloot
Tilburg Institute for Law, Technology, and Society (TILT)
Tilburg University, Netherlands