Facial Recognition Technology: Is an Optimal Balance between Security and Privacy Possible?

Helen Cussans

Abstract

This article examines the implementation of facial recognition technology in public spaces within the UK. The article explores concerns over accuracy and discrimination, highlighting the stratified implications of biometric technology. It is argued that the current nature of mass surveillance in public spaces in incompatible with the individual right to privacy. Until significant advances are made in accountability, accuracy, and security, the use of facial recognition technology should be restricted.

Keywords: Facial Recognition Technology, National Security, Privacy, Surveillance, Biometrics.

Introduction

Questions of security and privacy are at the forefront of contemporary debates concerning the surveillance of individuals and society. The policing of public space mobilises a variegated network of security apparatuses and the recent proliferation of biometric surveillance technology has further intensified existing privacy concerns.[1] However, current debates rest on the a priori assumption that privacy must be traded for security. This simplistic dichotomy fails to address the influence of social, cultural, and political context in shaping tacit knowledge of security practices.[2] These will be explored within the broader framework of surveillance theory, with particular focus on concepts of social sorting, surveillance capitalism, and the surveillant assemblage. This networked approach enables nuanced engagement with the highly complex issues of privacy and security.

For the purposes of this article, security is defined as 'freedom from fear',[3] referring more specifically to governments' duty to ensure

[1] James Ash, Rob Kitchin, and Agnieszka Leszczynski, "Digital Turn, Digital Geographies?," *Progress in Human Geography* 42, no. 1 (2016): 25–43.

[2] Vincenzo Pavone and Sara Degli Esposti, "Public Assessment of New Surveillance-Oriented Security Technologies: Beyond the Trade-off Between Privacy and Security," *Public Understanding of Science* 21, no. 5 (2010): 556–572.

[3] Ian Manners, "Normative Power Europe Reconsidered: Beyond the Crossroads," *Journal of European Public Policy* 13, no. 2 (2006): 192.

the safety of their citizens.[4] Privacy will be understood as an individual's right to freedom from unreasonable intrusions as codified under the Human Rights Act of 1998.[5] However, it is acknowledged that the concepts of security and privacy are social constructions that are enacted and performed within a given context. The current debate problematically represents them as objective, fixed categories. Discussions should instead be concerned with how privacy and security are *perceived*, which varies temporally, as well as across social and cultural contexts.[6] Therefore, this article will address privacy and security in relation to the covert implementation of facial recognition technology in public spaces within the UK.

The discussion will proceed in four parts. The first part outlines contemporary surveillance practices and the associated debates. These are then explored in a second part in relation to recent examples of facial recognition technology use in public space. The third part will examine questions of accuracy and discrimination. The final part addresses the security of the collected data and potential misuse. It concludes by demonstrating that until surveillance technologies are accurate, secure, and accountable, a balance between security and privacy is not possible.

Contemporary Surveillance Practices

In our increasingly digitised society, a plethora of surveillance technologies enable the enhanced securitisation of everyday life by rendering a person visible. The use of surveillance in public space is invariably accompanied by a debate over its relative impacts on security and privacy. Those who advocate for its use argue that security must be a priority and thus any invasion of privacy to this end is necessary and justified.[7] In contrast, critics view the use of surveillance technologies as an unnecessary and indefensible abrogation of the fundamental human right to privacy.[8] As a result,

[4] Pavone and Esposti, "Public Assessment of New Surveillance-Oriented Security Technologies."

[5] Jonathan Law, *A Dictionary of Law*, 8th ed. (Oxford: Oxford University Press, 2015).

[6] Joseph N. Pato and Lynette I. Millett, eds., *Biometric Recognition: Challenges and Opportunities* (Washington, DC: National Academies Press, 2010), 36–45.

[7] Bruce Schneier, *Schneier on Security* (Hoboken: John Wiley & Sons, 2009).

[8] Max Snijder, *Biometrics, Surveillance, and Privacy*, ERNCIP Thematic Group Applied Biometrics for the Security of Critical Infrastructure, https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC104392_biometrics_surveillance_and_privacy_final.pdf, accessed 28 November 2019.

the implementation of these technologies is often accompanied by a trade-off rhetoric. It is argued that privacy must necessarily be sacrificed in order to increase security, portraying the situation as inherently zero-sum.[9] This is inaccurate and simplifies what is a highly complex issue. In an attempt to move beyond this conceptual constraint, this article will demonstrate that the two are closely interlinked and often necessarily co-constitutive.

Privacy is a fundamental human right, codified in multiple international laws.[10] These include the right to 'protection from unreasonable searches'[11] and freedom from 'arbitrary interference' as outlined in the United Nation Declaration of Human Rights.[12] However, this ambiguous and subjective terminology has led to disagreements as to what constitutes an "unreasonable" or "arbitrary" invasion of privacy. Until there is a mutually agreed understanding of the concepts of privacy and security with regards to the collection of biometric data, the answer to the question of how to achieve an optimal balance between the two will remain largely unresolvable.

Facial recognition technology is a relatively new phenomena, posing unique challenges to existing conceptualisations of privacy and ongoing debates concerning surveillance.[13] Facial recognition technology is distinct from most biometric technologies as it enables 'a different *kind of tracking* that can occur from far away, in secret, and on large numbers of people'.[14] Thus, it supersedes the necessity of consent.[15] Privacy activists argue that there is a pressing need for legal

[9] Pavone and Esposti, "Public Assessment of New Surveillance-Oriented Security Technologies."; Raphael de Cormis, "Facial Recognition: Time the Regulators Stepped In?," *Biometric Technology Today* 2018, no. 9 (2018): 9–11.

[10] McKay Cunningham, "Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law," *George Washington International Law Review* 44, no. 4 (2012): 643–696.

[11] Chris Werner, *Biometrics: Trading Privacy for Security*, https://media.wiley.com/product_data/excerpt/26/07645250/0764525026.pdf, accessed 26 November 2019, 10.

[12] *Biometrics and Privacy: A Positive Match: How Organizations can use Biometrics Technologies and Protect Individuals' Privacy in the Journey to High Performance* (Accenture, 2012), www.accenture.com/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/dualpub_9/accenture-biometrics-privacy-positive-match.pdf, accessed 28 November 2019, 10.

[13] de Cormis, "Facial Recognition."

[14] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Georgetown Law, Center on Privacy & Technology, 2016), 10.

[15] Pato and Millett, *Biometric Recognition*, 36–45.

frameworks to be updated in response to these capabilities.[16] If not, there is the risk that the rapid development of sophisticated surveillance technology will lead to a social climate in which 'privacy is a thing of the past'.[17] However, this perspective fails to consider the potential to introduce security measures which employ technology in a way that actually *increases* privacy.[18] Understanding this possibility gives further impetus to this essay's contention that privacy and security must not be seen as disparate goals.

Security measures are implemented to render unknown threats visible.[19] This pre-emptive nature of security practices in public space prevents potential futures from becoming actualised, both at an individual and population level, representing a new form of anticipatory security.[20] Thus, when faced with unknown terrorist threats, the notion that biometric surveillance can significantly reduce the probability of an attack is highly appealing.[21] In response to 9/11 and the increased threat from terrorist organisations, security was explicitly prioritised over privacy.[22] The fear of future terror attacks was used in order to justify the widespread introduction of progressively extensive and complex biometric surveillance.[23] This demonstrates that the interaction between privacy and security is not static. Rather, the 'optimal' balance is a constructed ideal that varies significantly dependent upon the context and security threat. Therefore, it would be precipitous to advocate for a universally applicable compromise as the reality represents a highly fluid and atemporal equilibrium.

Biometrics are lauded as the solution to modern security problems and are increasingly relied upon in national security

[16] Garvie, Bedoya, and Frankle, *The Perpetual Line-Up*.

[17] Charles Raab and Benjamin Goold, *Protecting Information Privacy*, Equality and Human Rights Commission Research Report 69 (Manchester, UK: Equality and Human Rights Commission, 2011), 22.

[18] Marieke de Goede, *Speculative Security: The Politics of Pursuing Terrorist Monies* (Minneapolis, MN: University of Minnesota Press, 2012).

[19] Elia Zureik and Karen Hindle, "Governance, Security and Technology: The Case of Biometrics," *Studies in Political Economy* 73, no. 1 (2004): 113–138; Pavone and Esposti, "Public Assessment of New Surveillance-Oriented Security Technologies."

[20] Louise Amoore, "Algorithmic War: Everyday Geographies of the War on Terror," *Antipode* 41, no. 1 (2009), 49–69.

[21] K.W. Bowyer, "Face Recognition Technology: Security versus Privacy," *IEEE Technology and Society Magazine* 23, no. 1 (2004): 9–19.

[22] Lucas Introna and David Wood, "Picturing Algorithmic Surveillance: the Politics of Facial Recognition Systems," *Surveillance & Society* 2, no. 2/3 (2004): 177–198.

[23] Angus Willoughby, "Biometric Surveillance and the Right to Privacy [Commentary]," *IEEE Technology and Society Magazine* 36, no. 3 (2017): 41–45.

programmes.[24] The primary appeal of facial recognition technology is the ability to conduct 'fast, remote identification'[25] particularly in public spaces. However, there is a common misconception that conventional officer surveillance and facial recognition technology differ only in speed, and therefore facial recognition technology does not represent a disproportionate impact on privacy.[26] This is a simplistic understanding of the capabilities of biometric data. The pervasive implementation of surveillance technology represents an accelerated shift towards the increased normalisation of covert data collection, representing the shift towards an 'emergent social paradigm'.[27] The nature of the information gathered by facial recognition technology raises multiple privacy concerns as biometric data is inherently and inextricably linked to the individual. Biometric technology has facilitated a shift towards surveillance of the human body as opposed to the associated infrastructures with which the body interacts.[28] As such, the individual has become intricately implicated in the conduct of modern-day security procedures making it increasingly difficult to distinguish the boundary between the body and surveillance practices. These surveillance technologies have altered the monitoring and governance of public spaces as the body itself becomes the target of surveillance.[29] As a result, ensuring communal security through the use of biometric technology increasingly relies on the invasion of individuals' privacy in order to facilitate broader national security practices. This has further complicated the challenge of maintaining an optimal balance as our current conceptualisations do not reflect the highly intimate nature of contemporary surveillance practices.

Facial Recognition Technology in Public Spaces

In the UK, facial recognition technology has been used by the Metropolitan Police Service in multiple public spaces, including King's Cross, the Cenotaph in 2017, and Notting Hill Carnival in 2016

[24] Patrick H. O'Neil, "Complexity and Counterterrorism: Thinking about Biometrics," *Studies in Conflict & Terrorism* 28, no. 6 (2005): 547–566; Ayse Ceyhan, "Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics," *Surveillance & Society* 5, no. 2 (2008): 102–123.

[25] de Cormis, "Facial Recognition," 11.

[26] Benjamin Hale, "Identity Crisis: Facial Recognition Technology and the Freedom of the Will," *Ethics, Place and Environment* 8, no. 2 (2005): 141–158.

[27] Karen E. C. Levy, "Intimate Surveillance," *Idaho Law Review* 51, no. 3 (2015): 679.

[28] Ceyhan, "Technologization of Security."

[29] Garvie, Bedoya, and Frankle, *The Perpetual Line-Up*.

and 2017.[30] Facial recognition technology was trialled in these spaces as a means of assessing its potential to enhance existing policing strategies. At Notting Hill Carnival, 98 percent of the matches were false positives, which substantiated long-standing concerns over the accuracy and legitimacy of its use.[31] This demonstrates that the use of facial recognition technology constituted an unnecessary and disproportionate invasion of privacy in which the collection of biometric data had a negligible impact on security.

On these occasions, facial recognition technology was used as a form of pre-emptive policing in an attempt to prevent possible futures from actualising, rather than in response to direct security threats.[32] Identifying someone as a potential threat and removing them from public space is a highly contentious action that has multiple broader social implications and can set a dangerous precedent. The observed body is constructed using a collection of fragmented physical characteristics that create an incomplete and 'distinctively hybrid composition'.[33] As a result, individuals come to differently experience themselves through the digital gaze which shapes their engagement with public, social space.[34] This is highly problematic as the invasion of privacy is not restricted to the initial isolated collection of data, but one that has enduring impacts long after the event. Therefore, the widespread use of these inaccurate and intrusive surveillance methods is unacceptable and presents the dangerous possibility of normalising the technology rather than considering it an exceptional security measure to be used only in times of national emergency.[35] However, the combination of technological advances

[30] Sam Trendall, "Police Ethics Body to look at use of Facial-Recognition Technology," *Public Technology.net*, 13 March 2018, www.publictechnology.net/articles/news/police-ethics-body-look-use-facial-recognition-technology; Alex Howlett, "Facial recognition row raises fears about privacy breaches," *Property Week* 86, no. 33 (2019): 37.

[31] de Cormis, "Facial Recognition."

[32] Richard V. Ericson, *Crime in an Insecure World* (Cambridge: Polity Press, 2017); Louise Amoore and Marieke de Goede, "Introduction," *Journal of Cultural Economy* 5, no. 1 (2012): 3–8.

[33] Kevin D. Haggerty and Richard V. Ericson, "The Surveillant Assemblage," *British Journal of Sociology* 51, no. 4 (2000): 611.

[34] Simone Browne, "Digital epidermalization: Race, Identity, and Biometrics," *Critical Sociology* 36, no. 1 (2009): 131–150.

[35] Levy, "Intimate Surveillance"; Garvie, Bedoya, and Frankle, *The Perpetual Line-Up*.

and 'social and political drivers such as fear of crime and terror' have led to the proliferated use of video surveillance.[36]

An important distinction must be made about the nature in which surveillance is conducted. For instance, the collection of biometric data is universally implemented in border security systems. In this context, there is a consensus that facial recognition technology is a necessary and proportionate security measure. In contrast, the use of covert biometric surveillance techniques in public space faces increasing resistance.[37] Whilst this argument is applicable to instances of covert surveillance in public spaces, it does not purport to be universally relevant to every situation in which biometric data is collected.

Accuracy and Discrimination

Surveillance practices are not homogeneously experienced. Multiple concerns have been raised about the disproportionate and unequal impacts of facial recognition technology.[38] Facial recognition technology is most effective at positively identifying white males and has a high error percentage in recognising black and female faces, which is largely attributed to the inherent algorithmic bias in the training data used by facial recognition technologies.[39] This is an unacceptable differentiation whereby security measures ostensibly introduced to improve the security of society have a stratified and socially discriminatory effect. Surveillance along racialised lines is completely unjustifiable and leads to a heightened sense of insecurity and unreasonable lack of privacy for certain groups. Furthermore, once these faces are scanned, they are often stored in a database for an undetermined length of time, whether or not the individual is convicted of a crime. This raises a number of other questions as to the long-term implications of such biases as the data shadow left behind

[36] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social* Life (Stanford, CA: Stanford University Press, 2009), 22.

[37] Werner, *Biometrics: Trading Privacy for Security.*

[38] David Murakami Wood and Kirstie Bell, eds., *A Report on the Surveillance Society*: Public Discussion Document (London: Surveillance Studies Network, September 2006), https://ico.org.uk/media/about-the-ico/documents/1042388/surveillance-society-public-discussion-document-06.pdf.

[39] Browne, "Digital epidermalization"; Simone Browne, *Dark Matters: on the Surveillance of Blackness* (Durham: Duke University Press, 2015); Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research* 81 (2018): 1–15.

is not passive. Personal experiences are fundamental in informing people's perception of technology as an invasion of privacy or a necessary security measure.[40] Therefore, these experiences must be considered when addressing concerns of security and privacy as there is no universally optimal balance, and responses will vary significantly based on the context and individual's experience. This article focuses on the analysis of facial recognition technology in the context of the UK and, as a result, the arguments presented may not be equally applicable in different socio-political contexts with dissimilar national security and privacy narratives.

Discussions are largely restricted to the small-scale individual impacts rather than considering the bigger picture whereby surveillance practices have consequences at both an individual and societal scale.[41] Framing the issue as an individual concern overlooks the ways in which surveillance works as a form of social sorting that targets certain groups of the population.[42] By virtue of the relational nature of the surveillance assemblage, it is not only the privacy of the individual which is infringed upon, but the plethora of associated social infrastructures.[43] Until more nuanced assessments are conducted into the prevention of these pernicious social impacts, a balance cannot be struck between privacy and security.

Security of Collected Data and Potential Misuse

Political theorists have long argued that the aspiration to control the individual body, and society more generally, underpins every political movement.[44] Therefore, the unprecedented scalability of biometric surveillance as a tool to enhance national security efforts raises concerns about the incremental shift towards surveillance

[40] Pavone and Esposti, "Public Assessment of New Surveillance-Oriented Security Technologies."

[41] Pato and Millett, *Biometric Recognition*, 36–45.

[42] David Lyon, "The Snowden Stakes: Challenges for Understanding Surveillance Today," *Surveillance & Society* 13, no. 2 (2015): 139–152; Josef Teboho Ansorge, *Identify and Sort: How Digital Power Changed World Politics* (London, UK: Hurt & Company, 2016).

[43] Gilles Deleuze and Felix Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia* (Minneapolis, MN: University of Minnesota Press, 1987); Haggerty and. Ericson, "The Surveillant Assemblage."

[44] Susanne Bauer and Jan Eric Olsén, "Observing the Others, Watching Over Oneself: themes of medical surveillance in society in post-panoptic society," *Surveillance & Society* 6, no. 2 (2019), 116–127.

societies and Orwellian forms of governance.[45] This is reflected in the argument that these measures will inevitably be subject to 'function creep' whereby data which is purportedly collected to mitigate threats from terrorists and other criminal organisations is instead used for a 'more mundane control of public activities'.[46] There have already been cited instances in which facial recognition technology has been used in efforts to suppress dissent, support law enforcement, and strengthen governmental control over populations.[47] The use of facial recognition glasses by police in China demonstrates the potential for such technology to become a prosaic tool of surveillance.[48] Ensuring that the technology is used for its original purpose is essential as the implications of misuse are profound both in terms of civil liberty, but also with respect to social organisation.[49]

The extensive capabilities of the surveillant assemblage mean that the capturing of facial recognition data is not an isolated incident. The implementation of wide-scale surveillance programmes enables extensive monitoring and tracking, creating a data location trail which could be used to observe and profile the actions of groups within society.[50] This perspective has been advanced by a number of actors who emphasise the spectrum of issues that not only have a direct impact on the individual, but are scaled throughout the assemblage, particularly in cases of mass surveillance.[51] As they are such recent technologies, their long-term implications for privacy and civil liberty,

[45] Bowyer, "Face Recognition Technology."; David Murakami Wood and Kirstie Bell, eds., *A Report on the Surveillance Society*: Public Discussion Document (London: Surveillance Studies Network, September 2006), https://ico.org.uk/media/about-the-ico/documents/1042388/surveillance-society-public-discussion-document-06.pdf; Willoughby, "Biometric Surveillance and the Right to Privacy [Commentary]."

[46] Patrick H. O'Neil, "Complexity and Counterterrorism: Thinking about Biometrics," *Studies in Conflict & Terrorism* 28, no. 6 (2005): 547–566.

[47] Maureen Webb, *Illusions of Security: Global Surveillance and Democracy in the Post-9/11 World* (San Francisco, CA: City Lights Books, 2007).

[48] Josh Chin, "Chinese Police Add Facial-Recognition Glasses to Surveillance Arsenal," *The Wall Street Journal*, 7 February 2018, www.wsj.com/articles/chinese-police-go-robocop-with-facial-recognition-glasses-1518004353, accessed 7 December 2019.

[49] Schneier, *Schneier on Security*.

[50] Vassiliki Andronikou, Dionysios S. Demetis, and Theodora Varvarigou, "Biometric Implementations and the Implications for Security and Privacy," *Journal of the Future of Identity in the Information Society* 1, no. 1 (2005): 13.

[51] Haggerty and Ericson, "The Surveillant Assemblage."; David Lyon, "Surveillance as Social Sorting: Computer Codes and Mobile Bodies," 13–30, in David Lyon, ed., *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (London: Routledge, 2003).

particularly with regards to their gendered and racialised effect, remain undetermined.[52] The politics of this powerful technology are recurrently excluded in considerations of balancing security and privacy, leading to the uninformed and ill-considered use of facial recognition technology.[53]

Surveillance is no longer simply a state-citizen concern. Restricting analysis solely to state implemented facial recognition technology neglects to consider the increasing influence of non-state actors in the implementation and management of surveillance practices. Contemporary security practices aim to integrate surveillance technology into the wider assemblage in order to increase the net capacity of a network.[54] However, the multiplicity of stakeholders involved poses a heightened threat to both privacy *and* security due to conflicting priorities and understandings of privacy. For example, the increasing commodification of biometric data has led to a situation in which 'privacy is traded for products, better services, or special deals'.[55] Furthermore, the commercialisation of highly sensitive data by private companies is not subject to the same safeguards as its use by state organisations. An example of this is the use of facial recognition driven advertising like that used by Adidas and The Venetian resort in Los Angeles, whereby facial recognition technology systems were used in order to identify their customers' age and gender and then tailor adverts to people as they walked past their billboards.[56] There are serious concerns that if this technology is linked to other databases, such as an individual's social media, it will enable the widescale introduction of targeting advertisements based directly on what a person's face reveals about them. In the wrong hands, data collected even for security purposes could be manipulated for financial gain, causing adverse effects on privacy in the long-term.[57]

There are numerous possible uses for facial recognition technology that are as of yet under explored. In the event that criminal actors were to access biometric data, it would present a security threat of its own accord.[58] When considering the balance between security

[52] Garvie, Bedoya, and Frankle, *The Perpetual Line-Up*.

[53] Introna and Wood, "Picturing Algorithmic Surveillance."

[54] aggerty and Ericson, "The Surveillant Assemblage."

[55] Haggerty and Ericson, "The Surveillant Assemblage," 161.

[56] Shan Li and David Sarno, "Advertisers start using facial recognition to tailor pitches," *Los Angeles Times*, 21 August 2011, www.latimes.com/business/la-xpm-2011-aug-21-la-fi-facial-recognition-20110821-story.html, accessed 6 December 2019.

[57] Levy, "Intimate Surveillance."

[58] O'Neil, "Complexity and Counterterrorism."

and privacy, the susceptibility of biometric data to these threats is rarely addressed. Once this sensitive biometric data has been accessed by outside parties, it is irretrievable. Unlike passwords and banking information, biometric data is inseparable from the individual, making it extremely challenging to mediate the impact of breaches. Accounting for potential futures is a necessary consideration, yet insufficient measures have been introduced to safeguard against the range of possible eventualities. Security organisations must consider the ways in which biometric data is stored and protected from such threats.[59] The marked lack of transparency surrounding these technologies is a frequently cited reason behind people's lack of willingness to engage with the practice. Those implementing them offer no assurance as to the ways in which the data is subsequently stored, and who has access to it. Transparency is required on the part of those using the technology in order to ensure that the balance between privacy and security remains as we may expect in a free and democratic society'.[60] The need to ensure societal security must not lead to a disregard of the need for transparency and accountability.

It is essential to address concerns about the use and storage of the data as well as the accountability and transparency of operators.[61] Facial recognition technologies offer the tangible potential to mutually ensure both privacy and security.[62] If these issues are addressed, it may be possible to implement surveillance systems without requiring any trade-off between security and privacy. Encryption of biometric data presents one possible solution to enable the transition from a zero-sum model towards a positive sum model whereby facial recognition technology could offer advantages to both privacy and security.[63] This would allow governments to respond to the range of threats they face without disproportionately impinging on the privacy of citizens. However, it is precipitous to use facial recognition technology before these measures have been put in place.

[59] Cunningham, "Privacy in the Age of the Hacker."

[60] Snijder, *Biometrics, Surveillance, and Privacy*, 13.

[61] de Cormis, "Facial Recognition."

[62] Werner, *Biometrics: Trading Privacy for Security*.

[63] Ann Cavoukian and Alex Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy* (Toronto, Ontario: Commissioner of Ontario, March 2007).

Conclusion

The question of whether an optimal balance between privacy and security can be achieved is inherently problematic as it presupposes that the two are opposing objectives.[64] Furthermore, this understanding rests on the mistaken premise that privacy and security are fixed, static categories. With reference to contextual and temporal variations in the use of surveillance, this article has illustrated that privacy and security are essentially contested concepts.[65] The current understanding of privacy as 'a guarantee to individual bodily integrity'[66] is insufficient in addressing contemporary surveillance practices. If we are entering an 'emergent social paradigm', as Levy suggests,[67] a reconceptualisation of privacy and security may be necessary.[68]

Privacy and security are highly consequential social and political goals that are complicated by the current digital landscape in which biometric data has material value. Therefore, it is essential to promote a multifaceted and nuanced discussion as 'face recognition presents some problems for which there are no easy answers'.[69] Facial recognition technology represents an unprecedented social and political situation in which mass surveillance operations can be conducted without any awareness on the part of those being monitored. This article has highlighted the problematic tendency to analyse surveillance practices in isolation from the social, cultural, and political networks in which they exist.[70] These are critical considerations when responding to the perceived impact of facial recognition technology on security and privacy and there is an urgent need to consider the long-term social and political implications of such technology.[71]

Whilst facial recognition technology demonstrates an appreciable potential to enhance security in public space, a mass surveillance approach has not yet been proven to significantly

[64] Schneier, *Schneier on Security*.

[65] Deirdre K. Mulligan, Colin Koopman, and Nick Doty, "Privacy is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy," *Philosophical Transactions Royal Society* 374 (2016): 1–17.

[66] de Goede, *Speculative Security*, 236.

[67] Levy, "Intimate Surveillance."

[68] David Lyon, "The Snowden Stakes: Challenges for Understanding Surveillance Today," *Surveillance & Society* 13, no. 2 (2015): 139–152.

[69] Garvie, Bedoya, and Frankle, *The Perpetual Line-Up*, 57.

[70] Introna and Wood, "Picturing Algorithmic Surveillance."

[71] Pato and Millett, *Biometric Recognition*, 36–45.

increase security. Rather, it is argued that the use of such technology creates the *illusion* of security.[72] As the systems are continually being developed, their claimed benefits to security have not been extensively evaluated.[73] To fully understand the situation, scrutiny must be employed. Whilst there is no universally applicable response to this dilemma, it is evident that in the current debate some of the most crucial and pressing issues are overshadowed by the prevailing false dichotomy. This article has demonstrated that the current nature of mass surveillance in public space is incompatible with the right to privacy. Until these issues are resolved, the use of facial recognition technology is disproportionate and represents an arbitrary and unreasonable invasion of privacy.

[72] Webb, *Illusions of Security*.

[73] Ceyhan, "Technologization of Security."