

OXFORD

ARTIFICIAL INTELLIGENCE AND HUMAN RIGHTS

edited by
Alberto Quintavalla
Jeroen Temperman

Search in this book

CHAPTER

12 Artificial Intelligence, the Public Space, and the Right to Be Ignored

Andrea Pin

<https://doi.org/10.1093/law/9780192882486.003.0012> Pages 177–192

Published: September 2023

Artificial Intelligence and Human Rights

Jeroen Temperman (ed.), Alberto
Quintavalla (ed.)

<https://doi.org/10.1093/law/9780192882486.001.0001>

Published: 2023

9780191976797

9780192882486

Online ISBN:

Print ISBN:

Abstract

Artificial intelligence (AI) is capable of occupying, patrolling, and even controlling physical space. The issue of automated facial recognition (AFR) is only the most visible aspect of a much broader phenomenon, as computer vision empowers private and public entities to capture a great deal of information that is available in the public sphere in an unprecedented way, challenging how public law conceives public spaces. Despite significant differences, various legal orders are similarly concerned with this phenomenon, which is shifting the boundaries between what is private and what is public. This chapter (i) explains how, because of AI, public spaces are morphing into something new; (ii) argues for the protection of anonymity; (iii) demonstrates the failures of several contemporary theorisations of public places and that the standard privacy paradigm fails to provide sufficient protection; and (iv) proposes a new approach to the topic. Drawing from different legal orders, it ultimately argues for a reconceptualisation of the public sphere in a way that mitigates the impact of AI on social life.

Keywords: Confidentiality

Subject: Settlement of Disputes, International Responsibility, Human Rights and Immigration, Human Rights, International Criminal Law

Collection: Oxford Scholarly Authorities on International Law

1 Introduction

When they kicked off the endless debate on privacy, Warren and Brandeis complained about the invasion of ‘the sacred precincts of private and domestic life’.¹ They were desperate to insulate individuals from the eyes of private entrepreneurs who took advantage of technological advancements to sell pictures of people caught within private domains.

The right to privacy later morphed into a capacious legal device that—in several legal settings—would protect individuals and groups against private and public powers alike. Technology now allows for detecting, gathering, and processing information about individuals’ identities, behaviours, habits, and characters. Rules in place in certain legal settings, such as the European Union (EU), have severely limited the capacity to gather sensitive personal information such as an individual’s biometrics, thereby limiting what technology can do with people’s identities and personal details.² Such regulations showcase widespread awareness that ‘[a] society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy’.³ What time did not fix, however, was the vulnerability of people in public spaces.

Artificial intelligence (AI)-based technologies can monitor and process information about individuals who find themselves in public places. Several jurisdictions impose constraints on such phenomena, but these are certainly not sufficient. Information gathered in public places is relevant even when individuals themselves are not identified. Technology can detect how fast people walk, guess where they are heading, whether they have something in their hands, or identify what flags they are holding while they protest. Knowing what people hold in their hands ↵ while they cross a certain square, whether they use sunglasses, or their walking pace, is a valuable piece of information—it may help identify patterns, habits, and tendencies, which inform the economic value of an advertising campaign, or demographics.

The scholarship in the field has devoted its attention to the legal status of public places only rarely.⁴ Constitutional theory has mostly focused on the protection of private places, private lives, and the identity of individuals. Many of those who work in the ever-expanding field of law and tech have also looked elsewhere, focusing on the management, the risks, and the protection of data on the Internet. Especially within the EU, a strong sensitivity to what happens online has emerged:

contemporary data protection law [has been analogised] to environmental regulation. It seeks to protect the democratic ‘commons’, that is, the moral democratic, and cultural environment, as opposed to the natural, physical environment.⁵

Unfortunately, this approach may be misleading: for many tech giants, ‘the key move today is off the Internet’.⁶

The lack of interest in public places is alarming in light of the contemporary widespread recourse of surveillance systems.⁷ It is in public places, in fact, that AI’s capabilities ‘blur the line between being protected and spied on’.⁸ AI-based technologies, new global markets, and law enforcement strategies combine to render public places ideal environments for mass surveillance and monitoring.⁹ Although scholarship cursorily calls to reconceptualise public spaces as shared environments in which individuals and groups enjoy mutual rights and responsibilities,¹⁰ individuals and society at large do not enjoy strong safeguards against this surveillance. Most of the available protection relies on privacy which, unfortunately, ‘is said to be forfeited as soon as a person ventures out in public’.¹¹

p. 179 Because of this approach, public places—and places that are publicly observable—have not enjoyed the protection that is accorded to what does not happen in plain sight.¹² The EU may enjoy the reputation of having established a regime of data collection and processing that prioritises human rights, and which many non-EU citizens praise and long for.¹³ This protective approach, however, has not incorporated a significant preoccupation with the transformation that public places are enduring because of AI’s power and pressure.

The massive deployment of AI-based technologies in public places around the world is hardly surprising. If, as Shoshana Zuboff maintains, ‘companies can stake a claim to people’s lives as free raw material for the extraction of behavioral data’,¹⁴ public places are the perfect place to gather data, as companies can collect it even from those who are not connected to the Internet. Public spaces are areas within which people share their lives and will unavoidably be exposed to AI-based tools, whether they use them or not.¹⁵ If the new technologies are commonly said to remain in need of a ‘guiding philosophy’,¹⁶ this is especially true of the status of public places.

This chapter aims to heed these calls for a reconsideration of public spaces and contribute to filling the vacuum in comparative constitutional scholarship. It will proceed by analysing why the topic is so relevant from a social perspective (section 2). Then it will summarily review current contemporary scholarship when it comes to conceptualising public places and the insufficiency of the narrative of privacy in achieving that goal (section 3). Drawing on a variety of legal systems and an array of judicial rulings, it will identify the key legal principles that need to be taken into account in order to devise a more refined understanding of public places that would be helpful in regulating the deployment of AI-based tools (section 4). It will finally make the case for a broader conceptualisation of the issues at stake and for going beyond a purely individualistic approach to the subject (section 5).

2 Reaping the Benefits of AI in Public Spaces

p. 180 Nowadays, public and private institutions alike are exploiting AI's immense capabilities to monitor and patrol public spaces for a variety of purposes. Just to name a few examples drawn from significantly different environments, China has engineered a comprehensive system of public and private surveillance that connects ↪ private devices with video surveillance cameras, which account for 40 per cent of the total number of surveillance cameras in the world.¹⁷ Australia's anti-pandemic policy similarly includes drones that utilise a thermal recognition technology.¹⁸ Moscow has a new facial recognition tool throughout the city,¹⁹ and its schools are integrating a facial recognition system that goes under the telling name of *Orwell*.²⁰ The United States (US)-based *Clearview* Corporation has developed a face recognition software that compares live imaging with pictures of human faces that are already available online through social media and that has been so successful that twenty-four law enforcement agencies outside the US have at least experimented with it.²¹

Of course, such massive deployments of AI-based surveillance among law enforcement agencies spark controversy. Living in an established democracy does not reassure people about these practices, as they perceive themselves as being increasingly monitored, while their faces are restlessly compared with lists of persons of interest, suspects, or criminals.²² After enjoying initial success among law enforcement bodies, *Clearview* has experienced massive backlash and is being rolled back in more than one US state. A recent British case concerning facial recognition software deployed by South Wales Police for two years—and that was able to capture forty images per second—ended up in the Court of Appeal of England and Wales, which found this practice unlawful on a variety of grounds.²³

At least in the West, the concern with AI-based surveillance of public places has focused on one single aspect, namely the identification of individuals. But AI's capabilities do not stop there. Individuals and groups produce crumbs of data of any kind that can be exploited.²⁴ Identifying individuals' and groups' patterns, habits, or trajectories may serve economic or social purposes that have an impact on how citizens live their lives and socialise. Facial analysis systems can measure body temperature, heart rate, or minor facial details such as pupil dilation, drawing inferences about an individual's emotional state.²⁵ Public surveillance systems can ↪ identify and predict walking patterns.²⁶ Private corporations can harvest their knowledge of where people tend to look or stop by while walking, as this may be considered a meaningful detail to estimate what portions of a territory are more economically valuable. Detecting how many people flow into a city may help in designing urban mobility.

p. 181

Pervasive systems of surveillance do not always equate with Big Brother, of course. In recent years there has been a growing interest in leveraging the capacity of monitoring public places for purposes of utmost importance such as fighting terrorism and the pandemic.²⁷ Monitoring public places may help prevent gatherings that would spread the virus and even identify people who violate quarantine or lockdowns. How far surveillance systems can go in patrolling public places is therefore an extremely timely issue, which does not seem to have received adequate responses so far. Because of the overwhelming importance given to privacy and the Internet, the phenomenon of public places surveillance lacks adequate analysis. The flaws in this approach are reflected in the judicial rulings that often fail to address and even to understand the importance of preserving and protecting not just individuals in public places, but public places themselves, for what they have traditionally offered to citizens.

3 The Problem with Privacy in Public Spaces

Despite their quite different approaches to the topic, China, the US, and the EU share some commonalities. Their legal systems focus either on individuals or private precincts as the two main frameworks for the protection of data: what concerns legal systems seems to be either the protection of individuals or their dwellings. This does not happen by accident: as legal scholarship has largely understood privacy as a shield for the 'liberal self',²⁸ which is centred around the individual in isolation, what happens in places that are accessible to anyone is pushed aside in the theory. Little therefore is said about the protection of public places from the intrusion of surveillance and detection systems. What is public seems to be exposed to public and private powers.

p. 182 Despite widespread silence on the matter, AI-based surveillance techniques deployed in public spaces challenge the scholars' overwhelming preoccupation with ↪ AI's impact on privacy and private precincts. Luciano Floridi probably captured the spirit of the time when he coined the idea of *onlife*²⁹—individuals and societies being constantly in flux between the physical world and the online dimension, with their data spilling from the former to the latter without them being aware of it. But the idea of protecting public places is not just about putting the *onlife* dimension under check and limiting the flow of information from and about an individual's physical life to their online dimension. In fact, public places are inhabited by people who may not be—temporarily or permanently—online. Although this is becoming increasingly rare, as more and more people connect via the Internet every day, it is possible to think of individuals and groups not willing to engage in online activities. But since they still live a physical life, peoples' data can be gathered and processed when they are in public places. AI's capabilities can invade physical space and life, as the Pokémon Go saga displayed when millions of individuals around the globe reorganised their movements in order to catch virtual creatures.³⁰ Pokémon Go used virtual reality to make the videogame imaginary subjects appear in real locations. Videogame users captured them by taking snapshots of the environments within which such objects suddenly appeared. The process, which caused public disturbance and affected how users navigated public places, thus allowed the corporation to record massive amounts of pictures of private and public places from a variety of angles.

As AI-based systems of surveillance are 'minimally invasive',³¹ cities are the perfect scenario wherein various AI-based mass-monitoring systems can be deployed without imposing physical limitations or restraints on individuals.³² Although people gather, move, and interact with each other on a physical level in public mostly within the urban dimension, political institutions and scholars often overlook this phenomenon, as constitutions and constitutional studies regard cities and urban aggregations as mere parcels of broader territories.³³ AI technologies are therefore radically transforming urban environments, with little or no consideration from constitutional theory.³⁴

p. 183 Smart cities are a concept that captures how deeply '[m]obile and infrastructural components work together' in surrounding everyone's life³⁵ and silently prompting them to take up new habits. Such changes in how people live in public places may stem from private and public powers alike. Although public institutions can use ↪ smart-city technologies for public welfare, their massive public surveillance can, nonetheless, provoke significant alterations to individual and social life. Smart cities have thus become a matter of concern,³⁶ as they appear to mimic Bentham's ideal of panoptic surveillance.³⁷

The identification of people who enjoy or cross public places is both one of the most contentious topics and among the most sought after applications of biometric technology.³⁸ Such technology is a matter of contention because public surveillance can have a 'chilling effect'³⁹ on a variety of fundamental freedoms, including 'speech, expression, and association'.⁴⁰ It can discourage individuals from participating in public gatherings or protests for fear of being identified and recorded, as people may be concerned with how public institutions could exploit their data.⁴¹ Surveillance of public places can go as far as looking for individuals

who simply jaywalk, or make graffiti.⁴² AI tools can also covertly influence and nudge people in a variety of ways by integrating stealth stimulations in a public environment.⁴³

Although AI surveillance and monitoring systems seem to work passively, as they simply record and process information that is already available, it is actually the bystanders who are passive: they feed AI technologies without being approached and given the opportunity to choose whether they agree to share their data.⁴⁴ The impact of such an imbalance of roles on the social makeup and the political culture has become particularly evident after individuals in the United Kingdom (UK) were fined because they tried to avoid being captured on cameras.⁴⁵ It was their simple reaction to the deployment of AI-based surveillance techniques that discredited them and singled them out as individuals potentially engaging in unlawful activities and disrupting law enforcement procedures.

p. 184 The deployment of AI tools in public places can disproportionately impact particular social classes, exacerbating economic inequalities. Wealthier individuals or families can expand their privacy by residing in extensive real estate properties, using private transportation, and living more secluded lives.⁴⁶ This would expose ↪ them to less surveillance than people of lower socio-economic status, who might live a more exposed social life, as they need to use public transportation, commute more frequently, and share more public facilities or services.⁴⁷ The legal treatment of such technologies is, therefore, critical to preserve everyone's equal capacity to develop and enjoy social relationships,⁴⁸ regardless of social strata.

4 Going Beyond Privacy

Legal systems are clearly going in different directions in terms of promoting or limiting the deployment of surveillance technology. China envisions a near future within which it will be able to almost immediately identify any one of its 1.3 billion citizens.⁴⁹ Several US states are going the other way, banning or limiting the usage of drones, body cameras, and other tools previously deployed to monitor public places and identify individuals through AI-based surveillance techniques.⁵⁰ The EU famously protects privacy in the form of personal data in the public sphere and is anticipating discouraging AI-based surveillance that deploys facial recognition systems as a high-risk practice for the sake of such data protection.⁵¹ The AI Bill that is under consideration by EU institutions certainly considers public surveillance as a potentially high-risk practice, but does not rule it out nor does it seem to really consider factors that go beyond the identification of individuals. It therefore still omits a thorough conceptualisation of what surveillance of public places entails for law and society at large.

Articulating the need to preserve a level of privacy and discretion for individuals in public places has been quite challenging. As someone has noted, what is at stake within this scenario seems to be different from 'conventional privacy'.⁵² Privacy, in fact, is usually believed to protect 'people, not places'.⁵³ And that is where the problem begins.

p. 185 As the US Supreme Court has stated, the expectation of privacy 'generally ends when one enters the public'.⁵⁴ The possibility of being observed by the naked eye dissolves such an expectation, in the US as elsewhere.⁵⁵ The often implicit assumption underpinning this approach asserts that people cannot reasonably expect to enjoy privacy while they socialise or occupy shared places, so they should simply ↪ avoid doing in public what they prefer not to share with others.⁵⁶ In other words, when an individual is in public, it is her responsibility to keep information about herself discreet.

This assumption, however, has meant relinquishing most safeguards whenever an event or a person is observable with the naked eye. Even surveillance from above—which is not exactly what 'reasonable people' would expect—has been affirmed as lawful when it covered public spaces.⁵⁷ In fact, even the English and Welsh Court of Appeal in *Bridges*—the very judgment that found the deployment by South Wales Police of

face recognition technology to be unlawful in light of EU law—did not rule out this possibility. It simply found that the deployment itself left too much discretionary power to the police in selecting the individuals that it was attempting to locate and further found that the software that had been deployed could embed discriminatory biases.

The problem with privacy is how a century of scholarship, judicial rulings, and legislative activities have construed it. It is a capacious and multifaceted term, as it includes both the ‘physical and psychological integrity’ of a person, thereby embracing ‘multiple aspects of the person’s physical and social identity’.⁵⁸ However, it seems to end where the public begins. Despite significant historical differences, legal traditions as diverse as those of Italy,⁵⁹ Ireland,⁶⁰ New Zealand,⁶¹ the UK,⁶² and the US—just to name a few—seem to agree on one point: privacy claims in public places are hardly defensible because what meets the eye obviously cannot be said to be private, or to be believed to be private. This approach deprives even facts or details that were visible only under very special circumstances of protection: the Irish High Court found that events taking place within private precincts did not enjoy privacy if they were observable with the help of a ladder,⁶³ while the US Supreme Court stated that what a helicopter could notice within private properties did not infringe privacy expectations.⁶⁴

The average theorisation of what a privacy violation would consist of also weakens the articulation of privacy to cover public places. The concept of privacy usually associates the infringement with an act of ‘intrusion’⁶⁵ or ‘invasion’⁶⁶—those violating someone’s privacy are perceived as ‘intruding’ upon their sacred precincts. Nothing of this kind occurs in public.

p. 186 Admittedly, scholarship has occasionally urged to reconceive and expand privacy to cover information gathered in public places,⁶⁷ especially after AI-based surveillance systems took off. Scholars have become increasingly aware that such technologies are altering the self-perception of individuals whenever they find themselves in public places.⁶⁸

It is common sense that social life requires that individuals give up their expectation of enjoying the same degree of privacy that they expect in private.⁶⁹ When people are in public they are vulnerable, in the sense that they can be observed and noticed. However, there is a general expectation that such an event is unlikely to happen. People, in fact, do not imagine ‘that they are being observed any more than casually and by a limited number of people’.⁷⁰ But this is not the case anymore with AI-based surveillance. Such technologies can notice an individual’s unique features on a large scale: for instance, the automated facial recognition system deployed by the South Wales police was able to scan forty faces per second.⁷¹ Moreover, events and people that take place or appear in public can be recorded and processed; recording an event or a detail ‘is different in kind, not merely in degree, from being able to relate it verbally or even by way of a sketch’.⁷² Being noticed and remembered, which would usually happen by accident and cursorily, becomes the standard.

The European Court of Human Rights (ECtHR) has already tried to expand the protection of privacy in public places in the context of surveillance. Although admitting that ‘[a] person who walks down the street will, inevitably, be visible to any member of the public who is also present’, it has nonetheless recognised that technological monitoring of an area may raise privacy issues ‘once any systematic or permanent record comes into existence of such material from the public domain’.⁷³

However, the need for a sort of privacy in public looks substantially different from what one would expect when she is in private. If we look for the interest in not being spied on while in public, we would probably find a better definition of it in the concept of ‘anonymity’,⁷⁴ namely the unlikeliness that an event or a detail is connected with a specific individual or a group. Such anonymity is critical, as it enables people to socialise and participate in initiatives and events of public significance, such as protests, without fear of retaliation or other types of adverse consequences.⁷⁵ More broadly, it preserves people and their habits from being put

p. 187

↳ under a spotlight. Anonymity serves as a ‘breathing space’ for individuals who find themselves *in* a public place.⁷⁶ It is, however, possible to conceptualise also the anonymity *of* public places: what happens in publicly accessible areas is not expected to be processed and remembered. Public places have thus provided people with breathing spaces, but also society at large with areas of socialisation precisely because of the expectation that people and social relations enjoy anonymity within them.

AI-based surveillance undermines anonymity *in* and *of* public places. Anyone can be recognised by chance—or a certain event can be spotted and memorised by bypassers or bystanders. As has been contented, ‘[m]ost people reasonably make this assumption: either that they are not noticed, or that any single observer can observe and harbor only discrete bits of information’.⁷⁷ Public spaces’ surveillance systems that use AI make certain what should be unlikely. They spot, identify, and record events. They can gather and process them, making inferences that may have a huge-scale impact on those who are in those places. In fact, AI allows for the gathering, recording, storage, processing, and analysis of a potentially unlimited amount of information.⁷⁸

This is where the concept of ‘*confidentiality*’ may usefully kick in and supplement the legal analysis with additional factors. Courts around the world have more than once danced between confidentiality and privacy, sometimes arguing that the two concepts capture the same essence.⁷⁹ As Lord Phillips has noted, however, there is a gap between these two concepts. Confidentiality requires that someone is informed about someone else’s sensitive information, and a breach of confidentiality happens when the information is spread to other people.⁸⁰

Strictly speaking, this concept of confidentiality certainly does not respond to the challenge of surveillance in public places. Those who walk a certain square do not willingly share their information with the cameras and other devices patrolling a certain area, and such sharing does not establish a duty of confidence.⁸¹ But they still do share information, which may bear consequences, even at the aggregate level. The information about the shopping behaviours, ideological inclinations, or habits of a certain portion of the population can affect people’s lives, as they can become targets of economic or political campaigns.

p. 188 As some judicial rulings have acknowledged, a capacious concept of confidentiality helps at least in understanding that there are boundaries regarding what can be done with such data. In fact, as the Court of Appeal of England and Wales has ↳ stated, ‘[a] duty of confidence will arise whenever the party subject to the duty is in a situation where he knows or ought to know that the other person can reasonably expect his privacy to be protected’.⁸² Or, in the words of New Zealand’s Court of Appeal, ‘a pre-existing confidential relationship between the parties is not required for a breach of confidence claim. The nature of the subject matter or the circumstances ... may suffice to give rise to liability’.⁸³ Similarly, a sort of mutual expectation of confidentiality among people in public places who most of the time do not know each other, may be said to generate the duty not to further disclose and utilise the information.

The England and Wales’s and the New Zealand’s court statements help understand how public places should be treated. If people have an expectation of anonymity, then what is captured by surveillance systems might be seen as a sort of confidential information. And, as AI-based surveillance technology can gather crumbs of information to infer what types of individuals are walking down a certain street or where they are heading, the ‘subject matter’ covered by confidentiality may include bits of information that may appear to be without value, but the aggregation of which may be economically and politically valuable.

Attempts to tinker with the concept of privacy and make it broad enough to encompass what happens to the individual in public seem to be fraught with contradictions. At best, it limits what surveillance systems can capture, record, and process, but not the phenomenon of surveillance in itself.⁸⁴ Looking at the case law, it is quite difficult to square the circle and provide individuals with privacy in public places. Such a sea change requires going beyond the ideas of private precincts, intrusion, invasion, and observability.

What the scholarship that has been trying to expand the notion of privacy to cover public places certainly got right is that current technologies are different from the occasional chance of someone spotting someone else that is known to her in the crowd, or a specific detail of an individual. The difference is not a matter of degree: it is rather a matter of quality. In fact, it changes the character of public places, depriving them of their anonymity.

p. 189 Anonymity may not protect individuals and events that happen in public, as they are both observable and noticeable. But this is where confidentiality makes a contribution to the subject, especially if—as some have maintained—confidentiality may arise not just from a contract, but also from someone's expectations in light of the specific circumstances. Although it is construed as an obligation among ↪ specific persons, confidentiality certainly fosters a sense of discretion, conveying the need that what is seen is not spread and exploited.

5 Going Beyond Individualism in Public Places

Protecting public places from boundless exploitation of information regarding people gathered through pervasive AI surveillance and monitoring technologies does not go simply beyond the idea of privacy. It also goes beyond the idea that the individual is the only subject worthy of legal protection. This is another important step that is worthwhile considering in more depth.

Privacy protects *personal information*. Most jurisdictions protect certain information because it belongs to individuals. As long as information is disconnected from individuals, it loses much of its protection. The same is true about confidentiality.

AI-based surveillance is not problematic just because it identifies individuals and singles out specific details about them. Its impact is much broader than that. In fact, it can identify patterns, average age, walking speed, where people tend to go, where they usually slow down, and what they hold in their hands.

This type of information is of great importance for private businesses and public institutions alike. The speed of pedestrians can help estimate the worth of a billboard; their average age can supply information about the best shops to locate in a certain area; the walking patterns can help coordinate urban traffic and planning; from the way people dress AI can infer their wealth and cultural and political leaning; their skin colour can help determine if some urban areas are de facto racially segregated.

Such information may not just be of great value. It can also pose grave threats to the well-being of residents. Urban policies and private corporations can use this information to target selected strata of the population and discourage, encourage, or nudge certain economic classes into specific behaviours. They can quietly manipulate urban societies.

p. 190 The threat is grave also when the population is conscious that AI-based surveillance tools are patrolling public areas. Public places are both areas of anonymity as well as places of socialisation among peers; the importance of such areas for people is undeniable. The fact that their activities are spied on, recorded, processed, and gathered seems to also change the role of such places. The fact that people know they are being monitored may deter them from walking in public places and therefore boost the 'atomization of social life'⁸⁵ that is already underway: individuals ↪ may feel safer at home and prefer socialising online rather than offline. The relationship between individuals and monitoring and surveillance systems in public thus renders the necessity of protecting public places particularly acute. These aspects urge to reframe the issue of technological surveillance of public places and to go beyond the privacy paradigm and the focus on the individual.

6 Conclusion

Despite some scholarly efforts, constitutional theories generally have failed to address the uniqueness of public places and their relationship to privacy. Scholars who are aware of the perils of uninterrupted data mining on individuals suggest that '[w]e need consciously to create privacy zones in order to claw back some areas in which creativity and freedom can take flight unimpeded' — they therefore theorise that some areas should be preserved as secluded from the public.⁸⁶ The very idea of reaffirming the private/public distinction and the dichotomy between individuals and the public⁸⁷ as a viable solution, however, does not seem to grasp the meaning and uniqueness of public places for private and public institutions alike. The overwhelming focus on individuals also overlooks the fact that surveillance technologies have an impact on societies at large, not just on persons taken in isolation. As Virginia Eubanks has it, '[i]n his famous novel 1984, George Orwell got one thing wrong. Big Brother is not watching you, he's watching us'.⁸⁸

Both individuals and social life as a whole need protection from the ever-growing phenomenon of monitoring and surveillance. Courts have certainly identified safeguards by leveraging privacy rights, and legislatures are taking action around the world against massive deployments of such technologies. It is the notion of public places itself, however, that is lacking a proper assessment. This gap leaves people who are even offline in physical public places less protected than people who are online but can avail themselves of more crafted forms of legal protection that revolve around the concepts of personal data and privacy.

Drawing from existing case law in some jurisdictions that have shown sensitivity to the concepts of privacy in public places, I have proposed to tap into the issue of AI-based surveillance of public places the notions of anonymity and confidentiality. These concepts were conceived when information about *specific people and details of their lives were caught and spread by specific individuals and businesses*. But they can be married together to identify information that should not be shared and exploited *because of the circumstance* within which they are caught. In other words, also information gathered from AI-based tools in public places should also be covered by some degree of anonymity and confidentiality. This would not just protect individuals. It would also protect social life, thereby creating a general rule that prohibits public surveillance, except for reasons that are valuable for society at large. After all, some have already argued that privacy is nothing else than 'a facet of social life that gives people the confidence and moral space to share information with others'.⁸⁹ Vindicating this aspect of privacy is easier if privacy is married with anonymity and confidentiality. This would re-balance the equilibrium between the vast population whose information is captured inadvertently and discretely, and the private and public institutions that can exploit such information.

Notes

- 1 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review 193, 195.
- 2 Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2018) 28(1) Information and Communications Technology Law 65–66.
- 3 Julie E Cohen, 'What Privacy Is For' (2013) 126(7) Harvard Law Review 1904, 1912.
- 4 Notable exceptions include: Helen Nissenbaum, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public' (1998) 17(5/6) Law and Philosophy 559; Elizabeth Paton Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50(3) University of Toronto Law Journal 305; Sovanharith Seng and others, 'A First Look into Users' Perceptions of Facial Recognition in the Physical World' (2021) 105 Computers & Security 1; Bart van der Sloot, 'The Right to Be Left Alone by Oneself: Narrative and Identity in a Data-Driven Environment' (2021) 13(1) Law, Innovation and Technology 1.
- 5 Karen Yeung and Lee A Bygrave, 'Demystifying the Modernized European Data Protection Regime: Cross-Disciplinary Insights from Legal and Regulatory Governance Scholarship' (2021) 16(1) Regulation & Governance 1, 8.

- 6 Amy Kapczynski, 'The Law of Informational Capitalism' (2020) 129(5) Yale Law Journal 1460, 1470.
- 7 Adam Greenfield, *Everyware. The Dawning Age of Ubiquitous Computing* (New Riders 2006) 107.
- 8 Licia Califano and Valentina Fiorillo, 'Videosorveglianza' in R Bifulco and others (eds), *Digesto-Discipline Pubblicistiche* (UTET 2015) 504.
- 9 Roger Brownsword and Han Somsen, 'Law, Innovation and Technology: Fast Forward to 2021' (2021) 13(1) Law, Innovation and Technology 1, 3 ('In the Anthropocene, technologies drive the collapse of ... private/public divides.')
- 10 Simpson (n 4) 346.
- 11 *ibid* 307.
- 12 Italian Constitutional Court decision no 135 (21 May 2012).
- 13 Yeung and Bygrave (n 5).
- 14 Shoshana Zuboff, 'The Coup We Are Not Talking About' *The New York Times* (29 January 2021) <www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html>.
- 15 Stamatis Karnouskos, 'Symbiosis with Artificial Intelligence via the Prism of Law, Robots, and Society' (2021) 30(1) Artificial Intelligence and Law 1, 1–2.
- 16 Henry A Kissinger, Eric Schmidt, and Daniel Huttenlocher, *The Age of AI And Our Human Future* (John Murray 2021) 224.
- 17 Guglielmo Tamburrini, *Etica delle Macchine* (Carocci 2020) 127. A major breakthrough in China was the deployment of mass surveillance technology for the 2008 Beijing Olympics, when it put in place more than two million CCTV cameras in the city of Shenzhen. See Center for AI and Digital Policy, 'AISCI-2020: Facial Recognition Report on Facial Recognition' (February 2020) 5 <[file:///C:/Users/utente/Downloads/CAIDP-AISCI-2020-FacialRecognition-\(Feb2021\).pdf](file:///C:/Users/utente/Downloads/CAIDP-AISCI-2020-FacialRecognition-(Feb2021).pdf)>.
- 18 Meredith Van Natta and others, 'The Rise and Regulation of Thermal Facial Recognition Technology during the COVID-19 Pandemic' (2020) 7(1) Journal of Law and the Biosciences 1, 6.
- 19 Jonathan Turley, 'Anonymity, Obscurity, and Technology: Reconsidering Privacy in the Age of Biometrics' (2020) 100(6) Boston University Law Review 2179, 2186.
- 20 Center for AI and Digital Policy (n 17).
- 21 Ryan Mac, Caroline Haskins, and Antonio Pequeno IV, 'Police in At Least 24 Countries Have Used Clearview AI. Find Out which Ones Here' (*BuzzFeed News*, 25 August 2021) <www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table>.
- 22 Cathy O'Neill, *Weapons of Mass Destruction* (Crown Books 2016) 101.
- 23 *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058.
- 24 Kapczynski (n 6) 1468.
- 25 Van der Sloot (n 4) 16. On the risks of capturing emotions through public surveillance AI-techniques, see Carly Kind, 'Containing the Canary in the AI Coalmine: The EU's Efforts to Regulate Biometrics' (*Ada Lovelace Institute*, 30 April 2021) <www.adalovelaceinstitute.org/blog/canary-ai-coalmine-eu-regulate-biometrics/>.
- 26 Luca Montag and others, 'The Rise and Rise of Biometric Mass Surveillance in the EU' (2021) EIJ 91 <https://edri.org/wp-content/uploads/2021/07/The-Rise-and-Rise-of-Biometric-Mass-Surveillance-in-the-EU_Dutch-Summary.pdf>.
- 27 Van Natta (n 18) 1.
- 28 Cohen (n 3) 1905.
- 29 Luciano Floridi, 'Soft Ethics and the Governance of the Digital' (2018) 31(4) Philosophy & Technology 1, 1.
- 30 Kapczynski (n 6) 1471–72.
- 31 Van Natta (n 18) 7.
- 32 Joshua A Fairfield, *Owned* (CUP 2017) 62.
- 33 Ran Hirschl, *City, State: Constitutionalism and the Megacity* (OUP 2020) 52; Ran Hirschl and Ayelet Schachar, 'Spatial Statism' (2019) 18(1) ICON 387, 409.
- 34 Jathan Sadowski and Frank Pasquale, 'The Spectrum of Control: A Social Theory of the Smart City' (*First Monday*, 2015) <<https://firstmonday.org/ojs/index.php/fm/article/view/5903>>.
- 35 Fairfield (n 32) 62.
- 36 *ibid* 67.
- 37 Dan L Burk, 'Algorithmic Legal Metrics' (2021) 96(3) Notre Dame Law Review 1147, 1155.
- 38 Turley (n 19) 2213.
- 39 *ibid* 2082.
- 40 Simpson (n 4) 342.
- 41 Fairfield (n 32) 67.
- 42 Montag (n 26) 22. The Dutch Supreme Court judgment (Hoge Raad App no 02632/02/04, judgment of 20 April 2004) upheld the conviction of a defendant who was caught on camera painting graffiti on the streets, as it found that the deployment of a camera with the purpose of law enforcement did not violate the right to private life as enshrined in art 8 of the European Convention on Human Rights (I am thankful to Evert Stamhuis for pointing out this ruling to me).

- 43 Van der Sloot (n 4) 18.
- 44 Seng (n 4) 5.
- 45 Turley (n 19) 2196.
- 46 Ari Ezra Waldman, *Industry Unbound* (CUP 2021) 12, sarcastically notes that '[p]rivacy ... has a history of being less of a right for everyone and more of a benefit for the wealthy and privileged'.
- 47 Simpson (n 4) 345.
- 48 Eoin Carolan, 'Stars of Citizen CCTV: Video Surveillance and the Right to Privacy in Public Places' (2006) 13(1) Dublin University Law Journal 326, 345.
- 49 Turley (n 19) 2185.
- 50 *ibid* 2194.
- 51 See the chapter by Natalia Menéndez González in this volume.
- 52 Turley (n 19) 2196.
- 53 *Katz v United States* 389 US 347, 351 (1967).
- 54 Turley (n 19) 2202.
- 55 *ibid* 2203. See also Simpson (n 4) 306.
- 56 Simpson (n 4) 321.
- 57 *California v Ciraolo* 476 US 207 (1986) [213].
- 58 *Marper v the United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008), para 66.
- 59 Italian Constitutional Court decision no 149 (16 May 2008).
- 60 *Atherton v Director of Public Prosecutions* [2005] IEHC 429.
- 61 *Hosking v Runting Ltd* [2004] NZCA 101-03.
- 62 *Campbell v MGN Ltd* [2004] UKHL 22, [2004] 2 All ER 995 (Lord Nicholls of Birkenhead).
- 63 *Atherton* (n 60) [19].
- 64 *Florida v Riley* 488 US 445 (1989).
- 65 Nissenbaum (n 4) 569.
- 66 *Hosking* (n 61) 246 (Tipping).
- 67 Nissenbaum (n 4) 559.
- 68 Simpson (n 4) 340.
- 69 *Hosking* (n 61) 125 (Gault).
- 70 Simpson (n 4) 321.
- 71 *Bridges* (n 23) 16.
- 72 *Creation Records Ltd v News Group Newspapers Ltd* [1997] EWHC 370 (Ch) [29] (Lloyd).
- 73 *PG v United Kingdom* App no 44787/98 (ECtHR, 25 September 2001), para 57.
- 74 Simpson (n 4) 325.
- 75 Turley (n 19) 2196.
- 76 *ibid* 2228.
- 77 Nissenbaum (n 4) 576.
- 78 *ibid* 576.
- 79 *Douglas v Hello! Ltd* [2005] EWCA Civ 595 [83]: 'for the adjective "confidential" one can substitute the word "private"' (Lord Phillips).
- 80 *ibid* 55 (Lord Phillips).
- 81 *Hosking* (n 61) 26 (Gault).
- 82 *Douglas* (n 79) 72 (Lord Phillips).
- 83 *Hosking* (n 61) 33 (Gault).
- 84 In the field of personal identity recognition, China's new regulation on data protection also protects personal data, unless there is a public interest involved, and therefore echoes the privacy-oriented Western approach. See Editorial, 'China's New Comprehensive Data Protection Law: Context, Stated Objectives, Key Provisions' (*Future of Privacy Forum*, August 2020) <<https://fpf.org/blog/chinas-new-comprehensive-data-protection-law-context-stated-objectives-key-provisions/>> .
- 85 Angioletta Sperti, 'The Impact of Information and Communication Revolution on Constitutional Courts' in Martin Belov (ed), *The IT Revolution and Its Impact on State, Constitutionalism and Public Law* (Bloomsbury 2021) 184.
- 86 Carissa Véliz, *Privacy Is Power* (Melville House 2021) 195.
- 87 Antoine Garapon and Jean Lassègue, *Justice Digitale* (PUF 2018) 86–87.
- 88 Emphasis in original. Virginia Eubanks, *Automating Inequality* (St Martin 2018) 6.
- 89 Waldman (n 46) 51.