Introduction: conceptual directions for privacy in public space

Tjerk Timan, Bryce Clayton Newell and Bert-Jaap Koops

Since its start, the twenty-first century has posed new challenges to privacy—challenges that have affected many areas of professional practice and are straining legal doctrines drafted in the previous century. At a conceptual level, the private space/public space dichotomy also increasingly fails to capture and describe privacy problems in a satisfying manner. This volume is aimed at addressing these challenges, by exploring and developing a research agenda on privacy in public space that crosses disciplinary boundaries. It includes contributions from primarily legal and philosophical scholars, but because the issues raised by privacy in public space extend well beyond disciplinary borders, it also features contributions that draw on geography and other social sciences. Each of these chapters contributes to the debate about what privacy in public is or can be from a different angle, by providing new arguments, concepts, ideas or insights. Bringing together law and philosophy seems particularly fitting for an exploration of this topic; while the legal contributions draw on actual real-world examples to lay bare the problems of privacy in public space, the philosophical contributions explore how we can better conceptualize privacy in public space by drawing on examples, normative argumentation and existing empirical research.

The central theme of this introductory chapter is to explore conceptual paths for thinking about privacy in public. The authors in this volume have given various accounts of what privacy in public space is or can be, and discussed ethical, social and legal problems that arise when the *private* (information, activity, etc.) enters public space. Due to the proliferation of information and communication technologies (ICTs), more and more aspects of our private lives are spilling over into public space. We carry phones, laptops and other wearable computing devices—each of which potentially contains large amounts of personal (private) data—with us as we traverse a variety of public and private spaces each

day. Additionally, by connecting to wired or wireless networks (3G/4G, WiFi, etc.), which our devices often do automatically, even without our knowledge, we automatically bring all sorts of things into (virtual) public space that would normally be safely stored in private places under our control (e.g. at home) and therefore be relatively inaccessible to others. At the same time, the make-up of the public space we move through has been changing; it is becoming more sentient, empowered by the proliferation and increasing sophistication of embedded sensors and surveillance technologies (such as smart CCTV, WiFi, cellular networks, wireless mesh technologies, audio sensors, and automatic license plate readers).

In this chapter, we summarize and highlight the key insights made by the authors in the succeeding chapters and draw connections between the chapters.

1. PRIVACY IN PUBLIC: DIRECTIONS FROM THE BOOK

The chapters in this volume show several similarities in pointing out what privacy in public is, or can be, and how we should think about it conceptually. One common theme that emerges from many contributions is that context is important. Whereas privacy is often defined (including by legal scholars) in a de-contextual and abstract manner, there is a need to study privacy locally and in context. Doing so can enrich often-static legal definitions of privacy and generate new and novel directions for thinking about privacy, both conceptually and in terms of the law. The need for studying privacy in context primarily stems from an increasingly intertwined public and private context, facilitated by ICTs and other, related new technologies. This is creating new situations in which current legal protections no longer suffice.

Ever since Helen Nissenbaum introduced the concept of contextual integrity,[1] many privacy scholars have engaged with this concept, debating where and how contextual integrity would work. Having originated as a theoretical insight, and maybe as a direction for dealing with privacy in the twenty-first century, the idea of contextual integrity remains difficult to translate into (legal) practice. Some authors in this volume, such as

[1] H. Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 *Washington Law Review* 119. See more extensively, H. Nissenbaum, *Privacy in Context* (Stanford Law Books, 2010).

Brincker and Hildebrand, have provided theoretical advancements on context and contextual integrity as a starting point for thinking about privacy.

In this respect, many authors in this volume delve into what contextual privacy means and attempt to make this endeavor as concrete as possible. More precisely, they provide notions of action and agency as tentative answers to the question how to take context and contextual integrity into account when talking about privacy. The chapters show numerous contexts in which privacy in public is at stake, from DNA traces we automatically 'leak' into public space by just being there to the proliferation of smart devices in public space that blur the boundaries between public and private information and the storing and sensing thereof. Moreover, the authors discuss cases that reveal shifts in ownership of public space, an increasing privatization and social sorting, cases of masking and the social boundaries of being allowed (or not) to cover one's face in the crowd, and examples of economic and filmic analysis of how privacy in public is negotiated.

It seems difficult to transpose conceptual notions such as context and agency into particular privacy laws, especially because the terms have not been appropriated and used in legal practice and academic philosophy in the same way. In the following sections, we survey the new directions proposed by the authors in this book, grouped by key themes, in order to try and find a common language for privacy in public space.

2. ROLE OF CONTEXT IN PUBLIC SPACE

In Chapter 3, 'Privacy in public and the contextual conditions of agency,' Maria Brincker identifies what she sees as a flaw in Nissenbaum's notion of contextual integrity. Brincker states that without taking the actions and agency of the people and things that are part of a certain context into account, the notion of *context* does not help much in understanding what this context is exactly made up of. Consequently, Brinker argues, we cannot truly understand or classify possible privacy zones, or breaches thereof. Harkening back to Warren and Brandeis, Brincker recalls that their article featured the argument that privacy harms are mental, rather than physical, in nature. She continues by stating that privacy should be regarded as relational, and not only contextual; the relations between people and between people and things matter, because they influence what individuals can do in a particular context—their agency. The connection with privacy harms is that this agency is not only to be found in objectively observable actions, but also in the mind. Brincker asks,

'what if the nature of our mind and agency is more procedural, more embodied, more culturally and socially embedded than what has hitherto been acknowledged in the privacy debate and law?'[2] Indeed, according to Brincker, the problem with current scholarship addressing privacy from a legal perspective is that it considers 'norms and codes of social conduct as somehow neutral and thus non-negotiable', which is highly problematic. Accordingly, we should not only account for context when dealing with privacy, but also actors' agencies within this context insofar as they (rather than the context itself) shape privacy settings.

To exemplify Brincker's point, consider for instance the difference between classical public CCTV setup in a city center versus a body-worn police camera: at face value, and even maybe legally, the body-worn camera and the CCTV represent the same thing, namely a state-owned visual and audio recording device in a public space, serving as a surveillance instrument; the similarity could suggest that the same privacy laws should apply. Yet, in practice, these two technologies introduce very different ways of acting and agency: in the case of CCTV, with static cameras stuck to a wall, a citizen cannot talk back nor avoid the potential gaze of the camera. In the case of the body-worn police camera, a citizen can 'read' the camera, and the direction of the gaze. Moreover, when being subject to recording, an official warning to the subject should be in place.[3] Even though CCTV and body-worn cameras might look similar at first sight, the two technologies implicate possible threats to privacy in different ways. With CCTV, the threat often lies in the lack of knowledge about exactly where the cameras are and how they work, and if they work at all:[4] they are at a distance and often unrecognizable. In contrast, with the body camera and other types of mobile cameras such as smartphone cameras, the perspective of the surveillance technology[5] used in public space is also literally changing, because they come in closer vicinity of the subject of surveillance. In fact, with the ability to make more dynamic, intimate and close-up visual

---

[2] Brincker, Chapter 3.

[3] In most countries, see e.g. the code of conduct for the UK police regarding bodycameras, available at http://library.college.police.uk/docs/college-of-policing/Body-worn-video-guidance-2014.pdf (accessed 6 January 2017).

[4] See T. Timan and N.E.J. Oudshoorn, 'Mobile Cameras as New Technologies of Surveillance? How Citizens Experience the Use of Mobile Cameras in Public Nightscapes' (2012) 10 *Surveillance and Society* 167.

[5] R.K. Lippert and B. Clayton Newell, 'Introduction: The Privacy and Surveillance Implications of Police Body Cameras' (2016) 14 *Surveillance and Society* 113.

and/or audio recordings with mobile cameras and to share these recordings immediately,[6] the set of norms and values around what we deem 'normal' behavior in public space is also changing. Although Brincker does not mention the metaphors of bubbles or spheres of privacy, the call to take context and agency into account does hint at some form of control of agents over what happens in their surroundings and thus at a certain delineation of privacy in public space. The subject of the potential encounter or infringement of privacy should have a say within a given context in respect to what they share, disclose or keep hidden.

In Chapter 5, 'Visually distant and virtually close: public and private spaces in the *Archives de la Planète* (1909–1931) and *Life in a Day* (2011)', Julia Hildebrand shows, via a historical media comparison, that the role of the camera and the viewpoint of the *infringer* also determine the boundaries of an (invisible) sphere or bubble—boundaries that are and can be manipulated under the auspices of different types of cameras. By comparing two projects from two different eras that both try to capture daily life around the world on camera, Hildebrand shows how norms of what is private in public space have changed. Her cases include a documentary film-maker in the early twentieth century and a YouTube-based documentary in the early twenty-first century. Hildebrand proposes that the process of filming and narration have completely altered over the course of the century, and that turning the camera inwards onto ourselves allows viewers or spectators to enter a private sphere. She argues that the 'personal space afforded by communication technologies is applicable in the sense that such boundaries are established from the external gaze in respect of privacy as something akin to a spatial bubble'.[7] Even though several authors from different disciplines have tried to capture what is happening here (e.g. therapy culture,[8] interiority,[9] desirable visibility and empowering exhibitionism[10]), Virilio's[11] explanation that this entrance into the private sphere via a mobile camera is not only a visual

---

[6] T. Timan and A. Albrechtslund, 'Surveillance, Self and Smartphones: Tracking Practices in the Nightlife' (2015) *Science and Engineering Ethics* 1, available at http://doi.org/10.1007/s11948-015-9691-8 (accessed 6 January 2017).

[7] Hildebrand, Chapter 5.

[8] M. McLuhan, *Understanding Media: The Extensions of Man* (MIT Press, 1994).

[9] K. Ball, 'Exposure: Exploring the Subject of Surveillance' (2009) 12 *Information, Communication and Society* 639.

[10] H. Koskela, 'Webcams, TV Shows and Mobile Phones: Empowering Exhibitionism' (2004) 2 *Surveillance and Society* 199.

[11] P. Virilio, 'Speed and Information: Cyberspace Alarm!' (2009) *Ctheory* 8.

experience but also a form of tele-contact is a fruitful one. If privacy, and particularly privacy in public, is relational, then the norms and values connected to privacy are indeed also changing, and thus altering what is expected within a context. As Hildebrand puts it, '[e]lectronic media have shrunken the distances between places and people, but also extended traditional sights and insights, eventually causing us to rethink "your own business"'.[12] Consequently, one of the key questions addressed by the authors in this volume is how to open up and reconsider the public space/private space distinction and how to think of new ways to regulate and protect privacy in public space.

3. REGULATION AND GOVERNMENTALITY IN PUBLIC SPACE

If we are to take into account the specificity of all the contexts, relations and forms of agency in which privacy concerns arise, how are we to regulate at a general level? One viewpoint of thinking about regulation in public space is provided by Karsten Mause, (Chapter 4, 'A politico-economic perspective on privacy in public spaces') who introduces economic theory and the concept of property to conceptualize what privacy in public is and might be(come). He shows how public space has never been an equal or homogeneous space, asserting that 'a "public space" is not created by nature; what is a public or private space is defined by those actors which have the property rights over the particular space'.[13] Discussing different stances from economic theory, Mause offers different ways of thinking about responsibilities that might help framing new or emerging privacy harms in public space, and enhance our understanding who should intervene or regulate in those cases. The *liberal-individualistic standpoint* argues that 'individuals themselves can already do a lot in this respect. However, if someone does not invest any time, effort or money in self-protection, then they should not be too surprised if they become the victim of some kind of invasion of privacy'.[14]

From this perspective, the regulation of privacy in public space would be up to individuals and their understanding of the risks involved in interacting with possible privacy-infringing technologies. Countering

[12] Hildebrand, Chapter 5.
[13] Mause, Chapter 4.
[14] *Ibid.*

Mause's argument, however, not all technologies can be or are user-controlled, and, as argued by Froomkin, the reasonable expectation test is shown to be increasingly unsatisfactory as a principle of regulation.[15]

Another perspective for regulation is to have government step in to regulate technologies in public space. However, the *market-liberal perspective* that can be witnessed in many current forms of government, would entail also the conviction that 'more government action seems to be not necessary to enable individuals to make use of the mechanisms of "self-protection" and "legal protection" in order to protect their privacy in public spaces'.[16] Mause asks how different governance mechanisms could work to protect privacy in public, including the question to what extent the state is necessary to protect citizens' privacy in public spaces. The two faces of government in both safeguarding privacy and posing a threat to our privacy in (private and) public spaces through its (securitizing) 'protective' role leaves us with an uneasy feeling,[17] which requires careful investigation and deliberation.

From a different perspective, Bert-Jaap Koops and Maša Galič in Chapter 1, 'Conceptualizing space and place: lessons from geography for the debate on privacy in public', delve into the discipline of human geography to look for conceptual directions that may inform the regulation of public space. They find that, while legal reasoning is fixed in a static and 'objective' understanding of private and public space, geography offers a much richer and more complex understanding of these notions: geography scholars have grappled for decades with the difference between spaces and places, what constitutes public space, and how public spaces are regulated. One useful observation for legal scholars is that due to technological developments, public space is changing from a space of clearly delineated, static places to a space of flows[18]—a network society.[19] This also changes how we think of a place: the authors argue that our social lives are increasingly taking place (also) via social media, instead of (only) in physical places per se. However, place-making in this network society of (information) flows does not happen in a vacuum; rather, it is a new layer on top of physical space. Herein lies the problem of privacy in public space: if social media and other forms of digital information start to mix with the make-up of public spaces that transcend

---

[15] See Froomkin, Chapter 8.

[16] Mause, Chapter 4.

[17] *Ibid*.

[18] Freely interpreted from Koops and Galič, Chapter 1.

[19] M. Castells, *The Rise of the Network Society: The Information Age: Economy, Society, and Culture* (John Wiley & Sons, 2011), vol. 1.

physical boundaries of walls, fences and other physical boundaries, what does this do to the privacy expectations in spaces? Here, Koops and Galič make a useful point, namely that 'since the public and the private spheres are interdependent and establish each other, the implications of privatization and securitization of public space for privacy also require reflection. Public spaces should not be conflated with public actions, nor should private spaces be conflated with private actions'.[20]

This means sometimes we perform acts in public space that are private, or not meant for everyone to witness or be a part of (for instance, talking with another person), while we also sometimes do things in the home that are public (see, for instance, the *Life in a Day* project mentioned by Hildebrand, where people broadcast part of their life from their home for the entire world to see). Koops and Galič show, however, that acts in public space are increasingly regulated and that the range of behavior that is allowed in public space is narrowing. Often, these regulations are not targeted at people as such, but rather to particular spaces. As put by Koops and Galič, these are measures that:

> include zero-tolerance policing, widespread surveillance and new public nuisance laws with legal instruments such as anti-social behaviour (ASBOs) and public space protection orders (PSPOs). PSPOs, for example, allow for broad powers of local councils to criminalize behaviour that is not normally criminal. PSPOs are also not directed at individuals; rather, they are geographically defined, making predefined activities within a mapped area prosecutable. Such regulation of public space discourages a wide range of spirited expression (labelled as 'anti-social' or 'escalating behaviour') and encourages stereotyped behaviour and 'social neutrality' in general.[21]

Stephen Zhao's description (Chapter 6, 'Exposure and concealment in digitized public spaces') of using such legal instruments to 'privatize' a particular part of a city or square to disallow political protests[22] exemplifies the fact that these legal instruments can have a profound effect on what can be done in a public space.

Koops and Galič further argue that the practices of how places are made—and by whom they are made—need to be studied empirically if we want to truly rethink how to create sensible regulation for privacy in public. Drawing on urban geography and surveillance studies can be informative in this endeavor, because of the insights they bring about how public spaces are dynamic and that a proper (legal) analysis should

---

[20] Koops and Galič, Chapter 1.
[21] *Ibid.*
[22] Zhao, Chapter 6.

account for combinations of things, people and places, since each combination constitutes new situations and different expectations of privacy in public. Zhao points out that many public spaces are semi-public in the sense that they might be privately owned or only accessible to some part of the public; for example, highways (requiring a driver's license) and airports or train stations (requiring a valid ticket to reach the departure gate or platform). While regulation of such spaces has to do with ensuring a level of safety (dealing with fast-moving physical objects), access to places like shopping malls and plazas is also selective, and increasingly so. Here, however, the motives for disallowing access are not based on safety in the strict sense, but on surveillance and sifting out those who might show certain unwanted behavior—think of skate-boarders or homeless people being banned from a public shopping street. Zhao further observes that the purposes of a place need to be at the core of its public-ness:

> The principal purposes of a public space determine *the main involvement* that is an intrinsic part of social occasion or the meaning of what is going on in that public space; such a main involvement is taken as preferential and prescribes an associated obligation for public space users.[23]

In other words, in order to properly participate in a certain public place, one must be aware of the rules attached to that place. Where not knowing these rules can also be a part of the excitement or social learning, a commonly known or general sense of the social conventions or rules in a public space makes that space generally approachable, usable. Zhao states that the process of access to, or acceptance within, a place involves a mechanism regarding how much a person gives away and shares, and how much is concealed. He continues:

> A good starting point to understand the impact of digitalization on privacy expectation would be to analyse *the significance of exposure and concealment* in public space … In this sense, concealment of personal information (as a dimension of the privacy concept) allows and supports plurality in community by eliminating the need for collective choice or an official public stance.[24]

A bit of fuzziness is needed in the contexts and rules of public space, in order to foster plurality and different types of public spaces to emerge.

Regulation of public spaces and privacy in those spaces has to do with levels of concealment, with rules of engagement in particular places, and

---

[23] *Ibid.*
[24] *Ibid.*

with allowing for certain levels of deviant or non-standard behavior without triggering (automated) alarm bells. However, how do rules and regulations, or technologies that mediate these regulations, actually infringe privacy of individuals or groups? Recall that Warren and Brandeis's article on the right to privacy[25] asserted that mental harms need to be accounted for, since they are perhaps even more injurious than non-mental privacy intrusions that the law did not already adequately cover. One of their main examples deals with a picture being taken and used in ways the subject of the picture did not consent to, leading to emotional or psychological stress and/or reputational damage due to misuse of the image. Where this example concerns a human photographer in public space, in which the act of recording and the uncertainty of what would happen after the recording were at the basis of the mental harm, it seems that, with the introduction of more obscure and distant forms of sensing, the act in itself (of taking 'data' rather than 'pictures') might be less impactful, because less visible and unknown. Yet the uncertainty of what will happen with this data once captured might be increasing, thereby also possibly increasing the level of mental harm.

Contemporary examples mentioned by Zhao and others in this volume refer to technologies that take footage or measure other factors from a distance, the subject often being unaware of this sensing. This brings us to another prevalent theme in the book: the body.

4. THE BODY AS INTERFACE IN PUBLIC SPACE

Several authors, including Angela Daly (Chapter 7, 'Covering up: American and European legal approaches to public facial anonymity after *SAS* v. *France*') and Michael Nagenborg (Chapter 2, 'Hidden in plain sight'), provide examples of the body as a locus of surveillance, and as an interface for sensing technologies in public space. On the one hand, it seems logical that the body is at the center of 'privacy in public' deliberations, since it is closest to what people are or have and is necessarily carried along when moving in public. On the other hand, we have seen that, in network societies, privacy may be more closely linked to a tele-presence and to information flows than to particular physical places. Yet, the body is in itself a physical place, or entity, moving around in public spaces. While this is nothing new, technology that can sense and measure aspects of the body from a distance is. Consider, for

[25] S.D. Warren and L.D. Brandeis, 'The Right to Privacy' (1890) *Harvard Law Review* 193.

instance, smart CCTV cameras that can run facial recognition software, possibly in real-time; WIFI-tracking systems in shops tracking mobile phones that are often carried close to the body;[26] gait analysis that turns walking patterns into unique identifiers;[27] infra-red cameras at airports that link the temperature of individuals to diseases or a (dangerous?) level of nervousness;[28] and DNA collecting devices that can analyze virtually any bodily trace in public.[29]

These technologies raise the question as to what extent remote body-sensing technologies introduce new privacy infringements in public. They also beg the question to what extent we can hide our body language, faces or body material in public spaces from such sensing devices. Several authors in this volume mention masking as an interesting concept of renegotiating privacy in public space.[30] Whereas the reasons for covering one's face or facial features might differ from religious to protest reasons, the result of obfuscating your face is that it might make you unrecognizable to distant-sensing devices. On the other hand, masks and other forms of face-covering also make one stand out in a crowd. Daly discusses the *SAS* v. *France* case on the banning of face-coverings. The key issues here are what degree of facial concealment is acceptable in a society, and what minimum requirements are necessary to ensure 'respect for the minimum requirements of life in society' or 'living together'.[31] Legally banning face-covering clothing highlights issues relevant for conceptualizing privacy in public: although politically interpreted as laws against wearing a *niqaab*, the law in general is aimed at all sorts of face-covering clothing. The arguments presented in this case are relevant for privacy in public space, highlighting the tension between, on the one hand, freedom of expression and religion and, on the other, a level of openness and minimal requirements of living together, which, according to the French state, includes being able to 'read' someone's face. In this case, however, 'a blanket ban on facial coverings was not

---

[26] A.S.Y. Cheung, 'Location Privacy: The Challenges of Mobile Service Devices' (2009) 30 *Computer Law and Security Review* 41.

[27] See L. Lee and W.E.L. Grimson, 'Gait Analysis for Recognition and Classification' in *Automatic Face and Gesture Recognition, 2002, Proceedings, Fifth IEEE International Conference* (IEEE, 2002).

[28] See e.g. T.C. Ormerod and C.J. Dando, 'Finding a Needle in a Haystack: Toward a Psychologically Informed Method for Aviation Security Screening' (2015) 144 *Journal of Experimental Psychology: General* 76.

[29] See Scherr, Chapter 9.

[30] Nagenborg, Chapter 2; Daly, Chapter 7.

[31] See Daly, Chapter 7.

[considered] necessary, except in circumstances where there was a "general threat to public safety" which the French government had not shown'.[32] Daly compares this case with anti-masking laws in the United States that are often used to disallow protests and aimed at the need (for law enforcement) to identify citizens in public space. Daly concludes that, as a result of the *SAS* v. *France* case, 'a state cannot regulate mask-wearing solely because it is frightening to other people'.[33]

Masking is also a key theme in Nagenborg's chapter, in which he offers a historical-philosophical analysis of the mask and the act of masking. The mask guarantees both anonymity and recognizability—the mask makes one stand out—and it is often worn to be recognized, although with a particular persona or message attached to it. A recent example is the *Guy Fawkes* mask,[34] used in protests to identify with the Anonymous activist/hacker group, which exemplifies this double role of masking. Masking is, however, one particular way to disguise oneself in public space, and Nagenborg also discusses other forms of obfuscation, such as anti-drone hoodies or certain types of face-paint to fool facial recognition software. Nagenborg calls these sensing technologies *anthropotelemetric,* which he explains as 'a kind of surveillance that allows taking measurements on the human body from a distance'.[35] Where the distant measuring and assessment of the face in particular, and other parts or attributes of the body more in general, might be seen as the last step towards ubiquitous recognizability, the body can also form a new place of resistance: '"passive sabotage"—not by destroying the technological surveillance systems, but by denying anthropotelemetric surveillance access to the site on which it operates: our bodies'.[36]

Another aspect of body-related surveillance is offered by Albert Scherr in Chapter 9, 'Privacy in public spaces: the problem of out-of-body DNA', where he examines the limited legal protections against DNA tracing by, for instance, law enforcement agencies[37] in the United States. The development of DNA tracing technology allows users to capture and analyze DNA to such a level of detail that all sorts of personal details can

---

[32] *Ibid*.

[33] *Ibid*.

[34] See G. Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (Verso Books, 2014).

[35] Nagenborg, Chapter 2.

[36] *Ibid*.

[37] Scherr also mentions private detectives and amateur genealogists as parties interested in DNA tracing.

be identified and, to a certain degree, an individual's physical characteristics can also be derived. Out-of-body DNA is seen by many courts as waste material: something one has given away and is thus free for the taking and analyzing. This is problematic, since 'out-of-body DNA retains a kaleidoscope of information and identity that is personal, powerful, intimate, shared and timeless. It is also information that is useful to others for various identification, research and commercial purposes'.[38] While people can protect themselves to some extent from distant (visual) sensing technologies, it is much more difficult to prevent leaving DNA traces in public space. Scherr argues that US courts have applied the reasonable expectation of privacy test wrongly in out-of-body DNA cases, and that, at a minimum, more public awareness and access to information is needed if this type of DNA tracking is to stand this test.

A recurring theme in the chapters by Daly, Nagenborg and Scherr is the level of individuals' control over actions in public space. In their contributions, they describe situations that are changing from being harmless to 'worth recording' (a veil, a DNA trace, a mask). All three chapters discuss the changing nature of 'being in public space' and possible new technological ways of being read or sensed in public space from a distance, or over time. This can lead to new or more severe privacy infringements, and legal frameworks currently in place are often inadequate to provide proper protection against these infringements. Moreover, technological developments in remote sensing and DNA analysis go hand in hand with a changing political climate in the European Union and the United States, allowing for more state interference in public space. Where some technologies of measuring the body have sparked new forms of resistance or protection by citizens themselves, technologies such as DNA tracing call for a stronger response from law-makers. This brings us to the fourth theme that can be carved out of the rich variety of chapters: the developments in law and regulation regarding privacy in public and the main challenges for regulators in protecting privacy in public space.

5. PRIVACY MITIGATION AND REGULATION IN PUBLIC SPACE

The role of regulators in shaping privacy in public space ranges from creating new privacy-protecting laws to transparency obligations and

[38] Scherr, Chapter 9.

other forms of regulation. To meet the challenges highlighted by Scherr in applying the reasonable-expectation test for privacy in public (more public awareness and access to information), Michael Froomkin (Chapter 8, 'Privacy impact notices to address the privacy pollution of mass surveillance') draws inspiration from another legal domain that might prove fruitful as a basis for thinking about regulating privacy in public space: environmental law. A prominent feature of environmental law in the United States is Environmental Impact Statements (EISs). These are disclosures or notices on development plans of, for instance, industry, with a focus on the project's impact on the environment. The notices are publicly available and allow citizens to have a say. Moreover, these EIS requirements call for regular (for instance, yearly) reporting on the impact of the project on the environment.[39] Projecting the logic of EIS onto privacy and surveillance questions, Froomkin asserts that 'surveillance is polluting our privacy', and that the current privacy doctrine in the United States lacks a proper instrument to deal with the proliferation of mass surveillance. Instead of looking at the European model, such as Privacy Impact Assessments and compliance enforcement with EU data protection regulations, the United States could adopt Privacy Impact Notices (PINs) that are a variant of the EISs. These PINs would 'describe the costs and benefits of proposed surveillance. This will not only enrich public debate but will also help identify the aspects of data collection that may need regulation'.[40] PINs could form a new tool to enforce privacy laws and provide a potential economic benefit: not only would we gain insights into the actual costs of (a loss of) privacy; companies in turn could also use these notices to their competitive advantage.

Both Meg Leta Jones (Chapter 10, 'The Internet of other people's things') and Froomkin warn the reader of the speed of proliferation of novel ICTs and the upcoming Internet of Things (IoT), in which it will be difficult to distinguish public from private data and content from metadata. In her contribution, Jones, dubbing the coming world of connected devices an Internet of Other People's Things, explores the differences and pros and cons of data protection regulations in the United States and the EU and how well these legal instruments would work in a context of IoT and smart publics. One clear difference is the focus on regulation for companies that does not block innovation (US) versus a stronger protection for end-users (EU). An underlying question for privacy in public is who the actors or stakeholders are in publicly

[39] See Froomkin, Chapter 8.
[40] *Ibid.*

deployed technologies and who owns data produced in or taken from those spaces. When boundaries between data controllers and data processors are blurring, the current models of privacy regulation are under pressure. The EU framework focuses on end-users' informed consent and lifecycle data management, the latter meaning that the data processor should inform end-users about all processing of one (set of) data throughout the entire life of that data.[41] Such regulation, Jones argues, could seriously affect technological innovation. Yet, in an Internet of devices that might not all interact with us via screens (rather, for instance, via voice, facial or gesture recognition), the EU approach might offer a more stable way forward, because it is not based only on a narrow interpretation of consent (as would be the case in the United States).

In general, the regulation of privacy in public space is, in both the EU and US systems, pivoting around data collection, often not acknowledging that privacy infringements might go beyond data collection and processing and can be found also in acts of recording, monitoring or manipulating possible (inter)actions in public space. It can prove fruitful for the discussion of privacy in public to develop a sense of what the consequences are of privacy-infringing technologies in public space from a broader social-ethical perspective, rather than merely through the lens of data protection. One way of doing so is to ask what the role of privacy in public is or can be. That question will be discussed, from different angles, in the chapters that follow.

---

[41] See P. Korenhof, J. Ausloos, I. Szekely, M. Ambrose, G. Sartor and R. Leenes, 'Timing the Right to be Forgotten: A Study into "Time" as a Factor in Deciding about Retention or Erasure of Data' in S. Gutwirth, R. Leenes and P. De Hert (eds), *Reforming European Data Protection Law* (Springer, 2015).