

Who is looking at what – Digitization, CCTV surveillance and privacy

2 December 2020 5 min read

by Ahmore Burger-Smidt, Director and Head of Data Privacy Practice and member of the Competition Law Practice

*“Look you, sir,
Inquire me first what Danskers are in Paris,
And how, and who, what means, and where they keep,
What company, at what expense; and finding
By this encompassment and drift of question
That they do know my son, come you more nearer
Than your particular demands will touch it”*

Hamlet (II.i.6–12)

CCTV surveillance aims to achieve two distinct outcomes and these should not be left out of the equation when considering the concept of CCTV surveillance in terms of privacy legislation. On the one hand it aims to keep disruptive incidents and aspects out of the public arena, and on the other hand it aims to protect private life from the crippling effects of the external gaze.^[1]

But what is a public space? Indeed public space plays an important role in our day to day life, but it is not always clear to pin-point exactly.^[2] For instance, Moeckli proposed that the term refers to space, which is accessible to, and can be used by everyone without conditions (e.g. free of charge) at any time, and that whether a given place is part of public space or not depends on accessibility rather than ownership.^[3]

Definitions of public space could differ, but one thing remains and that is the profound trend of digitalization of these spaces.^[4] Digitalization has been taking place in multiple forms because of the ever increasing deployment of various digital technologies for many purposes. This introduces fundamental changes to what a public space actually means from a privacy perspective. One clear example of digitalization of public spaces is the popular use of CCTV systems, including CCTV cameras. This inevitably results in mass surveillance of one kind or another.

CCTV cameras are nowadays ever present in public parks, squares, roads, highways, schools, airport, to mention a few. Often forgotten and not seen CCTV surveillance happens through the use of small or hidden devises, like tiny cameras on ATMs and in elevators.^[5] But also, other initiatives bring about privacy-invading actions through the collection personal data, even though they aim to be neutral in nature. Think about Google Street View that uses cars i.e. mobile data collectors, to record street views and collect geolocation data. In this process, they also collect other data such as emails, usernames, videos, and other personal information from unsuspecting computers. Google even collected MAC addresses, network SSIDs (user assigned network ID names), and WiFi transmission data by interception.^[6] As a consequence, Google was accused of serious privacy invasions in both public and private spaces.^[7]

The world is evolving at a rapid pace and the digitalization process has been facilitated by the Internet of Things (IoT), that connect all smart or non-smart devices, whether in public or private spaces.

Digitalization of public spaces can offer many positive advantages. It can help improve business security. It can be installed for the purposes of crime investigation and anti-social behaviour prevention. While CCTV installation is effective to reduce shoplifting and other anti-social behaviour for instance, the accountability when it comes to CCTV devises has increased.

Public space surveillance allows for personal data to be collected without data subjects’ consent; previously presumed anonymity can disappear. Therefore, digitalization of public spaces enables what Allan Ford^[8] refers to as ‘unilateral invasions of privacy’. No longer to you and I, the data subjects, decide how information is collected, stored and disseminated, but instead outsiders make such decisions based on their judgment of potential benefits and costs.

The crux of digitalization of public spaces is, as Allan Ford notes, the creation and acceleration of more information flow,^[9] including information collection, processing and dissemination. Prior to CCTV cameras recording areas for security reasons, personal information could not be that easily collected, as easily stored for long periods, transferred and disseminated instantly, or processed on a large scale like today. Personal information collection, dissemination, analysis and retention have the ability to be combined in ways that we have never imagined.

This presents privacy challenges, amongst others, misuse and abuse of personal information.

It is often said that law and legal processes respond slowly to change. This is because it is important to foster legal certainty. However, despite this, we will learn as times goes by how the Information Regulator will approach digitization and the use of CCTV surveillance that is ever present in our environment as walk the streets of our beloved country – will this be embraced or not?

^[1] T. Nagel, *Concealment and Exposure: And Other Essays* (Oxford University Press, 2002) 15

^[2] V. Mehta, ‘Evaluating Public Space’ (2014) 19 *Journal of Urban Design* 53, 54

^[3] D. Moeckli, *Exclusion from Public Space: A Comparative Constitutional Analysis* (Cambridge University Press, 2016) 30, 34

^[4] Timan, T et al *Privacy in Public Space* (Elgar Law, 2017, 144)

^[5] *Ibid*

^[6] EPIC, ‘Investigations of Google Street View’, <https://epic.org/privacy/streetview/> (accessed 23 November 2020)

^[7] *Joffe v. Google, Inc.* 729 F.3d 1262 (9th Cir. 2013), available at <http://harvardlawreview.org/2014/04/joffe-v-google-inc/> (accessed 23 November 2020)

^[8] Ford, Roger Allan, Unilateral Invasions of Privacy (April 21, 2016). 91 Notre Dame Law Review 1075 (2016), Available at SSRN: <https://ssrn.com/abstract=2768531> (accessed 23 November 2020)

^[9] *Ibid* 1076

[Download PDF](#)



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)