Privacy protection in the 21st century

New concepts, theories, and applications

Symposium 14 May 2019 & TILTing VICI panels 15 May 2019

In privacy protection, the traditional distinction between private and public physical spaces is becoming less useful in determining what really is protection-worthy. The walls of the home are 'evaporating' and it is becoming increasingly more difficult to use them to shield in-home activities. At the same time, through ubiquitous datafication and mobile devices, the home itself has lost its privileged role as the primary place of private life. Many people carry more private information in their pocket than could be revealed by a thorough search of their home. Public space and digital spaces are thus becoming important places for private life, while also becoming subject to increasingly omnipresent and sophisticated surveillance.

These challenges bring forward a number of interesting questions. What are the various aspects of private life that deserve protection in the 21st century? Can spatial approaches to privacy protection remain useful going forward? If the place-based boundary no longer works, can we identify a core of privacy which should receive a more robust protection? Can we 'recreate' the physical architecture that delimits a protected private sphere in digital space? How should we protect privacy in public spaces?

These questions have been addressed in 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. We will present the project's results at this final symposium and continue the discussions in three VICI panels at the *TILTing 2019* conference.

Symposium 14 May 2019

In the final closing conference of the VICI project, the VICI team will present the project's findings and conclusions. These will be discussed by international scholars (including Michael Froomkin, Seda Guerses and others) and the audience.

Program highlights

- Privacy typology and surveillance theory
- Content approaches: the core of privacy and mosaic spheres theory
- Spatial approaches: home 2.0, the digital home, and computer castles
- Application spaces: surveillance in public, Dutch criminal procedure, and laws of nature

Full program: see below.

To register (free of charge), visit https://forms.tilburguniversity.edu/674**.**

TILTing panels 15 May 2019

Call for abstracts

Researchers working on similar questions are invited to present their work at the TILTing Perspectives 2019 Conference in Tilburg. We especially encourage researchers in the fields of constitutional and criminal law to present interesting privacy frames and concepts emerging in their jurisdictions, but the call is open for researchers from all disciplines as long as the contribution fits within one of the following themes:

- Content-focused privacy protection: which substantive frameworks can help protect privacy in the 21st century?
- Spatial-based privacy protection: can privacy be protected by protecting 'containers' of private life?
- Surveillance in public space: which concepts and frameworks work to protect privacy in surveilled public spaces?

The deadline for abstracts for these panels is **11 January 2019**. Abstracts (of 500-1000 words) should be sent to i.skorvanek@tilburguniversity.edu. *Full call: see below.*

Privacy protection in the 21st century

New concepts, theories, and applications

VICI symposium 14 May 2019

This one-day symposium is the final closing conference for the NWO-funded VICI project *Privacy in the 21st century. Finding a new paradigm to protect citizens in the age of ubiquitous data*, led by prof. Bert-Jaap Koops. The VICI team will present the project's findings and conclusions, which will be discussed by invited scholars and the audience.

10:00-10:15 Welcome and introduction (Bert-Jaap Koops)

10:15-10:45 **Groundwork**

- A Typology of Privacy (Bryce Newell)
- Surveillance Theory from Bentham to Deleuze and beyond (Tjerk Timan)

10:45-12:15 **Content approaches**

- The core of privacy (Robin Pierce)
- Location tracking by police and the mosaic theory (Bryce Newell)
- Mosaic spheres theory (Bert-Jaap Koops)

discussant(s): TBD

Lunch

13:15-15:15 **Spatial approaches**

- Conceptualising space and place (Maša Galič)
- Privacy spaces (Bert-Jaap Koops)
- From home 1.0 to home 2.0 and the digital home (Bo Zhao)
- My computer is my castle (Ivan Škorvánek)

discussant(s): TBD

15:30-17:00 **Areas of application**

- Surveillance in public space (Maša Galič)
- Modernising the Dutch Code of Criminal Procedure (Bert-Jaap Koops)
- Securing home 2.0, the digital home and the laws of nature (Jaap-Henk Hoepman)

discussants: **Michael Froomkin, Seda Guerses**

17:00-17:30 General discussion and wrap-up

To register for the symposium (free of charge), go to https://forms.tilburguniversity.edu/674.

(Note: the topics will be further discussed during three panels on 15 May, the first day of the *TILTing 2019* conference. See *Call for abstracts* below. For more information about the conference, venue, fees and dates, see the conference website at: http://www.tilburguniversity.edu/tiltingperspectives/.)

Call for abstracts

Privacy protection in the 21st century. New concepts, theories, and applications

TILTing VICI panels 15 May 2019

Researchers working on **new conceptual approaches to privacy protection** are invited to present their work at the TILTing Perspectives 2019 Conference in Tilburg, the Netherlands. We organise three privacy panels on 15 May 2019, featuring three panels to discuss novel approaches to privacy protection.

We especially encourage researchers in the fields of constitutional and criminal law to present interesting privacy frames and concepts emerging in their jurisdictions, but the call is open for researchers from all disciplines as long as the contribution fits within one of the following themes:

1. Content-focused privacy protection: which substantive frameworks can help protect privacy in the 21st century?

2. Spatial-based privacy protection: can privacy be protected by protecting 'containers' of private life?

3. Surveillance in public space: which concepts and frameworks work to protect privacy in surveilled public spaces?

These themes are elaborated below. (Please note that the discussions will focus on privacy in its many manifestations, not limited to informational privacy. Submissions purely focusing on data protection will not be considered for acceptance.)

The deadline for abstracts for these panels is **11 January 2019**. Abstracts of 500-1000 words should be sent to i.skorvanek@tilburguniversity.edu, including a short bio and indication of the relevant panel.

Panel 1. Content-based privacy protection: can privacy be protected by focusing on the substance of private life?

Privacy is usually protected in the law through proxies. Often, the law uses as proxies certain 'containers' of private life (e.g., protection of homes and communication channels, which protect these spaces regardless whether the contents are privacy-sensitive in particular cases). Proxies can also be content-related, i.e., protecting the substance of private life. This panel focuses on the latter approach, questioning whether and how the substance of private life can be captured in today's datafied and all-connected society.

Data protection law is an example of content-related protection: it protects all personal data *qua* personal data, regardless whether the data are privacy-relevant in particular cases. Protection of "sensitive" data uses proxies of "special categories of data", such as data relating to health, religion, or sexual life. This is a coarse approximation of "sensitiveness", because not all health or sex-related data are sensitive in each case, and because in a world of Big Data, also non-special categories of data can, in combination, give deep insight into private life.

Content-related protection of privacy goes beyond data protection, however. Criminal law and criminal procedure have several protection mechanisms, focused on, e.g., bodily integrity (with strict conditions for strip searches by police), reputation (e.g., criminalizing slander), secrets, and confidential oral communications. While such proxies still work relatively well to capture physical privacy intrusions, the datafication of everything raises questions on the adequacy of current proxies of content-related privacy protections in the law.

Against this backdrop, this panel aims to discuss issues including, but not limited to:

a) In the post-digital age, what is the role of traditional concepts aiming to capture the substance or core of privacy?

b) How can their roles be adjusted to the new privacy circumstances characterized by datafication and the intertwining of physical and informational privacy?

c) Can we identify new concepts that capture the substance of privacy in today's world and that can be used in the law to draw lines between more and less serious privacy intrusions?

Panel 2. Spatial-based privacy protection: can privacy be protected by focusing on the 'containers' of private life?

Privacy is usually protected in the law through proxies. These proxies can be content-related (e.g., data protection law protects all personal data, regardless whether the data are privacy-sensitive in particular cases). They can also be container-related, i.e., protecting a container of private life, regardless whether the inside of the container is privacy-sensitive in particular cases. This panel focuses on the latter approach, given that the law has been using substantial containers as an important legal proxy to protect private life within certain physical boundaries.

One such well-known example is the home as the place and space that separates the public from the private, providing private activities taking place within home boundaries with a strong legal protection in most modern jurisdictions. However, with increasing digitalization and connectivity of our modern home (as in the IoT context), it is questionable whether the home can still be functioning as the best container for privacy protection against external intrusions, especially non-physical ones such as thermal scanning or hacking. Other containers may include automobiles, business premises, envelopes, and public toilets. Nowadays, portable smart devices hold various activities of a private nature and are starting to be protected by law to different extents. At the same time, our continuous online private life reaches beyond any particular physical containers (e.g., through the cloud), which should be equally protected by law. Thus, online boundary-less activities crossing multiple physical boundaries have led to the decline of traditional containers in privacy protection.

Against this backdrop, this panel aims to discuss issues including, but not limited to:

a) What are the new roles of traditional privacy containers in the post-digital age?

b) How can their roles be adjusted to the new privacy circumstances characterized by the co-existing of physical and virtual spaces?

c) Can we find new types of containers to tackle privacy protection in cyberspace?

Panel 3. Surveillance in public space: which concepts and frameworks work to protect privacy in surveilled public spaces?

The law traditionally strongly protects privacy in 'private' spaces (in particular the home, but also in other closed spaces). In 'public' space(s), however, privacy is protected much less through legal safeguards. Historically, this can be explained by the fact that in public urban spaces, people were theoretically visible and observable, but practically usually inconspicuous. As a default, you could be 'just another face in the crowd', so there may not have been particular needs for legal protections of privacy in public.

With the rise of surveillance technologies and their ever-increasing application in public spaces, the default of moving around in public is no longer inconspicuousness, but visibility. Similarly, the default of being usually practically anonymous is giving way to a default of often being practically identifiable, e.g., through location monitoring, WiFi tracking, and facial recognition.

While the *need* for adequate privacy protection in public space has been highlighted in the literature, it is less clear *which types or aspects* of privacy exactly need protection, and it remains a challenge to identify suitable *means* for protecting privacy in public. Data protection law, while applicable, may be difficult to enforce, and will be insufficient to address the broader privacy challenges, which are not all reducible to informational privacy. This raises questions which additional protection mechanisms can be included in the law to protect privacy in public. Should we look for spatial-based privacy protections (e.g., protecting particular areas in public space, or set limits to sensing in public spaces as such), or rather for content-related privacy protections (e.g., setting limits to monitoring vulnerable people or socially awkward situations), or both? Or can other proxies be identified that the law can use to protect the privacy in public?

Against this backdrop, this panel aims to discuss issues including, but not limited to:

a) Which types or aspects of privacy need legal protection in the context of surveillance of public spaces, besides and beyond informational privacy?

b) How can intrusions into these types or aspects privacy be regulated in the law? Should legal protection focus on people, not places? Or rather on places, not people? Or on something else?

c) Which conceptual approaches are most promising to protect privacy in public in view of prevalent surveillance technologies and applications?