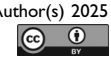
*Article*

# Surveillance evangelism: Private technology companies and the digital futures of crimmigration control

Theoretical Criminology
1–22



DOI: 10.1177/13624806251336758
journals.sagepub.com/home/tcr


**Samuel Singler**
University of Essex, UK

## Abstract

This article contributes to criminological research on surveillance and border technologies. By analysing private security companies' visions of future technologies as surveillance imaginaries, I argue that these companies can be conceptualized as 'surveillance evangelists'. Rather than marketing existing technologies, surveillance evangelists aim to convince state agencies and the wider public about the desirability and plausibility of particular – contingent and contestable – technological futures. Private security companies' visions of digital borders across the African continent contribute to the ideological normalization of crimmigration control, by promoting digital futures in which technologies of criminal justice and border control are fully interoperable. The notion of evangelism is useful for highlighting the speculative, ideological nature of these imaginaries as well as the postcolonial hierarchies that underpin the construction of technical expertise relating to digital crimmigration control.

## Keywords

Borders, imaginary, privatization, surveillance, technology

**Corresponding author:**
Samuel Singler, Department of Sociology and Criminology, University of Essex, Wivenhoe Park, Colchester CO4 3SQ, UK.
Email: samuel.singler@essex.ac.uk

## Introduction

Cutting-edge surveillance technologies have contributed to the rapid contemporary digitalization of policing and surveillance practices. Futuristic surveillance tools based on biometric identification technologies are frequently proposed and tested by public agencies and private companies, ranging from automated live facial recognition to artificial intelligence (AI)-powered lie-detecting border control officers (Sánchez-Monedero and Dencik, 2022). Researchers have argued that such proposals are underpinned by a 'biometric imaginary' or 'ideal' (Dauchy, 2023; Frowd, 2017). This imaginary presents the expansion of intrusive digital surveillance devices as inevitable, feasible and desirable. But where do such visions of the future come from?

This article contributes to the literature on surveillance technologies by turning from past and present to the future. I draw on the sociology of expectations and the political theory of ideology to analyse the promotional materials and presentations of private security companies that develop digital surveillance tools. These companies' visions of upcoming security- and crime-control oriented border technologies demonstrate that the future is 'already here': private security actors promote sociotechnical imaginaries to influence state agencies and make particular – contingent and contestable – futures likelier than others (Halford and Southerton, 2023). In the case of border control tools across the African continent, these imagined technologies contribute to the future expansion of 'crimmigration control' by blurring the boundaries between criminal justice and border control (Dekkers, 2020).

I conceptualize these private security companies as ideologically motivated surveillance evangelists. My use of this term is not (strictly) meant to be provocative; companies and individuals in the digital technology sector have themselves enthusiastically embraced and popularized the term (Kawasaki, 2015). In this context, evangelism refers to the activity of passionately promoting a particular technology over alternative, competing solutions. The aim of technological evangelism is to establish one company's vision of future technological development as hegemonic over alternative conceptions by establishing a new standard across the industry. Shaping technical standards is linked to private companies' attempts to get ahead of the regulatory efforts of states in the context of contemporary regulatory and surveillance capitalism (Schmidt and Scott, 2021; Zuboff, 2022). The speculative and overly optimistic nature of evangelizing is presented as a natural stage in the 'hype cycle' relating to new technologies (Borup et al., 2006).

I use the term 'evangelism' over alternatives such as 'promotion' or 'marketing' for two main reasons. First, surveillance evangelism is broader and more speculative than marketing specific products. As I demonstrate below, private technology companies seek to reshape the political landscape of digital policing and border control not only by developing and marketing new technologies, but also by constructing broad imaginaries that present expanded digital surveillance as inevitable and desirable. Because the real-world deployment of new security technologies is often characterized by failure, friction and contestation, these evangelists' surveillance imaginaries provide ideational resources to smooth over political controversies by reinforcing a general techno-optimism and solutionism.

Second, the notion of evangelism connects contemporary surveillance imaginaries to earlier 'civilizing missions', foregrounding the postcolonial epistemic hierarchies that underpin the global deployment of surveillance technologies. Eva Stambøl (2021: 538) has shown that Northern actors influence Southern states' 'penal power by shaping penal legislation and providing funds, equipment and training to build and change penal institutions'. In addition to material practices of 'neo-colonial penality' (Stambøl, 2021), Global North-based technology companies also shape the ideational landscape of the future of border digitalization in several African countries through public–private partnerships, promotional events and conferences such as the prominent ID4Africa annual meeting. Although this article focuses on private companies operating across the African continent, the notion of evangelism is also relevant for highlighting how surveillance imaginaries produced by these companies reinforce forms of racialized exclusion and postcolonial hierarchy enacted through border controls and law enforcement practices in the Global North.

The notion of surveillance evangelism is particularly pertinent for analysing the practices and technologies of 'crimmigration control'. Originally theorized in the context of immigration and criminal law (Stumpf, 2006), the notion of crimmigration is now used more broadly to refer to the shared legal, operational and technical frameworks that characterize the merger of criminal justice and border control (Dekkers, 2020; Ferraris, 2022). The blurred boundaries between these fields create threats to individual rights and protections enshrined in criminal justice systems and can make it difficult to formulate calls for political accountability (Bosworth and Singler, 2022; Zedner, 2019).

These shared practices are commonly characterized by interoperable digital infrastructures including databases, risk assessment tools and biometric surveillance technologies (Ferraris, 2022). Crimmigration control technologies are often experimental, because border zones are treated by security companies and officials as 'laboratories' for developing new digital tools in 'grey zones of accountability' owing to a lack of regulatory oversight (Molnar, 2021). Border surveillance tools are criminologically relevant because they can reshape domestic policing practices through processes of function creep and the ideational normalization of expansive surveillance (Singler and Milivojevic, 2024). Although domestic policing is also characterized by the deployment of experimental technologies such as automated facial recognition and risk assessment tools, policing technologies tend to attract much more critical public attention along with political and legal challenges (Fussey et al., 2020).

Below, I first develop the concept of 'surveillance evangelism', which suggests that private security companies' promotional materials create and reinforce ideological surveillance imaginaries. These imaginaries perform and legitimize private actors' expertise and authority in shaping the future of biometric surveillance. I then introduce the expansion of biometric border controls in Africa as a criminologically relevant case of contemporary surveillance evangelism. The findings section critically analyses the key themes of what I call the 'gospel of biometric border surveillance'. In the conclusion, I consider the broader analytical utility and normative importance of expanding criminological critiques of past and present surveillance practices to include the examination of future technologies as well.

## Private security companies and surveillance evangelism

### *Private sector influences, the digital surveillance agenda and crimmigration control*

Criminologists have long examined the role of private sector actors in practices of public order and criminal justice (South, 1988). This influence has expanded in recent decades through public–private partnerships, corporate lobbying and the growth of a transnational security–industrial complex (Abrahamsen and Leander, 2016; White, 2012). Private companies have promoted the digitalization of policing and surveillance through the provision of technologies such as risk assessment algorithms, biometric surveillance systems, body cameras and other tools (Hannah-Moffat, 2019).

The digitalization of policing and surveillance has also expanded and blurred the formal boundaries of criminal justice. Surveillance technologies are frequently used to promote 'interoperability' between law enforcement agencies and border control officials. Tools initially created for limited use-cases, such as refugee registration or visa management, can later expand to allow access to law enforcement authorities. In the European Union (EU), systems such as the asylum database EURODAC and the Visa Information System have displayed this law enforcement 'function creep' (Dekkers, 2020). New systems, in turn, are often designed for interoperability between border control and law enforcement agencies from the outset, as with the EU's new Entry/Exit System (Vavoula, 2021). In the African context, function creep of existing systems is less common because several states have only recently begun digitalizing their borders. However, these new tools are usually developed by Northern private companies and Northern-funded international organizations whose technologies are already underpinned by this 'crimmigration control' logic (Singler, 2025).

Critical researchers have described the deployment of biometric borders as motivated by a 'political imaginary', 'ideal' or 'international norm'. In this view, biometric tools represent an '"ideal" that promises greater legibility of mobility as well as symbolic modernity' for African states (Frowd, 2017: 344). Leonie Jegen (2023) has highlighted how Northern-funded capacity-building practices are underpinned by postcolonial logics of 'modernizing' Southern states. The deployment of biometric tools is reflective of a dominant norm of 'biometric statehood', according to which states must demonstrate their capacity to collect digital biometric data at their borders to be politically active in the international community of sovereign states (Muller, 2010).

These imaginaries and norms are not only shaped by state agencies. Researchers have highlighted the extent of private contracting arrangements that underpin the digitalization of borders. In the EU, for instance, private companies such as IDEMIA and Sopra Steria have made hundreds of millions of euros off border technology contracts (Valdivia et al., 2022). Eleftherios Chelioudakis (2022: 94) has explained how public funds are used to support private companies' technological innovation processes, while corporations control the research and innovation agenda: 'states become dependent on the technical expertise of their private partners, without having sufficient knowledge about or effective oversight over the research operations'. State agencies and international organizations such as the United Nations (UN)-affiliated International Organization for Migration

(IOM) have explicitly argued that 'the innovations and potential' of private sector technology companies 'are of fundamental importance to biometrics, identity, migration and border management systems' (IOM, 2018).

## Future expectations and surveillance imaginaries

If indeed private actors are exerting increasing influence over the development of criminal justice and border control technologies, what kinds of values and ideas underpin these practices? Elaine Campbell (2024: 72, original emphasis) has called for criminologists to move beyond 'a retrospective critique of events, processes and practices which have already occurred' by taking 'the future(s) of techno-digital policing [as] *the* temporal point of departure'. In addition to the literature on sociotechnical imaginaries that Campbell builds upon, the sociology of expectations provides useful analytical tools for interrogating the assumptions and values that guide technological innovation in the surveillance sector (Bazzani, 2023; Borup et al., 2006). According to this approach, visions of the future exert performative effects in the present. In other words, 'the future is "already here", with imaginaries and claims about different futures acted on through investments, policies and everyday decisions that make some futures more likely and others less so' (Halford and Southerton, 2023: 273).

Of course, expectations about future surveillance technologies are uncertain, contingent and contestable. Private security companies do not simply predict likely future developments in the surveillance sector; they actively attempt to build support for particular technological futures. Giacomo Bazzani's (2023) distinction between predictions and imaginaries is useful for foregrounding the contingent and political nature of these companies' promotional materials. According to Bazzani (2023: 385–387), predictions are based on 'what actors expect will happen in their future given the present situation and constraints but more or less independently of their influencing capacity'; imaginaries, by contrast, depict 'possible future states of the world that cannot be deduced from the present context and expected dynamics'.

Visions of future surveillance practices can be characterized as imaginaries due to the levels of uncertainty that currently characterize processes of technological innovation. Several authors have referred to the 'surveillance imaginary' or 'biometric imaginary' that guides the development and deployment of digital surveillance tools in criminal justice and border control contexts (Dauchy, 2023; Lyon, 2017). However, these insightful analyses have focused on how imaginaries of present technologies inform current social practices, rather than how they shape expectations. By connecting surveillance imaginaries to the inherent uncertainty of future predictions, the sociology of expectations foregrounds their political nature by asking how these imaginaries are constructed and legitimized, and with what social and political effects.

## Surveillance evangelism and enacting the future today

The political nature of surveillance imaginaries helps situate them within the broader context of ideological beliefs about the desirability, feasibility and inevitability of digitalization in the future. Criminologists have pointed out the ideological assumptions

underpinning the increasing dependence of criminal justice processes on digital technologies. Michael McGuire and Karen Renaud (2023), for instance, have argued that a dominant 'technological rationality' has shaped understandings of digitalization in criminal justice contexts. These technological assumptions are ideological in that they represent a specific – political and contestable – worldview structured by 'patterned and situated combinations of political concepts that temporarily define our understanding of the political and that compete with alternative conceptions over political support' (Freeden, 2006: 14).

Political theorist Gabriele Balbi (2023) has critically analysed the ideology of the 'digital revolution', which constitutes the dominant ideational framework shaping the imaginaries of technological innovators. This ideology is reflected in contemporary tech hype surrounding a range of topics including AI, ideas about space travel and colonizing Mars, and predictions that new tools will eventually solve the problem of climate change (Markelius et al., 2024; Tutton, 2021). Prominent individuals, companies and media outlets play an important role in constructing and legitimizing the ideology of the digital revolution by engaging in 'social struggles in which particular visions become dominant' (Beckert and Suckert, 2021: 11). These individuals and companies now describe themselves as digital 'evangelists' or 'gurus' (Balbi, 2023). Tech venture capitalist and founder of the pioneering internet browser Netscape, Marc Andreessen, has even published a 'techno-optimist manifesto' composed of a series of 'beliefs' akin to a theological creed (Andreessen, 2023).

Such self-descriptions can be critically reoriented by conceptualizing private security companies that construct and promote future technological imaginaries as 'surveillance evangelists'. Doing so helps deconstruct the ideological assumptions and values underpinning these future visions, resisting attempts to foreclose alternative futures by highlighting their contingency. In this way, critically examining the imaginaries of surveillance evangelists contributes to the broader criminological project of bringing 'taken-for-granted aspects of security – notably the "industrial market" for security technology – more fully under the scholarly and public gaze' (Goold et al., 2013: 992).

The notion of evangelism complements narrower concepts of 'promoting' and 'marketing' specific security products, which criminologists have used to critically analyse the commodification and privatization of security (White, 2012). This framework highlights the ideological, speculative and future-oriented dimensions of the innovative and promotional activities of private technology companies. A crucial question, from this perspective, is how these companies deal with the potential dissonance between utopian visions of future biometrics on the one hand, and the reality of technical failures, messy practices and political challenges to these technologies on the other. In contrast to the flashy and futuristic content of surveillance imaginaries, border control and surveillance technologies often operate in a mundane register, and their use is characterized by failure, friction and contestation (Glouftsios, 2021). Private technology companies' surveillance evangelism plays an important role in smoothing over potential technical failures and controversies relating to particular technologies, while garnering public support for broader surveillance futures. Evangelism is akin to practices of 'corporate storytelling' through which private companies have sought to normalize future visions of 'smart' surveillance in public spaces (Söderström et al., 2014). These broader efforts also explain why

companies promote similar surveillance imaginaries even while competing over markets for specific products. In this way, surveillance evangelism provides an additional, future-oriented normative dimension for explaining institutional isomorphism in the private surveillance sector (Caplan and boyd, 2018).

In the context of the global diffusion of biometric crimmigration control technologies, the theological undertones of evangelism also highlight affinities between contemporary surveillance imaginaries and earlier colonial 'civilizing missions'. Critical researchers have highlighted the 'coloniality of biometric power' by demonstrating how digital biometric tools produce 'continuities of race, racialization, and coloniality' in mobility governance (Nishiyama, 2022). The provision of training and equipment by Northern actors seeking to reshape Southern criminal justice and bordering practices has been critically conceptualized as a form of 'neo-colonial penality' (Stambøl, 2021). Beyond capacity-building practices and the provision of specific tools, epistemic postcolonial hierarchies also underpin the ideational and discursive struggles through which the digital futures of crimmigration control are being shaped. The field of surveillance evangelism relating to biometric border controls is marked by the dominance of Global North-based actors, who seek to create global technical standards and convince Southern states of the desirability and inevitability of biometric border surveillance. New digital technologies in this field are not only related to ideas of modernization, but also entrench racialized hierarchies of global mobility that are enacted through the postcolonial order of sovereign states (Sharma, 2020). Surveillance imaginaries relating to the future of biometric borders in Africa obscure and reify these global hierarchical mobility structures by normalizing exclusionary principles of citizenship and identity.

## Methods: narrating the futures of digital surveillance

Surveillance imaginaries are communicated to audiences through narratives that bridge the gap between imagined futures and present courses of action. The construction of these narratives is guided by value-based assumptions and particular interpretations of the social world. They aim to legitimize contemporary practices and sustain the emotional commitment needed to cope with the uncertainty and inevitable failures that characterize the process of technological innovation (Bazzani, 2023). Sociologists have utilized thematic analysis of media publications and technical documents to analyse the construction of future-oriented narratives. Such discursive analysis focuses on 'understanding the stories, conversations, metaphors, public and expert controversies in which future states of the world are expressed' through an analysis of 'verbatim transcripts, audio recordings, reports, and other archival material' including public pronouncements, promotional materials and technical documents (Beckert and Suckert, 2021: 12).

The analysis below is based on publicly available documentation created by private technology companies that are particularly influential in the field of border security, and which regularly attend the ID4Africa annual meeting. Existing research has highlighted the growing influence of companies such as IDEMIA, Sopra Steria, Thales and others in both the Global North and South (Trikanad and Bhandari, 2022; Valdivia et al., 2022). These companies are regular and prominent presenters at the ID4Africa annual meeting, which has been characterized as the most important forum bringing

together policymakers and private companies across the continent to discuss the future of digital identity and biometric technologies (Trikanad and Bhandari, 2022). According to the World Bank (2017: vi) ID4Africa has been 'a positive source of knowledge sharing and has helped engender a community of practice across the continent'.

The continental reach of the ID4Africa movement underpins the methodological choice to analyse surveillance evangelists' imaginaries relating to the African continent as a whole. Although I wish to avoid the uncritical presentation of Africa as a cultural monolith (Faloyin, 2023), the surveillance imaginaries presented at ID4Africa describe the continent in homogenous terms and avoid mentioning specific country contexts. While these private security companies also provide services to address specific social problems in several African states, their presentations at ID4Africa operated in the speculative, future-oriented register of surveillance imaginaries that were 'less explicit, less issue-based, less goal-directed, less instrumental and less politically accountable' than specific policies or products (Campbell, 2024: 72).

I analysed more than 100 documents including both text and images, consisting of transcripts of presentations to public authorities, promotional brochures, technical documentation, PowerPoint slides presented at border industry conferences, public statements and press releases. The documents were collected from publicly available archives of ID4Africa as well as the companies' own webpages. The analysis focuses on materials from 2014 onward – the year ID4Africa was founded – as the past decade has witnessed a remarkable intensification in the promotion of biometric identity and surveillance technologies across Africa. I thematically coded these documents in NVivo according to themes that emerged as salient during the analysis (Castleberry and Nolen, 2018). I used these themes to structure the findings section.

Notably, the most influential companies identified in existing research are based in the Global North while offering services in Southern states. Thales, for instance, is partly owned by the French government and has provided biometric systems to former French colonies such as Algeria, Cameroon and Gabon (Thales, 2025). As a white, male scholar from the Global North, I seek to contribute to a decolonial criminological agenda by highlighting the postcolonial dimensions of surveillance evangelists' imaginaries, while acknowledging that the construction of alternative, more equitable digital futures should be the result of a participatory process that is directly inclusive of Southern voices (Aliverti et al., 2021; Carrington et al., 2019).

## Biometric borders and crimmigration control in Africa

### *The African continent as a key site of digital biometrics innovation*

Digital biometrics are already widespread at border-crossing points across the Global North, and such tools have begun to proliferate across the Global South as well. Several Southern states have rolled out biometric border management and policing tools that have been developed by Northern states, Northern-funded international organizations or Northern-based private technology companies. For instance, 20 states, mostly in Africa, have adopted the Migration Information and Data Analysis System (MIDAS) developed by the IOM (Singler, 2021). Across West Africa, funded by the European

Union Emergency Trust Fund for Africa, states have expanded their use of Interpol's West Africa Police Information System (Dauchy, 2023).

These developments are taking place against the background of a global 'datafication' of border control and identity management (Valdivia et al., 2022). Spurred by UN Sustainable Development Goal 16.9, aiming to provide all the world's population with a 'legal identity' by 2030, states and private companies have interpreted this goal in terms of providing a digital, biometrically verified identity. National large-scale biometric databases such as India's Aadhaar have normalized the notion of digital identity as a condition for accessing rights and entitlements (Trikanad and Bhandari, 2022). In the words of Joseph Atick, executive chairman of the ID4Africa movement, 'in a world that's becoming digital, you cannot exist by becoming invisible' (Speed, 2020).

Digital ID initiatives have proliferated across Africa in recent years. Although most African states already issue e-passports that accord with the International Civil Aviation Organization's standards on Machine Readable Travel Documents, the inclusion of a digital biometric chip is a much more recent – and ongoing – development. Current initiatives also include the use of digital ID beyond border control contexts and the establishment of interoperable databases between states. For instance, in 2016 the Economic Community of West African States (ECOWAS) launched the ECOWAS Biometric ID card initiative that requires member states to issue a biometric ID to facilitate cross-border travel across the region. However, as of 2023, only six of the fifteen member states have successfully rolled out the ID cards (Mascellino, 2023). In 2023, Gabon, Ghana, Guinea, Rwanda, Tunisia and Zimbabwe signed a declaration on data sharing and interoperable digital ID, meant to facilitate travel and economic integration across these states (MacDonald, 2023a).

## *Who are the surveillance evangelists and where do they preach?*

Alongside the proliferation of biometric borders and digital ID initiatives in Africa, a host of media channels, industry expos and public–private networks have sprung up to facilitate information exchange and discussions regarding future biometric innovations between public and private actors in Africa. *Biometric Update* has undoubtedly become the primary transnational media outlet for surveillance evangelism. This online publication provides news about recent and future innovations in the biometrics sector to over 3 million readers annually, aiming to create new linkages between public and private actors such as 'governments, law enforcement agencies, financial institutions and many other vertical industries along with OEMs, service providers, system integrators, enterprise and industry professionals' (Biometric Update, 2024).

Industry-led meetings and workshops attract large audiences consisting of state officials and private technology companies. The ID4Africa movement has become the most prominent organization bringing together public and private biometric technology stakeholders (Soskis, 2022). Its annual meeting is attended by African state officials, UN agencies and non-governmental organizations, and hundreds of private biometrics companies each year (ID4Africa, 2024). Trikanad and Bhandari (2022) have highlighted the role of security companies' ID4Africa presentations in creating 'narratives' that help 'influence policy decisions' in several African states.

Surveillance evangelists' presentations at the ID4Africa meetings constitute important political moments in which broad, speculative surveillance imaginaries can shape policymakers' preferences regarding desirable digital futures while marginalizing potential criticisms and concerns. As argued by Trikanad and Bhandari (2022: 16), 'these presentations evidence an uncritical endorsement of the use of big data for real-time governance, without any mention of surveillance concerns or the need for data protection laws and protocols'. These techno-optimistic imaginaries can later shape policy preferences. For instance, the Nigerian government explicitly drew on ID4Africa's 'Principles on Identification for Sustainable Development' when developing the country's new national biometric identification system. According to a report by the Center for Global Development, this case constitutes 'a leading example of ID4D's impact in the field through the dissemination of the principles; the principles were frequently discussed at ID4Africa general meetings' (Soskis, 2022: 16).

The most active presenters at these industry events are also key players in the European border control market, including 'Accenture, Thales Digital Identity, IDEMIA, SITA, Secunet Security, Indra Sistemas, Gunnebo Networks, Vision-Box, NEC Corporation, and HID Global' (Jarrahi, 2021). Many of these firms have recently been awarded large contracts to develop new biometric borders for various African states. For instance, IDEMIA Group, based in France with an annual turnover of €2.9 billion, is one of the most prominent winners of EU border control contracts and in 2023 won a contract to develop a new 'seamless' biometric border management system in South Africa (IDEMIA, 2023). German technology companies Veridos and Secunet Security are part of the Giesecke + Devrient conglomerate with an annual revenue of €2.4 billion. In 2023, Veridos won contracts to develop border management and digital ID systems in Botswana, Namibia and Uganda (McConvey, 2023). The French conglomerate Thales Group, with an annual order intake of €23.1 billion in 2023, acquired the Dutch biometric surveillance company Gemalto in 2019 for €4.8 billion. Since then, the company has won contracts to produce digital ID solutions and border surveillance technologies in several African countries such as Cameroon, the Democratic Republic of the Congo, Gabon, Niger, Senegal and Uganda. Many of these contracts have later been investigated under suspicion of bribery and corruption (MacDonald, 2023b).

## The gospel of biometric border surveillance

In this section, I analyse private technology companies' promotional materials, which are used to construct future surveillance imaginaries. The speculative character of these documents was acknowledged by the companies themselves. For instance, IDEMIA explained that its promotional documents outline a 'belief' in its 'vision for the future' (IDEMIA, 2019b); United States-based transnational technology consulting company, Accenture, referred to its 'vision of digital identity' as 'the key to unlocking a fairer future' (Accenture, 2019); and French digital services and software giant, Sopra Steria, outlined a broad and speculative 'future immigration vision' (Sopra Steria, n.d.). What were the key elements of these surveillance imaginaries?

## A 'biometric revolution' and the inevitability of expansive surveillance

The first notable feature of these biometric surveillance imaginaries was that their discourse regularly referred to the 'digital revolution' (Balbi, 2023). In a promotional document relating to digital ID documents, Accenture argued that 'digital identity is possibly one of the most pervasive technology trends to take place in our lifetime', before directly linking this trend to the 'Fourth Industrial Revolution' (Accenture, 2019). Sopra Steria, in turn, suggested that contemporary biometric border controls represent a 'holistic transformation' of migration control practices, and claimed that 'the immigration system of the future must be very different to today' (Sopra Steria, n.d.: 3). The link between these companies' surveillance imaginaries and the broader ideology of the digital revolution was also reflected in the changing themes of annual industry events. Presentations at ID4Africa have mirrored successive waves of broader technological trends, from mobile biometrics and the 'Internet of Things' in 2015, to blockchain in 2018, to AI in 2023 and 2024.

Technology companies claimed that the 'biometrics revolution' originated in the disruptive innovation practices of the private sector. According to Sopra Steria (n.d.: 5), 'governments wait for industry standards to guide policy', indicating the need for the private sector to develop new border control solutions that should subsequently become the basis for technical standards set out by public authorities. Similarly, IDEMIA (2021: 4) located the primary source of technical innovation in 'the travel industry [which] has been continuously innovating to maintain safe and smooth travel in the face of complex challenges'. Contemporary practices are only the beginning of this new biometrics revolution, and according to IDEMIA (2021: 3) 'the story is far from complete. A newer generation of secure and efficient solutions are just beginning'.

These arguments reflect the evangelizing endeavour of promoting speculative and broad surveillance imaginaries today to influence technical standards and shape state regulations in the future (Schmidt and Scott, 2021). Sopra Steria (n.d.: 5) explicitly referred to the temporal lag between technical innovations and public regulations and standards: 'Policy standards/regulatory issues are unclear or have not yet caught up with the technology ask'. Switzerland-based SITA argued that we are living through 'an ID management revolution' in which private sector actors should play a key role in setting 'standards and recommended practices that govern how biometric technology will be integrated into existing airline and airport business processes, infrastructure and business systems' (Farrell, 2019).

These surveillance imaginaries relied heavily on contestable predictions regarding the future development of border control technologies. Technical forecasts were often stated as certainties, although companies rarely provided any evidence to support them. At the 2019 ID4Africa Annual Meeting, the American security technology company HID Global claimed that the 'role of biometrics' will increase in linear fashion without any supporting evidence to explain why or how this might happen (HID, 2019). Accenture (2019) argued that new biometric technologies 'will provide the foundation by which our digital selves will interact with online systems, control our connected devices, leverage the learnings of applied intelligence, and protect the earth's resources'. The potential incompatibility of, for instance, increased air travel and 'protecting the earth's resources' was not mentioned.

A curious tension was evident between these predictions' certainty and the claim that these future visions will only come about through the innovation and lobbying efforts of private companies. German security company Secunet (2019) noted that the biometric future is nearly here, and indeed 'border control authorities simply need to embrace this technology and make use of it', yet obstacles to implementation remain: 'many still seem to fear interconnected [border control systems] as extremely complex and unfathomable'. The French firm IN Groupe (2022) similarly recognized that an important determinant of the future expansion of biometrics at African borders was 'political will'. According to IDEMIA's (2019b) 'vision for the future', the remaining political obstacles, social concerns and technical problems will be overcome soon, so that 'in 2030, IDEMIA envisions a world where everyone has an identity' and 'where digital is almost everywhere and coexists intrinsically with the physical'.

Despite recognizing these logistical and political obstacles, technology companies nonetheless presented their surveillance imaginaries as the unequivocal 'future of identity' (IDEMIA, 2019b). The implicit acknowledgement of the contingency of these companies' future visions highlights the political role of surveillance evangelism in shaping technological expectations and normalizing particular visions of the future while marginalizing alternatives. As Elaine Campbell (2024: 74–75) has argued in her analysis of the National Policing Digital Strategy of England and Wales, the strategy simultaneously 'expresses a sociotechnical imaginary in which techno-digital innovations will "come to the rescue"', while working to 'dismiss and discredit particular viewpoints which militate against, challenge or do not conform to the preferred sociotechnical imaginary'.

## *Universality, modernization and postcolonial hierarchy*

IDEMIA's reference to a 'world in which everyone has an identity' points to another central theme underpinning surveillance imaginaries regarding the future of African borders: the conception of digital identity as a modern, universal basis for accessing individual rights. Several companies explicitly referred to UN Sustainable Development Goal (SDG) 16.9 relating to digital identity in their promotional materials, along with optimistic visuals of people smiling and laughing in joy at their newfound ability to possess a digital identity (Veridos, 2021). Although this SDG does not necessarily relate to border control practices, these technology companies promoted biometric border control technologies as a useful starting point for expanding biometric identification practices in other contexts. According to Dutch biometrics company Gemalto (2018), now Thales DIS, 'for citizens, passports protect their identities and are the best proof of ID they have'.

The African continent was regularly singled out as the region of the world that, in the words of Secunet (2019), still has to 'do some homework' when it comes to digital identity infrastructures. Companies regularly referred to African 'underdevelopment', which could be rectified through 'modernization' by implementing digital biometric controls at the border. Thales (n.d.), for instance, referred to Namibia's use of its biometric border control tools in terms of 'modernization' that will 'ensure a modern and efficient welcome is always extended to visitors'. According to Veridos (2021), 'an international identity crisis […] is large and it is global. But nowhere is it as starkly evident as it is on

the continent of Africa'. Although companies like IDEMIA (2022) argued that Africa is characterized by a 'mindset of free movement', technological underdevelopment was represented as holding the continent back from increased cross-border mobility.

The postcolonial nature of these imaginaries was evident in the characterization of the African continent in homogenous terms and as trailing the 'modern' Global North. In this way, surveillance evangelism reinforced epistemic hierarchies that reflect the coloniality of knowledge production and expertise relating to border control and criminal justice technologies (Jegen, 2023; Singler and Babalola, 2024). Empirical research has demonstrated how Northern actors have sought to reshape crimmigration control practices in several Global South countries through 'capacity-building' practices (Singler, 2024). Complementarily to these material interventions, surveillance evangelism at forums such as ID4Africa allowed private security companies to shape dominant ideas and expectations relating to crimmigration control technologies according Northern-produced norms and technical standards.

## *Citizenship and 'real people'*

Connecting biometric surveillance to digital identity and access to rights brings into view the implicit politics of citizenship that is being played out in imaginaries of biometric surveillance. British biometrics company iProov (2022) noted that although border control checks are often still arduous and slow, biometrics offer the promise of 'streamlining' border controls, and 'the good news for many citizens worldwide is that this is becoming a reality'. Nearly all these surveillance evangelists made regular reference to the benefits of biometric border control for citizens, while highlighting 'illegal immigration' as one of the key problems these systems are meant to rectify.

These companies' public discourse was clearly aimed at a globally mobile elite for whom biometric surveillance primarily represents increased cross-border mobility. Although the digital identity agenda was presented as a platform for empowering individuals to access their right to be recognized as a person and become more globally mobile, such social inclusion was restricted to citizens. As Veridos (2021) explained, 'we have long recognized the proven value of identity systems in securing social inclusion for all citizens'. Whereas citizenship has historically been recognized as the basis of the 'right to have rights', in Hannah Arendt's (1958) formulation, digital biometrics were presented not only as the basis of citizenship rights, but also a prerequisite for having an identity at all. In this vein, iProov (2024) suggested that biometric identification tools not only confirm that an individual is the 'right person', but also that they are a 'real person'. Gemalto's (2019) promotional materials explained that 'your biometric data are your identity'.

Katja Franko Aas (2011: 153) has noted how biometric border control technologies are underpinned by the assumption that the body 'tells the truth, and it is an encoded truth which, like numbers, computer passwords and PIN codes, is objective and unambiguous'. This terminology of truthfulness and suspicion characterized the implicit politics of citizenship evident in the imaginaries of surveillance evangelists. iProov (2022) noted that biometric identification documents act 'as a source of truth to match the person against'. The truths told by the body are, according to Thales (2023), 'permanent,

as they don't change over time' in addition to being 'recordable (with or without consent)'.

## *Solutionism and 'suitability'*

Claims about the permanence of biometric identifiers were often used to explain why biometrics constitute a 'solution' to the 'problems' posed by border control. Slovakian technology company Innovatrics (2023; see Figure 1), for instance, claimed that biometrics are 'universal' insofar as digital biometric recognition technology 'works all the time for everyone, and it never fails'. Critical researchers have noted that biometric technologies have widely varying error rates for different groups of people, depending on gender and ethnicity (Buolamwini and Gebru, 2018). Moreover, activities like manual labour can erode fingerprint ridges, precluding registration using the most common fingerprint scanners (Olwig et al., 2020). Surveillance evangelists were aware of these issues but presented them as technical problems to which technical fixes were imminent. The presentation by Innovatrics (2023), in fact, explicitly outlined some of the key challenges to making biometrics truly 'universal', before going on to claim that each of these obstacles will be overcome by new technologies in the near future. Such arguments demonstrate how surveillance imaginaries were used to smooth over current technical controversies by 'isolating them as special or peculiar cases with little technically or organizationally in common with the newly proposed promissory solution' (Borup et al., 2006: 290).

Reflecting their awareness of the contested accuracy and reliability of biometrics, several companies refrained from providing identification rate accuracy statistics or comparisons between various forms of identity verification. Instead of presenting biometric technologies as the most accurate form of identification and verification, Thales (2023,


**Figure 1.** Innovatrics presentation at the ID4Africa 2023 annual meeting.

emphasis added) presented these tools as 'the most *suitable* means of identifying and authenticating individuals'. Veridos (2024), in turn, referred to digital biometric identification tools as the 'proper and measured' response to the problem of traveller authentication.

This focus on 'suitability' reinforced the ideological positioning of biometrics as a universal solution to a range of social problems relating to border control. In response to these complex issues, biometrics were, in the words of Aware (2021), 'border control made easy'. iProov (2022) explained that 'if it isn't easy to use, people won't use it', and according to HID Global (2024), biometric identification would ideally operate in the background of everyday social life, remaining as hidden as possible from sight or mind: 'proving who we are as we go about our busy days should be done in the blink of an eye […] and handled in a convenient, frictionless manner'. Despite the complexity of social problems related to border control, biometric surveillance seemed to offer simple solutions, so long as the preferred solutions were those provided by surveillance evangelists themselves.

## *Interoperability and the expansion of crimmigration control*

To critical researchers focusing on border control, it will come as no surprise that the imaginaries constructed by private technology companies were highly securitized. Some of the contestable assumptions that were glossed over by claims of simplicity were that migration control is primarily an issue of crime control and law enforcement, and that interoperability between immigration control and criminal justice practices is both necessary and desirable. According to Thales (n.d.), biometric technologies provided 'robust protection against twenty-first-century threats such as terrorism, illegal immigration, and people trafficking'. Countering terrorism and enhancing crime control were key themes in several companies' ID4Africa presentations, such as SITA's presentation which explicitly highlighted 'terrorism', 'trafficking' and 'international crime' as primary 'drivers' of the border industry (SITA, 2023).

In surveillance evangelists' imaginaries, not only do biometric surveillance tools offer increased security by allowing states to identify suspicious individuals at the border, but these tools should be interoperable between law enforcement agencies and immigration control authorities to achieve these security goals. According to Sopra Steria (n.d.), the goals of 'criminal justice' and 'efficient immigration and cross-border travel' could both be effectively pursued by interoperable biometric surveillance systems. IDEMIA (2021) highlighted 'global interoperability' as a key goal of future technological innovation. What critical scholars have termed 'function creep' of migration control systems was promoted as central to the digital futures of crimmigration control (Dekkers, 2020). IDEMIA, for instance, argued that their Border Control Suite could initially be used strictly for migration control purposes, but eventually interoperability with law enforcement databases would be needed to 'anticipate threats and assess risks' (IDEMIA, 2019a).

An uneasy tension persisted between these surveillance evangelists' expertise as developers of security devices and their supposedly progressive and equitable technological utopianism. Alongside frequent mention of security issues such as terrorism

and transnational crime, their surveillance imaginaries were infused with a focus on facilitation and future visions of 'seamless travel' (SITA, 2023; Thales, n.d.). In these visions of the future, exclusionary and intrusive border surveillance technologies were a necessary corollary to freedom and privacy within borders on a global level. These surveillance imaginaries smoothed over the potentially violent and exclusionary implications of conceptualizing migration as a security threat or crime control issue, while continuing to position intrusive biometric technologies as a necessary building block of desirable digital futures.

## Conclusion

Criminological research has made invaluable contributions to challenging expansive and intrusive surveillance practices. Existing and experimental technologies have been critiqued by highlighting their adverse implications in terms of privacy rights, their discriminatory effects, and their inaccuracy and unreliability (Fussey et al., 2020). In this article, I have suggested that visions of digital futures also play a crucial role in determining which tools eventually become taken for granted and 'banal' (Goold et al., 2013). Private technology companies act as surveillance evangelists that construct imaginaries and attempt to convert state authorities and the wider public into believers of these contingent and contestable future visions. In doing so, they shape what kinds of future surveillance practices appear acceptable and desirable.

Conceptualizing private security companies as surveillance evangelists – rather than just surveillance 'experts' or actors involved narrowly in 'marketing' new products – can expand criminological critiques beyond claims about the inaccuracy or unreliability of surveillance technologies today. Because surveillance imaginaries are highly speculative, they cannot be challenged only by pointing to the inaccuracy of current tools. Surveillance evangelists actively construct imaginaries to smooth over current technical and social issues by suggesting that their resolution is only a matter of time. Problems are brushed aside in techno-solutionist fashion, blunting the force of well-founded evidence-based criticisms. As Marc Andreessen (2023) put it in his techno-optimist manifesto: 'Give us a real world problem, and we can invent technology that will solve it'.

The intersection of border control and criminal justice provides a particularly fruitful context for speculative surveillance imaginaries, thanks to the conceptualization of border zones as 'laboratories' for testing highly experimental digital technologies (Molnar, 2021). These tools can later reshape domestic policing and surveillance practices through processes of technological function creep and the normalization of biometric surveillance. Beyond the context of crimmigration control, surveillance evangelists are also actively involved in shaping the digital futures of domestic policing; critically analysing surveillance imaginaries in other criminal justice contexts provides important avenues for future research. In the rapidly evolving and experimental field of security technologies, surveillance evangelists themselves have noted the importance of winning what Palantir CEO Alex Karp has called the 'intellectual debate' regarding the future, long before new tools are developed (Haskins, 2024). Uncovering and contesting the ideological and political assumptions underpinning contemporary surveillance imaginaries is crucial if we wish to effectively shape these debates.

## Acknowledgements

This paper benefitted from constructive feedback from participants at the CRIMKNOW workshop held at the University of Oslo in February 2024, and the STS-MigTec Circle work-in-progress seminar in May 2024. I owe special thanks to Eamonn Carrabine, Pete Fussey and Nigel South for comments and criticism on an earlier draft. The anonymous reviewers' in-depth engagement with this article greatly improved the clarity of the arguments. I also thank Innovatrics for permission to reproduce an image from their promotional materials.

## Declaration of conflicting interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## Funding

The author received no financial support for the research, authorship, and/or publication of this article.

## ORCID iD

Samuel Singler https://orcid.org/0000-0001-6231-7095

## References

Abrahamsen R and Leander A (eds) (2016) *Routledge Handbook of Private Security Studies*. London: Routledge.

Accenture (2019) Human-centric digital identity: The key to unlocking a fairer future. Available at: https://www.id4africa.com/2019/almanac/Accenture-Security-Christine-Leong.pdf (accessed 12 June 2024).

Aliverti A, Carvalho H, Chamberlen A, et al. (2021) Decolonizing the criminal question. *Punishment & Society* 23(3): 297–316.

Andreessen M (2023) The techno-optimist manifesto. Available at: https://a16z.com/the-techno-optimist-manifesto/ (accessed 26 May 2024).

Arendt H (1958) *The Origins of Totalitarianism*. New York, NY: Meridian Books.

Aware (2021) Border control made easy with biometric technology. Available at: https://www.aware.com/blog-biometric-border-control/ (accessed 12 June 2024).

Balbi G (2023) *The Digital Revolution: A Short History of an Ideology*. Oxford: Oxford University Press.

Bazzani G (2023) Futures in action: expectations, imaginaries and narratives of the future. *Sociology* 57(2): 382–397.

Beckert J and Suckert L (2021) The future as a social fact: the analysis of perceptions of the future in sociology. *Poetics* 84: 101499.

Biometric Update (2024) About us. Available at: https://www.biometricupdate.com/about-us (accessed 27 May 2024).

Borup M, Brown N, Konrad K, et al. (2006) The sociology of expectations in science and technology. *Technology Analysis & Strategic Management* 18(3–4): 285–298.

Bosworth M and Singler S (2022) A mundane spectacle? (in)visibility, normalisation and state power in the UK's migrant escorting contract. In: Bosworth M and Zedner L (eds) *Privatising Border Control: Law at the Limits of the Sovereign State*. Oxford: Oxford University Press, pp. 179–189.

Buolamwini J and Gebru T (2018) Gender shades: intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research* 81: 1–15.
Campbell E (2024) Techno-digital policing and speculative fictions: towards a criminology of the future. *Crime Media Culture* 21(1): 69–95.
Caplan R and boyd d (2018) Isomorphism through algorithms: Institutional dependencies in the case of Facebook. *Big Data & Society* 5(1), DOI: 10.1177/2053951718757253.
Carrington K, Dixon B, Fonseca D, et al. (2019) Criminologies of the global south: critical reflections. *Critical Criminology* 27: 163–189.
Castleberry A and Nolen A (2018) Thematic analysis of qualitative research data: is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning* 10(6): 807–815.
Chelioudakis E (2022) Privatization of security, border management, and defense in the EU: does reliance on tech companies erode states' sovereignty? In: Hudson G and Atak I (eds) *Migration, Security, and Resistance*. London: Routledge, pp. 83–103.
Dauchy A (2023) Dreaming biometrics in Niger: the security techniques of migration control in West Africa. *Security Dialogue* 54(3): 213–230.
Dekkers T (2020) Technology driven crimmigration? Function creep and mission creep in Dutch migration control. *Journal of Ethnic and Migration Studies* 46(9): 1849–1864.
Faloyin D (2023) *Africa is not a Country: Breaking Stereotypes of Modern Africa*. London: Penguin.
Farrell S (2019) Taking steps now to realize the seamless passenger journey. Available at: https://www.sita.aero/pressroom/blog/taking-steps-now-to-realize-the-seamless-passenger-journey/ (accessed 12 June 2024).
Ferraris V (2022) Entangled in the technology-driven borderscape: border crossers rendered to their digital self. *European Journal of Criminology* 20(5): 1740–1758.
Franko Aas K (2011) 'Crimmigrant' bodies and bona fide travelers: surveillance, citizenship and global governance. *Theoretical Criminology* 15(3): 331–346.
Freeden M (2006) Ideology and political theory. *Journal of Political Ideologies* 11(1): 3–22.
Frowd P (2017) The promises and pitfalls of biometric security practices in Senegal. *International Political Sociology* 11(4): 343–359.
Fussey P, Davies B and Innes M (2020) 'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing. *British Journal of Criminology* 61(2): 325–344.
Gemalto (2018) Passport security features: 2018 report. Available at: https://www.id4africa.com/2019/almanac/GEMALTO-Joseph-Leibenguth.pdf (accessed 12 June 2024).
Gemalto (2019) Benefits of biometrics for border control. Available at: https://www.id4africa.com/2019_event/presentations/InF8/1-Alexandre-Caschetta-Gemalto.pdf (accessed 12 June 2024).
Glouftsios G (2021) Governing border security infrastructures: maintaining large-scale information systems. *Security Dialogue* 52(5): 452–470.
Goold B, Loader I and Thumala A (2013) The banality of security: the curious case of surveillance cameras. *British Journal of Criminology* 53(6): 977–996.
Halford S and Southerton D (2023) What future for the sociology of futures? Visions, concepts and methods. *Sociology* 57(2): 263–278.
Hannah-Moffat K (2019) Algorithmic risk governance: big data analytics, race and information activism in criminal justice debates. *Theoretical Criminology* 23(4): 453–470.
Haskins C (2024) 'I'm the new Oppenheimer!': My soul-destroying day at Palantir's first-ever AI warfare conference. Available at: https://www.theguardian.com/technology/article/2024/may/17/ai-weapons-palantir-war-technology (accessed 27 May 2024).
HID (2019) How advanced identification technologies are transforming border control in Africa. Available at: https://www.id4africa.com/2019_event/presentations/InF8/4-Joby-Mathew-HID.pdf (accessed 12 June 2024).

HID (2024) Biometric authentication & verification. Available at: https://www.hidglobal.com/solutions/biometric-authentication (accessed 12 June 2024).

ID4Africa (2024) About ID4Africa 2024. Available at: https://id4africaevents.com/2024/about/ (accessed 27 May 2024).

IDEMIA (2019a) Augmented identity at borders. Available at: https://www.id4africa.com/2019/almanac/IDEMIA-2.pdf (accessed 12 June 2024).

IDEMIA (2019b) The future of identity. *ID4Africa*. Available at: https://www.id4africa.com/2019/almanac/IDEMIA-1.pdf (accessed 27 May 2024).

IDEMIA (2021) The Digital Travel Credential: Taking seamless travel one step further by simplifying the travel process while increasing security and privacy. Available at: https://www.idemia.com/insights/digital-travel-credential-taking-seamless-travel-experience-one-step-further (accessed 22 April 2025).

IDEMIA (2022) Securing land and sea borders in Africa. Available at: https://www.idemia.com/insights/securing-land-and-sea-borders-africa (accessed 12 June 2024).

IDEMIA (2023) IDEMIA to supply seamless Passenger Flow Facilitation solution at Airports Company South Africa (ACSA). Available at: https://na.idemia.com/2023/12/06/idemia-to-supply-seamless-passenger-flow-facilitation-solution-at-airports-company-south-africa-acsa/ (accessed 22 April 2025).

IN Groupe (2022) What are the advantages of decentralized digital identity? Available at: https://ingroupe.com/insights/advantages-decentralized-digital-identity/ (accessed 12 June 2024).

Innovatrics (2023) 'Exceptional' biometrics: Solving local peculiarities of biometric identity projects. Available at: https://id4africa.com/wp-content/uploads/2023/06/PS3-3-Jan-Lunter-Innovatrics.pdf (accessed 12 June 2024).

IOM (2018) IOM and biometrics. Available at: https://www.iom.int/sites/default/files/our_work/DMM/IBM/iom_and_biometrics_external_info_sheet_november_2018.pdf (accessed 12 June 2024).

iProov (2022) How can biometrics streamline border control and immigration? Available at: https://www.iproov.com/blog/biometric-border-control-and-immigration-bio-corridor (accessed 12 June 2024).

iProov (2024) Biometric solutions for border control, visas, and immigration. Available at: https://www.iproov.com/use-cases/visas-borders-immigration (accessed 22 April 2025).

Jarrahi J (2021) Biometrics to drive dramatic growth in automated border control market. Available at: https://www.biometricupdate.com/202102/biometrics-to-drive-dramatic-growth-in-global-automated-border-control-market (accessed 27 May 2024).

Jegen LF (2023) 'Migratising' mobility: coloniality of knowledge and externally funded migration capacity building projects in Niger. *Geoforum; Journal of Physical, Human, and Regional Geosciences* 146: 103862.

Kawasaki G (2015) The art of evangelism. *Harvard Business Review* May: 108–111.

Lyon D (2017) Surveillance culture: engagement, exposure, and ethics in digital modernity. *International Journal of Communication* 11: 824–842.

MacDonald A (2023a) African countries reach data, digital ID interoperability deal to foster growth. Available at: https://www.biometricupdate.com/202305/african-countries-reach-data-digital-id-interoperability-deal-to-foster-growth (accessed 31 January 2024).

MacDonald A (2023b) France probes Thales subsidiary over past ID deals in Africa. Available at: https://www.biometricupdate.com/202302/france-probes-thales-subsidiary-over-past-id-deals-in-africa (accessed 27 May 2024).

Markelius A, Wright C, Kuiper J, et al. (2024) The mechanisms of AI hype and its planetary and social costs. *AI and Ethics* 4: 727–742.

Mascellino A (2023) ECOWAS Commission urges remaining 9 member states to issue biometric regional ID card. Available at: https://www.biometricupdate.com/202305/ecowas-commission-urges-remaining-9-member-states-to-issue-biometric-regional-id-card (accessed 31 January 2024).

McConvey J (2023) Botswana and Namibia select Veridos technology for cross-border digital ID. Available at: https://www.biometricupdate.com/202305/botswana-and-namibia-select-veridos-technology-for-cross-border-digital-id (accessed 31 January 2024).

McGuire MR and Renaud K (2023) Harm, injustice & technology: reflections on the UK's subpost-masters' case. *The Howard Journal of Crime and Justice* 62(4): 441–461.

Molnar P (2021) Surveillance sovereignty: migration management technologies and the politics of privatization. In: Molnar P (ed.) *Migration, Security, and Resistance*. London: Routledge, pp. 66–82.

Muller B (2010) *Security, Risk and the Biometric State: Governing Borders and Bodies*. Abingdon: Routledge.

Nishiyama H (2022) Bodies and borders in post-imperial Japan: a study of the coloniality of biometric power. *Cultural Studies* 36(1): 120–140.

Olwig K, Grünenberg K, Møhl P, et al. (2020) *The Biometric Border World: Technologies, Bodies and Identities on the Move*. Abingdon: Routledge.

Sánchez-Monedero J and Dencik L (2022) The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl. *Information, Communication & Society* 25(3): 413–430.

Schmidt R and Scott C (2021) Regulatory discretion: structuring power in the era of regulatory capitalism. *Legal Studies* 41(3): 454–473.

Secunet (2019) Three letters to ease inspection of electronic identity documents: PKI. Available at: https://www.id4africa.com/2019/almanac/SECUNET-Heiko-Bihr.pdf (accessed 12 June 2024).

Sharma N (2020) *Home Rule: National Sovereignty and the Separation of Natives and Migrants*. Durham, NC: Duke University Press.

Singler S (2021) Biometric statehood, transnational solutionism and security devices: the performative dimensions of the IOM's MIDAS. *Theoretical Criminology* 25(3): 454–473.

Singler S (2024) "Do it yourself!" Pedagogical performances, technical expertise, and crimmigration control in the IOM's capacity-building practices in Nigeria. *Geopolitics*. DOI: 10.1080/14650045.2024.2331802.

Singler S (2025) *Outsourcing Crimmigration Control: Digital Borders, the IOM, and Biometric Statehood*. Oxford: Oxford University Press.

Singler S and Babalola O (2024) Digital colonialism beyond surveillance capitalism? Coloniality of knowledge in Nigeria's emerging privacy rights legislation and border surveillance practices. *Social & Legal Studies*. DOI: 10.1177/09646639241287022.

Singler S and Milivojevic S (2024) The technopolitics of crimmigration control: targeting bodies and re-scaling borders. In: Bosworth M, Franko K, Lee M and Mehta R (eds) *Handbook on Border Criminology*. Cheltenham: Edward Elgar, 189–204.

SITA (2023) The digital transformation of borders and travel. Available at: https://id4africa.com/wp-content/uploads/2023/06/PS3-9-Jeremy-Springall-SITA.pdf (accessed 12 June 2024).

Söderström O, Paasche T and Klauser F (2014) Smart cities as corporate storytelling. *City* 18(3): 307–320.

Sopra Steria (n.d.) Transforming the immigration system through smartphone biometric enrolment. Available at: https://www.soprasteria.co.uk/docs/librariesprovider2/sopra-steria-uk-documents/thought-leadership/biometrics-paper-vf.pdf?sfvrsn=90cd10dc_3 (accessed 27 May 2024).

Soskis B (2022) CDG and support to the field of biometric identification for development. *Center for Global Development*. Available at: https://www.cgdev.org/sites/default/files/cgd-and-support-field-biometric-identification-development.pdf (accessed 22 April 2025).

South N (1988) *Policing for Profit: The Private Security Sector*. London: Sage.

Speed M (2020) Activists sound alarm over African biometric ID projects. Available at: https://www.aljazeera.com/economy/2020/12/10/activists-sound-alarm-over-african-biometric-id-projects (accessed 31 January 2024).

Stambøl E (2021) Neo-colonial penality? Travelling penal power and contingent sovereignty. *Punishment & Society* 23(4): 536–556.

Stumpf J (2006) The crimmigration crisis: immigration, crime, and sovereign power. *American University Law Review* 56(2): 367–420.

Thales (2023) Biometrics: Definition, use cases, latest news. Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (accessed 4 February 2024).

Thales (2025) Visa management system. Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/eborder/eborder-visa-management (accessed 13 January 2025).

Thales (n.d.) Namibia invests in world-class border management. Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/border-management-namibia (accessed 12 June 2024).

Trikanad S and Bhandari V (2022) Surveillance enabling identity systems in Africa: Tracing the fingerprint of Aadhaar. *Center for Internet and Society*. Available at: https://cis-india.org/internet-governance/surveillance-enabling-identity-systems-in-africa (accessed 13 January 2025).

Tutton R (2021) Sociotechnical imaginaries and techno-optimism: examining outer space utopias of silicon valley. *Science as Culture* 30(3): 416–439.

Valdivia A, Aradau C, Blanke T, et al. (2022) Neither opaque nor transparent: a transdisciplinary methodology to investigate datafication at the EU borders. *Big Data & Society* 9(2): 20539517221124586.

Vavoula N (2021) Artificial intelligence (AI) at Schengen borders: automated processing, algorithmic profiling and facial recognition in the era of techno-solutionism. *European Journal of Migration* 23: 457–484.

Veridos (2021) Identity for all: Africa rises to the challenge of enfranchising citizens lacking legal identities. Available at: https://web.archive.org/web/20250120093617/ https://www.veridos.com/en/topictrends/identity-for-all-africa-rises-to-the-challenge-ofenfranchising-citizens-lacking-legal-identities.html (accessed 12 June 2024).

Veridos (2024) Border management: Ensuring all guests are welcome. Available at: https://web.archive.org/web/20250214134747/https://www.veridos.com/en/border-management.html (accessed 12 June 2024).

White A (2012) The new political economy of private security. *Theoretical Criminology* 16(1): 85–101.

World Bank (2017) The state of identification systems in Africa: Country briefs. Available at: https://documents1.worldbank.org/curated/en/298651503551191964/pdf/119065-WP-ID4D-country-profiles-report-final-PUBLIC.pdf (accessed 13 January 2025).

Zedner L (2019) The hostile border: crimmigration, counter-terrorism, or crossing the line on rights? *New Criminal Law Review* 22(3): 318–345.

Zuboff S (2022) Surveillance capitalism or democracy? The death match of institutional orders and the politics of knowledge in our information civilization. *Organization Theory* 3(3): 1–79.

## Author biography

**Samuel Singler** is a Lecturer in Criminology in the Department of Sociology, University of Essex. His research focuses on the intersection of surveillance technologies, criminal justice, and border control. He co-leads the Technology & Digital Futures thematic group of the Border Criminologies network.