Science and Public Policy, 2024, **51**, 274–284
DOI: https://doi.org/10.1093/scipol/scad071
Advance Access Publication Date: 4 November 2023
Article

OXFORD

Biometrics, presents, futures: the imaginative politics of science–society orderings

Christopher Lawless[*]

Department of Sociology, Durham University, 32 Old Elvet, Durham DH1 3HN, United Kingdom

[*]Corresponding author. Department of Sociology, Durham University, 32 Old Elvet, Durham DH1 3HN, United Kingdom. E-mail: c.j.lawless@durham.ac.uk

Biometric technology encompasses a proliferating array of data forms, applications, and stakeholders but has raised numerous social and ethical concerns. This article examines contending perceptions of biometrics by developing a three-way framework of science–society orderings, drawn from social studies of biometrics and wider science studies literature. By analysing documentary sources and participant observation data through this framework, the article identifies a series of distinct normative interpretations or imaginaries of biometrics. It is argued that these imaginaries, described, respectively, as 'public good', 'collective control', and 'societal risks', project contending normative framings of science–society relations. These imaginaries were also however found to reflexively encompass perceived challenges, giving rise to practices that I term imaginative politics. These findings raise the need for science policy studies to consider the distinction between imagining and realizing in greater depth and to consider more profoundly the politics of science–society co-production.

Keywords: biometrics; imaginaries; artificial intelligence.

1. Introduction: anticipating and imagining the societal impact of biometric technology

While its precise definition may be contested, biometrics can be broadly construed as referring to technologies that measure and evaluate bodily data. Biometrics are increasingly employed as a means to identify individuals or verify identity. DNA, fingerprint, facial, and voice analysis are often cited as commonly used biometrics, particularly in relation to law enforcement or migration management (Home Office 2018). Biometric technologies have been valorized as presenting efficient solutions to policy issues in parts of the Global North such as the UK and European Union (EU) (Kaunert and Leonard 2012; European Commission 2018). The seemingly rapid evolution and development of biometric systems are however regarded as presenting a significant governance challenge in the light of possible impacts on privacy (Aston 2017; Scottish Parliament 2019). In addition, questions over the accuracy and reliability of systems such as facial recognition (FR) have raised concerns over whether biometric technology may unduly discriminate against certain groups (Buolamwini and Gebru 2018; Chowdhury 2020; Gebru 2020). The wide variety of biometric data forms and potential and actual use cases further compounds the challenge to biometric policymaking and ethical governance. Coupling biometric technology with artificial intelligence (AI) or virtual reality (VR) in the near future, as has been promulgated, may increase its power and scope, but also raises further governance challenges. For example, AI algorithms used in such technologies may evade scrutiny (Office of the Biometrics Commissioner 2018), and the capacity to use biometrics to impersonate others, either within VR environments or online, raises a host of further ethical and policy issues (Paterson and Hanley 2020).

The potential affordances and risks of contemporary biometric technologies have lent themselves to being analysed through various lenses related to technology anticipation and responsible innovation. Social researchers have critically examined methods such as DNA phenotyping (which claims to predict appearance from DNA samples) and DNA biogeographical analysis (the use of DNA sequences to identify the supposed geographical origin of an individual's ancestors) (Samuel and Prainsack 2019; Wienroth 2018, 2020; Hopman and M'charek 2020). These studies have challenged the assumption of technological development being a simple linear process of innovation (Godin 2006) and unproblematic application within society (Wienroth, McCormack, and Joyce 2014; Hopman, van Oorschot, and M'charek 2020). Instead, this research has revealed how biometric technologies entangle and encode scientific and sociocultural assumptions (Wienroth 2018; Hopman and M'charek 2020).

Political and commercial drivers that promote the widespread use of biometrics may be regarded, at least by some, as widespread social experiments (Nordmann 2009), in the sense that inter-related technical, social, and ethical outcomes may not be seen as readily predictable (Wienroth, McCormack, and Joyce 2014). Perceptions of potential outcomes, and whether they are regarded as more or less positive or negative, may vary with standpoint. Forensic DNA profiling methods have been found to entail fluid interactions between the differing epistemological and ethical perceptions of various actors, including scientists, law enforcement officials, lawyers, commercial actors, and regulators (Samuel and Prainsack 2019; Granja, Machado, and Queiros 2020; Wienroth 2020). These interactions reflect how developing and applying biometric technology may involve multiple legal, regulatory, and technical adjustments (Hopman, van Oorschot, and M'charek 2020). With this however come consequences for the co-construction of notions of race, ethics, justice, and other social orderings and valuings (Hopman and M'charek 2020). In addition to DNA, FR technology has been observed to coproduce social categorizations in ways some regard as markedly problematic (Wu and Zhang 2016; Levin 2017; Hamidi, Scheuerman, and Branham 2018; Wang and Kosinski 2018). Biometrics thus represents an analytically and ethically challenging example of the co-production of scientific and social orderings (Jasanoff 2004).

The interactional complexity and socioethical implications revealed by these studies only serve to reinforce the challenges to regulating and governing biometric technology. Taken in its entirety, biometrics represents a landscape that encompasses an increasing variety of stakeholders, data forms, and use contexts, which can transcend national borders. Embedded within this landscape are various hopes and fears (Williams and Johnson 2004; Machado and Granja 2019). The former, for example, may relate to the claimed ease that biometrics may bring to everyday life, such as travel or banking, framing biometrics less as a social experiment and more as an instrumental and unproblematic gateway to desired futures. Biometrics continues to be associated with ready solutions to crime and migration concerns (Franko Aas 2011; Singler 2021). On the other hand, the use of systems such as FR and DNA profiling has raised concerns over the consequences for human rights and the fears of unjust surveillance societies (Strittmatter 2019). Differing imaginaries have thus been associated with biometric systems. In some cases, these may reflect interpretations of technology already in use, or concerns about future use cases, as in the notion of 'function creep' (Koops 2021).

Emerging biometric technology thus stimulates various forms of anticipation and expectation. The complex social impacts, rapid development and proliferation of biometric data forms and technologies however test conceptual frameworks of technology policy, innovation management, and the sociology of expectations (Borup et al. 2006). This literature has often tended to focus on singular examples of technology (Korsnes 2016; Hilscher and Kivimaa 2019) rather than the proliferating and entangling arrays of technologies that characterize biometrics. Much of this broader literature has also benefited from being able to examine singular empirical examples of technology over relatively long historical periods (Hilscher and Kivimaa 2019). Such an approach may yield ample historical data but means that any analysis only comes retrospectively through hindsight. How then to address complex technological forms, whose futures, due to their fast-developing nature, may already have at least partially arrived?

A small number of studies have addressed biometrics explicitly in terms of imaginaries (Donovan 2015; Markó 2016; Gunnarsdottir and Rommetweit 2017). Donovan (2015) and Markó's (2016) studies of the rollout of biometric systems by the South African and South Sudanese governments uncovered marked differences between official visions and the practical application of biometric systems. In South Africa, the deployment of biometric identification systems for welfare claimants was beset by technical difficulties and allegations of corrupt tendering bids by firms (Donovan 2015). In South Sudan, Markó (2016) found that a costly biometric system to bestow citizenship in the newly independent state was circumvented by other forms of identification, which were notably nonscientific. These studies show how biometric imaginaries may impact a wide range of actors, including policymakers, technology providers, regulators, bureaucrats, and publics, albeit not necessarily on their own terms. As Donovan and Markó's studies indicate, different actors embedded into imaginaries may hold different standpoints, leading to different ways of engaging with and responding to technological initiatives. These studies invite a closer look at the diversity of perceptions and experiences on the part of those who find themselves engaging with biometric systems.

Much science and technology studies research has developed the related concept of the sociotechnical imaginary (Jasanoff and Kim 2009). Sociotechnical imaginaries have been described as technological plans or visions through which 'collectively imagined forms of social life and social order' (Jasanoff and Kim 2009: 120) are pursued. Sociotechnical imaginaries may be more or less optimistic or pessimistic (Kim 2014), and differing imaginaries may compete for predominance within particular policy domains (Delina 2018). Differing standpoints and interpretations of technology may lead to contested plans and imaginaries (Lawless 2020).

This article explores the possibility that biometrics may be embedded into multiple contending imaginaries. It considers how these imaginaries may differ, who invests in different imaginaries, and how they reflect different standpoints. The article examines how these imaginaries engage with biometric systems, and the wider societal contexts in which this technology is embedded but which it also shapes. It is shown here how this wider sociotechnical landscape presents perceived challenges to realizing imaginaries. This may lead imaginaries to interact with other contending visions. In addressing how imaginaries are advanced and challenged, the article identifies what I term imaginative politics. It is argued here that imaginative politics significantly reveals profound normative differences between stakeholders over desired science–society relations.

In what follows, I draw upon public understanding of science literature, and social studies of forensic science and biometric technology, to elucidate a three-way framework that I use to conceptualize differing visions of science–society orderings among biometric stakeholders. This enables the article to pursue a series of research questions that have so far been under-explored in the literature. I then draw upon fieldwork and documentary analysis to consider the differing kinds of envisioned science–society relations that seek to embed biometrics, and the challenges to promoting these differing orderings, as seen through the standpoints of stakeholder interest groups.

2. Three discursive models of science–society relations

The use of science and technology in law enforcement has been characterized by some researchers in terms of varying normative interpretations (Fraser 2007; Williams 2008). Social research on the contribution of forensic science to police investigations identified differing attitudes among police to the role of forensic practitioners. The latter were found to be regarded either as providing subordinated technical assistance to police who controlled the application of science or as alternatively representing a more epistemically authoritative means of contributing to police functions (Williams 2004).

Research on the public understanding of science has for some time focused on the differing assumptions concerning extra-scientific audience's expectations and engagement with science. Critical studies examined the implications of the so-called 'deficit' model. This model was posited as assuming that lay audiences lacked knowledge of science but would accept its claims and socially transformative potential once sufficiently educated (Bodmer 1985; Miller 2001).

Other reflections on forensic uses of biometric data have focused on claims that lay audiences assume too much knowledge about scientific evidence. This has been associated with the supposed over-exposure to forensic science from television programmes such as *CSI* (Cooley 2007; Hawkins and Scherr 2017). The notion that television had given audiences a distorted over-familiarity, or 'surfeit' of scientific knowledge, was claimed to necessitate re-educating the public about the limitations of forensic science and biometric data (Huey 2010). The 'surfeit' model has however itself been critiqued for reflecting another form of scientific hegemony over lay audiences (Lynch 2009; Cole 2015). The surfeit model nonetheless also reflects concerns about the extent to which lay users of biometric systems, such as police, understand their scientific basis and limitations (Granja, Machado, and Queiros 2020). The surfeit model reflects a normative interpretation of epistemic caution, emphasizing the risks of assuming certainty from what might actually be uncertain or ambiguous data.

Critical public understanding of science research has challenged these seemingly hegemonic assumptions of science–society relations. This line of research has instead highlighted the diversity of views that participate in differing ways to scientific understandings (Wynne 1996; Michael 2002). Similarly, the sociotechnical imaginaries literature highlights how technology can be perceived through a variety of standpoints from different actors, which shape and reflect contending imaginings that may frame science and technology in more or less positive terms (Jasanoff and Kim 2009; Kim 2014; Smith and Tidwell 2016). Social research has attended to the potentially problematic social impact of biometric technology and related ethical concerns, for example, in relation to racism (Granja and Machado 2020; Skinner 2020). This work indicates how biometric technology may be framed as emergent and potential due to being embedded in wider social contexts and issues. Scientists may themselves invoke extrinsic factors, such as commercial imperatives or legal processes, as barriers or affordances to their work (Lawless 2013).

This invocation of extra-scientific factors points to a third way of conceptualizing science–society engagement, which contrasts with the deficit and surfeit models. This normative interpretation solicits a more interdependent ordering of science and other social imperatives commensurate with Jasanoff's (2004) notion of 'co-production'. It invokes a mutual interdependency, rather than a hierarchical or deterministic relationship between science and society. Technologies are framed here as impacting upon society but are also regarded as shaped in turn by extra-scientific domains such as law, national boundaries, commerce, and social justice. The sociotechnical imaginaries literature has shown how visions of technology may be linked to projected societal risks and fears as much as they can be envisioned to produce benefits. Some studies have suggested that technology may not always be presumed to entail inevitable and irresistible developments and that societies may have greater agency to collectively make alternative choices. For example, Felt's (2015) study of Austrian public opposition to nuclear power and agro-biotechnology demonstrated how national histories and sensibilities shaped a more inclusive politics of technological choice, which embedded into a distinctly 'Austrian' sociotechnical imaginary.

The deficit and surfeit models both project forms of epistemic hegemony which assume that publics are ignorant of the 'realities' of science and should be educated by experts (Cole 2015). Critical public understanding of science and sociotechnical imaginaries literature however suggests the coexistence of contending normative interpretations of science–society relations, where hegemonies may be challenged and participation in scientific futures may be more diverse. Yet while previous research has pointed to the existence of different framings of forensic and biometric technology, much less has been said about *how* these interpretations coexist and interact. How do actors advance their own normative interpretations of science–society orderings over others, and how do actors perceive how others understand biometric technology? How are certain normative framings of science–society relations promoted, and what might challenge them? This article addresses these questions by examining the politics of science–society orderings across the community of biometric stakeholders.

The following section draws upon a range of data sources. These include public records of UK and Scottish parliamentary inquiries in the form of written submissions and transcripts of oral evidence. Parliamentary committees have devoted much attention to biometric technologies and they have captured a wide range of stakeholder views. The material used in this study includes five UK and Scottish inquiries over the years 2018–22, encompassing a total of 228 written submissions and thirty-nine oral evidence proceedings. The study also draws upon reports and position papers published by organizations such as the European Commission (EC) and nongovernmental organizations (NGOs) over the same time period.

This article also draws upon participant observation at a range of biometrics events that brought together representatives of industry, government, policy, law enforcement, academia, and civil society, which were attended between 2019 and 2022. Such events have been found to be highly fruitful sites of ethnographic inquiry on biometric technology, allowing researchers to observe the production of sociotechnical imaginaries and to examine how stakeholders collectively understand themselves and technology (Hockenhull and Cohn 2021; O'Neill et al. 2022). The events attended as part of this study were variously self-described as conferences, workshops, seminars, congresses, and summits. They were organized by bodies who described themselves as associations or institutes, or by academic institutions. The events ranged from 1-hour duration to 2.5 working days. The total duration attended was 53 h. Extensive notes were taken during these events, assisted by presentation slides where provided. The three-way framework described here was used to guide data collection and analysis by helping to identify specific discursive forms. The framework informed a deductive approach through which some hitherto unexpected findings emerged, as described in the next section.

3. Contending normative interpretations of biometrics

Biometrics was found to be framed as a high-level political issue. The EC has proposed legislation and regulation in the form of the AI Act, much of which addresses the development and use of biometric systems. Yet, as the following quote from a representative indicates, Members of the European Parliament (MEPs) are significantly polarized in terms of their attitudes towards this technology:

> It's really fifty-fifty…this is one of the very high-level political topics in the Parliament…you have two camps, and one camp is advocating for more bans, more restrictions and underlining how dangerous the use of biometrical data is, that we could become a kind of surveillance state, or states in the European Union, also underlining that companies are using those kinds of technologies more and more and spying on consumers and citizens and so on. Versus another political group in the Parliament which is kind of supportive of the Commission's approach and is saying well its good to address in the AI Act and besides that there is already a lot of existing legislation like anti-discrimination directives or GDPR [General Data Protection Regulation] and so on. So there is not really a need to put in additional provisions to prevent misuse of biometrical data. Again as you see, they are very far from each other and honestly right now I don't really know how we will find a compromise on that. (European Parliament Representative 2022)

Hence, MEPs are divided between those who view biometrics as threatening fundamental rights such as privacy and those who see the AI Act and other existing legislation as sufficient to guard against misuse. Here, biometrics was portrayed either as posing an intractable societal threat or as something which could be managed through European policy-making.

Elsewhere biometrics was framed in explicitly more positive terms. The use of biometric data to identify victims of the 2004 Asian tsunami was given at one conference as an example of one such public good (UK Biometrics Event 2022). It was therefore possible to discern a range of voices that projected biometrics in society in distinct but different ways: either in terms of *public good*, as amenable to *collective control*, or as posing *societal risks*.

3.1 Public good

Voices that framed biometrics in positive ways tended to legitimize them in terms of instrumentally delivering societal benefits, or public good, in various sectors including travel and law enforcement. These exhortations often reflected a certain recourse to authority. For example, positive portrayals often included the stated need to educate publics about the benefits:

> We need to educate…or to explain to them, what we are doing…we need to communicate so that our mother or our father can understand it. Normal people. But what we do is sometimes or often quite complicated, the technology, how does it work? Maybe it's easier to explain why we were are using it, we want to have security, we want to have seamless travel, the right to make life easier and secure at the same time, that's why we want to use biometrics. And I think a lot of people can understand that. (Discussion during UK Event 2022)

What is notable here is a sense of publics operating with an assumed deficit of knowledge about how biometric systems may actually work, but an assumption that they would accept them if their positive social impact could be clearly explained. The use of biometric technologies such as FR was at times normalized by reference to their use in more routine settings, projecting an idea that publics were already familiarizing themselves with these systems:

> Facial recognition is a technology we all encounter with increasing frequency. Whether it be at automated passport gates at airports, access to electronic devices or within digital photographic applications. (Scottish Police Federation 2019)

The *public good* interpretation was notably evident among statements and discussions involving police, government, and industry actors. The notion that technology could exert a significant positive impact, for example by rationalizing police functions, is illustrated by oral evidence given to the House of Lords Justice and Home Affairs Committee by the then UK Minister for Crime and Policing, Kit Malthouse:

> We essentially believe that technology can play a huge part in the prevention and detection of crime, and there are exciting developments under way as we speak that are already assisting and where we think we will see significant increases in police productivity and greater public safety as a result. (Kit Malthouse, oral evidence session, House of Lords Justice and Home Affairs Committee 2022: 2)

The emphasis placed by the former minister on perceived measurable impacts, such as public safety and 'police productivity', reflects a sense in which biometric technology may be perceived to deterministically shape benefits to public services. The UK Home Office Biometric Strategy, published in 2018, also promoted the idea of biometric systems delivering greater efficiency to public services:

> Rapid advances in the reliability and availability of biometric technologies, and the ability to search and match across different biometric data sets have the potential to support integrated services and better outcomes – such as finding or eliminating suspects or delivering more efficient services. (Home Office 2018: 6)

The public good interpretation also emphasized apparent public support for the police use of technologies such as FR. Publics were sometimes framed as expecting police to use new technology. Written evidence provided by the Metropolitan Police Service (MPS) to the House of Lords Justice and Home Affairs Committee exemplifies an ethical concern over the risk of law enforcement being prevented from using biometric technology:

> To declare technologies as being 'off limits' to policing risks denying law enforcement the tools it needs to keep the

> public safe whilst leaving these tools easily available for criminals and commercial users to consume and exploit. (Metropolitan Police Service 2021: 2)

Convincing others of the societal benefits of biometric technology was however seen to face challenges. One discussion, involving approximately fifty international representatives of industry, government, and law enforcement, heard numerous expressions of a perceived powerlessness and inability to inform the public about the positive impact of biometrics:

> Who stole our narratives? What about the good news? (Discussion during UK Event 2022)

In the discussion from which the above quote is taken, it was repeatedly claimed that certain (unnamed) organizations 'intentionally mispresent' biometrics and that the media also did so (UK Event 2022). During this exchange, it was also stated that a '…minority has a loud voice'. As before, education was emphasized as necessary in the light of such perceived distortions:

> The only way for a common societal consensus is common understanding…there is lots of misrepresentation. We should reach out and tell them they are wrong. There are legitimate use cases for FR. (Discussion during UK Event 2022)

In this exchange, publics and politicians were accused of being influenced by these supposed misrepresentations. During this discussion, it was claimed that US law enforcement had tried to push back against FR bans put in place in many jurisdictions. Politician's supposedly undue concerns over biometrics were framed as leading to unnecessary bureaucracy, hindering its effective use by law enforcement (UK Event 2022) a concern echoed during a UK inquiry:

> I would hate to see red tape getting in the way of our police being equipped with the correct tools to do their jobs effectively and provide the very best public protection. (Liam Owens, oral evidence session, House of Lords Justice and Home Affairs Committee 2021a: 13)
>
> We do not want to stand between a chief constable and a piece of kit or software that they want to have a go at. Being too bureaucratic or, if you like, strategic—with a small 's'—about that can often stand in the way. (Kit Malthouse, oral evidence session, House of Lords Justice and Home Affairs Committee 2022: 2)

Biometric technology was also framed as a threat outside of the hands of law enforcement. The term 'little brother' was repeatedly invoked during one event to describe how the public's access to smartphone cameras enabled them to record police activity, supposedly a hindrance to the latter's work (UK Event 2022). The ability to upload photographs and identify people's faces on social media was claimed to pose a severe hindrance to police covert activities. The private sector was responsibilized for allowing this to happen, and thus the unrestricted access to biometric technology was framed as a threat to public safety.

3.2 Collective control

Another discernible interpretation emphasized the risks of ignoring the limitations of biometric systems or related technologies such as AI:

> Part of the problem is the lack of nuance in the public debate on the use of technology and artificial intelligence. We all seem to think that it is a panacea and it will deliver us something that it may not necessarily be able to. There needs to be some acceptance of that. (Dr David Lewis, oral evidence session, House of Lords Justice and Home Affairs Committee 2021a: 8)
>
> A lot of people are hoping AI can do things it absolutely cannot do. A lot of people are claiming that they are able to make AI do a thing that it is not possible to do. (Professor Sandra Wachter, oral evidence session, House of Lords Justice and Home Affairs Committee 2021a: 14)

This more epistemically cautious interpretation raised concerns about assuming too much certainty of the impact and reliability of biometrics. As shown by the quotes above, this concern with the possible technical limitations of biometric technology was linked with a perceived need to manage expectations on the part of users and procurers:

> Users are too reliant and unquestioning when dealing with providers. (Discussion during UK Event 2022)
>
> Policing needs to be an intelligent customer: it needs to understand the problem it is trying to solve and how it is thought the technology will contribute to that. (David Tucker, oral evidence session, House of Lords Justice and Home Affairs Committee 2021b: 15)

This epistemically cautious normative interpretation responsibilized procurers and users to educate themselves about the precise utility and suitability of biometric systems when applied to specific use cases:

> What are my responsibilities if we introduce a biometric system? (Discussion during UK Event 2022)

One biometrics industry group has developed a Good Practice Framework to enable potential users or buyers to assess the possible technical and ethical risks which biometric systems may present. (Discussion during UK Event 2022)

As can be seen, epistemic caution was a notable aspect of discussions in fora such as parliamentary inquiries and others concerning oversight, regulation, and standardization of biometrics. There have been numerous inquiries into biometric policy conducted by the UK and Scottish Parliaments over the last decade (House of Commons Science and Technology Select Committee 2015; 2018; 2019; 2021; House of Lords Science and Technology Committee 2019; Scottish Parliament 2019; 2020b). These inquiries have variously considered forms of regulation and oversight of biometric data. The UK Parliament Select Committee on Science and Technology has however repeatedly criticized the levels of oversight of biometric systems such as FR in the UK:

> We reiterate our recommendation from our 2018 Report that automatic facial recognition should not be deployed until concerns over the technology's effectiveness and

> potential bias have been fully resolved. We call on the Government to issue a moratorium on the current use of facial recognition technology and no further trials should take place until a legislative framework has been introduced and guidance on trial protocols, and an oversight and evaluation system, has been established. (House of Commons Science and Technology Select Committee 2019: 4)

Much debate around oversight referred to biometrics as a 'landscape' or an 'ecosystem', reflecting the sense in which this technology was viewed as incorporating a complex assortment of data types, technologies, and use cases, across a heterogeneous array of stakeholders including researchers, developers, producers, vendors, and users. The proposed EC AI Act includes a standards regime. Introducing oversight mechanisms via the AI Act was seen by one EC representative to entail educating a wide array of stakeholders about their responsibilities in relation to proposed future regulations or pieces of existing data protection and equality legislation:

> What are the obligations? So you have the provider, who needs to undergo conformity assessment, and for biometrics there would be third party conformity assessment, to establish a quality management system, also a risk management system, to draw up the technical documentation, to conduct post-market monitoring, to collaborate with market surveillance authorities…the user obligations…are to use them [biometric systems] in accordance with the instructions of use, to ensure human oversight, monitor operations for certain risks, and meet all the existing legal obligations like the data protection rules, they continue to apply. There might also be other operators with certain obligations, it depends on where the system comes from, and how it has been dealt with, so there could be importers, distributors, or other third parties substantially changing the system. (EC Representative 2022)

However, in the UK context, the legislative and regulatory oversight of biometrics was regarded by some as extremely complex and challenging:

> The issue with regulation in this space is that there are so many regulators. Somehow we need to rationalise the number of regulators so that there is not a constant crossover of regulators and confusion about how they operate. (Dr David Lewis, oral evidence session, House of Lords Justice and Home Affairs Committee 2021a: 12).

A protocol for creating standards is being developed as part of the EC AI Act regime, but this study discerned a reflexive sense of the difference between the standards process in theory and the task of developing standards in practice. The latter was viewed as extremely difficult, given the proposed timescale for implementing the AI Act. Concerns were expressed over whether the right kind of technical expertise was being sought and how such experts could be contacted. This was perceived to represent a significant challenge to the timely introduction of standards:

> From a technical perspective it's a really tough and challenging problem…I think it won't be feasible even if you manage all these organizational issues of going from the national to the international level of having all of the stages included that are necessary, I think we need more time. (German Government Official 2022)
>
> We need many competencies. There is a challenge to break down the silo between different competencies in order to address the issue of regulation. It's really not easy finding such competencies, it's pretty tough in fact. To get them to one project is really a challenge. (French Government Official 2022)

Standardization itself was seen to present significant issues given the recognized interpretive flexibility of biometric terminology:

> Definitions are very difficult. (EC Representative 2022)

Definitions are nonetheless seen as integral to the work of key global actors such as the International Standards Organization. While some definitions have been formulated, for example in legislation (Scottish Parliament 2020a), in many other discussions biometrics were regarded as evading straightforward definitions. During one discussion, for example, an interlocutor questioned whether behavioural analysis (the inference of human behaviours from data) should be considered part of biometrics even though that has been included in definitions elsewhere:

> When did behavioural become biometric? Its analysis not measurement. (Discussion during UK Event 2022)

The drafting of the AI Act has been characterized by negotiations over the precise wording of definitions in the text. For example, remote biometric identification systems (RBISs), which could include forms of FR, are a key focus of the AI Act. As mentioned at one event (Biometrics Workshop 2022), the precise definition of RBIS has however been subject to amendment in the draft legislation text. An initial proposal defined RBIS thus:

> 'Remote biometric identification system' means an AI system for the purpose of identifying natural persons *at a distance* through the comparison of a person's biometric data *with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified*. (Article 3(36) Proposal, emphasis added for comparison)

The current working definition at the time of writing has however been altered:

> 'Biometric identification system' means an AI system for the purpose of identifying natural persons, through the comparison of a person's biometric data with the biometric data contained in a data repository. (Article 3(36) Compromise text)

Language was seen as a key issue for biometrics in other fora:

> Verification and authentication mean different things in different contexts…even within the biometrics industry

> words are used differently because of different use cases, different expertise backgrounds. (Discussion during UK Event 2022)

The possibility of developing a common knowledge base through standards and regulation was widely seen as hindered by the difficulties in deriving a universally agreed vocabulary for biometrics.

3.3 Societal risks

Normative interpretations of epistemic caution sometimes raised concerns about social harms of biometrics, such as the risk of FR discriminating against certain groups, by perceiving risks through technical shortcomings or lack of education on the part of the users. A third normative interpretation however was distinct, which framed extra-scientific factors as directly shaping biometric technology and its subsequent social impacts. This interpretation was particularly evident among civil society and civil liberties organizations that are critical of the use of biometrics by governments, in addition to some academic researchers.

During fieldwork, civil society organizations, for example, claimed that problematic moral sensibilities on the part of the state may influence how biometric systems are deployed. The placing of FR cameras outside abortion clinics, or LGBTQI+ spaces, were stated as examples of how biometric technology reflected the power of the state to use biometric technology to perpetuate prejudicial or discriminatory national attitudes and policies (Biometrics Workshop 2022). Other state-centric factors were invoked in discussions of the scope of the AI Act, for example around supposed 'military' or 'national security' uses of biometrics and whether they should be exempt from this legislation. One civil society representative claimed that what counted as a 'military' application was regarded by some as a grey area:

> [A European legal NGO] has focused on this question of military purposes and pointed out that military purposes doesn't actually have a specific definition…so there's potential that military purposes could be interpreted very broadly. Some readings could see it even being applied to humanitarian action, where people are often at their most vulnerable. (Civil Society Representative 2022)

'National security' was claimed to be another nebulous term:

> There just isn't right now, legally or technically, a clear line between what is law enforcement and what is national security. (Civil Society Representative 2022)

Yet, these terms were regarded as nonetheless significantly shaping attitudes towards legitimate uses of biometric technology.

Jurisdictionality was associated with other potentially problematic uses of biometrics. The draft AI Act has been criticized for potentially prohibiting the use of some biometric systems in the EU while still allowing EU-based producers to sell their products for use elsewhere:

> One big issue we would advocate for is the sale of AI systems by companies founded within the European Union to countries or actors outside of the Union. To take one example, there's a Spanish company we were on a panel with, when we pointed out they were developing ethnic profiling capabilities or selling it as part of their facial recognition, the CEO said "we don't sell that part of our technology within the EU" and I think it's not right that people can be ethnically profiled by machines elsewhere in the world by an EU company. (Civil Society Representative 2022)

By highlighting these kinds of potential discrepancies, jurisdictionality was framed as a significant factor that could shape differential thresholds of acceptability. Civil society organizations regarded this as problematic, given that technologies opposed in Global North jurisdictions may be developed and used in parts of the Global South, perpetuating what has been termed 'technocolonialism' (Madianou 2022), and thus an unequal two-tier global biometric order. Earlier colonial legacies were also invoked through this narrative. Voice analysis, for example, has been framed as highly intrusive, potentially claiming to reveal personal information pertaining to home location, health, intoxication, or age, which may or may not be accurate or valid. Critical framings pointed to markets for this technology in areas outside the EU with colonial histories linked with the imposition of European languages such as French, Spanish, and Portuguese (Academic researcher, Biometrics Workshop 2022).

This framing also invoked the influence of commercial interests in shaping biometric usage and policy. Discourses concerning the EU's broad AI strategy have emphasized a global competition in which the EU has to maintain a leading position in order to reap the supposed economic benefits (European Commission 2018, 2020). Critical voices claimed that the AI Act may bestow more powers to commercial companies over an individual's data even while limiting the Member State's capacity for biometric surveillance (Academic researcher, Biometrics Workshop 2022). A perception of a complex entanglement of commercial and state interests was thus part of this alternative framing.

Aligned with this interpretation was the narrative that civil society has the agency to decide what are acceptable and unacceptable use cases of biometrics. For example, one event attended as part of fieldwork included a discussion of the Europe-wide 'Reclaim Your Face' campaign, which opposes FR in public spaces. A presentation depicted photos of individuals placing paper bags over their heads as symbolizing the capacity of citizens to resist.

As with the examples given of biometrics impacting LGBTQI+ spaces and abortion clinics, the societal risks interpretation emphasized concerns over the impact of biometrics in terms of diversity. This is also exemplified by concerns over the risks of FR to perpetuate discriminatory practices (Big Brother Watch 2018). Diversity was however recognized as challenging, given that different technologies and use cases, even if contentious to some, may be perceived differently by others. Public surveys of FR, for example, indicate more support among respondents reporting as white than persons of colour and greater support among older age groups compared to younger respondents (Ada Lovelace Institute 2019; London Policing Ethics Panel 2019; Chowdhury 2020).

The potential ubiquity of AI-linked biometrics was also seen as representing a challenge to maintaining ethical vigilance. One workshop participant claimed that the normalization of this technology could lead to ethical concerns being ignored or forgotten:

> Although technically we could have biometric systems everywhere…if we get to a stage where almost every service, or at least the good services, the cheap services…if you're incentivised to use the biometric option, what does it mean…does that push us more towards a future where people don't think about the rights, risks, of certain use cases or where it helps to make certain use cases appear like they have fewer risks than they do? (Civil Society Representative 2022)

Here, the wider societal embrace and entanglement of biometric technology, seen to be aided and abetted by state and commercial drivers, was perceived to shape public and political attitudes in a potentially risky way.

4. The imaginative politics of biometrics

Each normative interpretation projected different rights and responsibilities for different groups. The public good interpretation obligated the media to depict biometric technology in the 'correct' manner, and not to mislead publics and politicians, so that authorities could uphold public safety. The collective control interpretation responsibilized all parties to be fully cognizant of technological limits and to uphold standards. The societal risks interpretation emphasized the need for citizens to protect their rights.

Moreover, these interpretations all projected differing ideas about what the relationship between science and society *should* be. Public good projected a form of technological determinism in emphasizing the rationalization of societal functions. The sense that publics would accept biometric technology once educated is also redolent of a deficit-model discourse. Collective control emphasized a sense of epistemic caution, urging that providers and users had to educate themselves about the limitations of technology, reflective of a surfeit-model discourse. While sometimes invoking engagement with civil society, the collective control interpretation emphasized a largely technocratic vision in which the role of scientific experts in regulating biometrics featured prominently. Finally, the societal risks interpretation framed the evolution of biometric technology and its uses in a way redolent of a decidedly less hierarchical form of science–society co-production, expressed through the concern of biometrics reinforcing pre-existing state and commercial power structures, and the perceived need for greater public engagement.

These three normative interpretations can be regarded as imaginaries in that each framed a series of perceived sociotechnical challenges that needed to be overcome in order that particular desired science–society orderings be realized. Promoting imaginaries was sometimes seen as a contest against opposing groups, such as from those who projected particularly positive or more wary imaginaries of biometrics, as in the case of public good versus societal risks. The collective control interpretation alternatively framed biometrics as presenting a challenge in terms of how it could and should be regulated, as technology that evaded easy definition and encompassed an ever-increasing variety of use cases and stakeholders.

The reflexive recognition of challenges or opposition from within these imaginaries is a significant and unexpected finding. In the case of public good, this entailed a perception of disempowerment among law enforcement, government, and industry actors in the face of media and other (largely unidentified) actors who were regarded as misrepresenting biometrics to under-informed publics and politicians. For the collective control imaginary, the rapid evolution of data forms, technologies, and use cases represented a sociotechnical ecosystem that was seen as presenting difficulties in formulating cohesive regulatory arrangements and in educating a wide range of stakeholders. The societal risks imaginary framed the enduring power of state and commercial structures as almost implacable opponents, but also saw a challenge in addressing public opinion, which was seen as diverse and heterogeneous.

The perceived challenges invoked from within these imaginaries represented points at which differing assumptions of science–society orderings sometimes engaged with each other. The broadly technological determinist imaginary of public good engaged with the epistemic caution of collective control via concerns about bureaucracy being perceived to impede the use of biometric systems for public benefit. This faced up against concerns about how well-informed users were about these systems and their attendant risks. The collective control imaginary engaged with the societal risks imaginary over the extent to which the risks of biometric technology could be managed. Policymakers saw regulation and legislation such as the AI Act as key, but other voices expressed concern over whether these measures might not go far enough and could indeed themselves perpetuate adverse outcomes such as inequities between the Global North and South. The collective control and societal risks imaginaries also differed over who should have a say in the shaping of biometric technology. The greater emphasis on technocratic oversight within the collective control imaginary contrasted with the primacy given to civil society by the societal risks imaginary. Finally, public good engaged with the societal risks imaginary in contestations between the perceived power relations between authorities on one hand, and supposedly 'misinformed' audiences on the other.

Engagements between imaginaries were thus manifest in how interactions between these standpoints, encompassing law enforcement and government, industry, academia, policy, and civil society, represented efforts to embed biometric systems within contending science–society framings. This involved collective anticipations of where resistance lay, in the form of certain perceived sociotechnical assemblages of biometric technology and actors, in which obstacles to each imagined science–society ordering were to seen to lie. These differing kinds of engagements between contending imaginaries of science–society orderings can be said to represent instances of *imaginative politics*, which are summarized in Table 1. Here, imaginative politics revolved around contests for which desired notion of science–society relations should be institutionalized and thus for which particular sociotechnical configuration should prevail. Imaginative politics was performed in a variety of ways. These included rhetorical exhortations about opposing or misrepresenting forces, varying forms of responsibilization, expressed desires to build consensus and

Table 1. The imaginative politics of normative interpretations of biometrics.

Normative interpretation	Science–society ordering	Perceived challenges
Public good	Technological determinism	Misrepresentation of biometrics 'Irresponsible' publics and producers Excessive bureaucracy
Collective control	Epistemic caution/technocracy	Complexity/variety of biometric ecosystems Stakeholder awareness of risks and limitations of technology Standardization and interpretive flexibility of definitions
Societal risk	Co-production	Power of governments, authorities, and commercial actors Normalization of biometrics obscuring ethical concerns Diverse public attitudes

coalitions, the desired mobilization of civil society, and recognition of established political institutions and debates over whether these should be challenged or engaged with. Here, the space in which imaginative politics was played out was inherently sociotechnical, given that biometrics inevitably entangles a wide range of scientific disciplines, data forms, and technologies with public and private services, policy, governance, jurisdictionality, human rights, ethics, and other societal imperatives.

5. Conclusion

This article has identified contending normative interpretations or imaginaries of biometric technology among a wide array of stakeholders. These were examined through the analytical lens of a three-way framework of projected science–society relations derived from science studies literature. By identifying these normative framings, this article has drawn attention to the different possible worlds biometrics are collectively viewed to both potentially shape and inhabit. Contending normative interpretations projected different envisaged sociotechnical orders which varied in terms of who should control data flows, who should decide how biometrics are developed and applied, what types of biometrics and use cases are deemed acceptable, and how these systems should be tested and assessed. These imagined orders legitimate differing science–society relations which in turn uphold or challenge institutions and hierarchies. By promoting the assumption that technology instrumentally enhances public safety and security, public good legitimates the freedom of law enforcement to use biometric systems in any way they see fit. Collective control's epistemically cautious emphasis on technocratic regulation and stakeholder education reflects a scientific hegemony supported by entrenched national and international policy institutions and processes. In contrast, the societal risks framing promotes the right for publics to have a much greater say in how biometrics are developed and used, by projecting a less hierarchical science–society ordering and claiming that the self-interested actions of government and commerce can and should be challenged. Thus by envisioning distinct sociotechnical orders, differing normative interpretations may reinforce or critique state authority and commercial interests (e.g. public good versus societal risks), or transcend state boundaries and public/private distinctions through technical collaboration, most notably exemplified by collective control.

This article advances sociotechnical imaginaries literature by first highlighting how contending imaginaries may interact, a phenomenon that still merits much more concerted inquiry. Moreover, this article contributes to ongoing conversations on sociotechnical imaginaries by drawing attention to how normative interpretations legitimate themselves and underpinning science–society orderings not only by projecting and promoting certain sociotechnical arrangements but also by projecting resisting configurations of actors, data flows, and objects. These normative interpretations thus promoted visions of desirable sociotechnical orders by building less desirable worlds which needed to be reshaped. The latter were seen to challenge desired science–society relations underpinning differing imaginaries, in the form of, for example: 'misinformed' media and publics, and unnecessary bureaucracy (public good); users unaware of the limitations and risks of biometric technology, and technology evading regulation partly through disagreements on definitions (collective control); or power structures perpetuating unjust mutual shapings of science and society (societal risk).

The awareness of such resistance advances previous literature on biometric imaginaries that uncovered disjunctures between imaginaries and their practical implementation, albeit in hindsight (Donovan 2015; Markó 2016). This article instead identifies how forms of collective imagining entail a significant degree of reflexivity, rather than uncritical projection. Here, this reflexivity was based on a recognized distinction between imagining and realizing, brought about by the anticipation of the seeming challenges raised by various perceived sociotechnical entanglements. The distinction between imagining and realizing has received relatively little consideration in the wider corpus of sociotechnical imaginaries studies to date. Awareness of this distinction however alerts us to how reflexivity within imaginaries drives imaginative politics, based on actual or perceived sociotechnical resistance. As we have seen here, profound issues of science–society orderings are at stake. Imaginative politics, as contests for which desired notion of science–society relations should prevail, points to a need to consider in much more depth the normative aspects of science–society co-production. Here, imaginaries reflecting technological determinism and epistemic caution contended with an imaginary more redolent of Jasanoff's idiom of co-production (Jasanoff 2004). Rather than thinking of politics purely as a contributor **to** co-production, or politics **as** co-production, this study has therefore opened the need to consider more profoundly the politics **of** co-production.

Acknowledgements

The author wishes to thank the two anonymous reviewers and the editors for their feedback.

Conflict of interest statement. None declared.

Funding

This article was not supported by any funding.

Data availability

Some data used here are on the public record via parliamentary inquiries. Other data are not publicly available in order not to compromise the privacy of respondents. Please contact the corresponding author for further details.

References

Ada Lovelace Institute. (2019) *Beyond Face Value: Public Attitudes to Facial Recognition Technology*. London: Nuffield Foundation.

Aston, V. (2017) 'State Surveillance of Protest and the Rights to Privacy and Freedom of Assembly: A Comparison of Judicial and Protestor Perspectives', *European Journal of Law and Technology*, 8: 1–19.

Big Brother Watch. (2018) *Face Off: The Lawless Growth of Facial Recognition in UK Policing*. London: Big Brother Watch.

Bodmer, W. (1985) *The Public Understanding of Science*. London: Royal Society.

Borup, M. et al. (2006) 'The Sociology of Expectations in Science and Technology', *Technology Analysis & Strategic Management*, 18: 285–98.

Buolamwini, J., and Gebru, T. (2018) 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', in *Proceedings of Machine Learning Research*, Vol. 81, pp. 1–15.

Chowdhury, A. (2020) *Unmasking Facial Recognition: An Exploration of the Racial Bias Implications of Facial Recognition Surveillance in the United Kingdom*. London: Webroots Democracy.

Cole, S. A. (2015) 'A Surfeit of Science: The "CSI Effect" and the Media Appropriation of the Public Understanding of Science', *Public Understanding of Science*, 24: 130–46.

Cooley, C. M. (2007) 'The CSI Effect: Its Impact and Potential Concerns', *New England Law Review*, 41: 471–502.

Delina, L. L. (2018) 'Whose and What Futures? Navigating the Contested co-production of Thailand's Energy Sociotechnical Imaginaries', *Energy Research & Social Science*, 35: 48–56.

Donovan, K. (2015) 'The Biometric Imaginary: Bureaucratic Technopolitics in Post-apartheid Welfare', *Journal of Southern African Studies*, 41: 815–33.

European Commission. (2018) *Artificial Intelligence for Europe: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*. Brussels: European Commission.

European Commission. (2021) 'Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts', COM(2021) 206 Final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206, accessed 28 Aug. 2021.

Felt, U. (2015) 'Keeping Technologies Out: Sociotechnical Imaginaries and the Formation of Austria's Technopolitical Identity', in S. Jasanoff and S.-H. Kim (eds.) *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*, pp. 103–25. Chicago, IL: Chicago University Press.

Franko Aas, K. (2011) '"Crimmigrant" Bodies and Bona Fide Travellers: Surveillance, Citizenship and Global Governance', *Theoretical Criminology*, 15: 331–46.

Fraser, J. (2007) 'The Application of Forensic Science to Criminal Investigation', in T. Newburn, T. Williamson, and A. Wright (eds.) *Handbook of Criminal Investigation*, pp. 381–402. Cullompton: Willan.

Gebru, T. (2020) 'Race and Gender', in M. D. Dubber, F. Pasquale, and S. Das (eds.) *The Oxford Handbook of Ethics of AI*, pp. 253–70. New York, NY: Oxford University Press.

Godin, B. (2006) 'The Linear Model of Innovation: The Historical Construction of an Analytical Framework', *Science, Technology & Human Values*, 31: 639–67.

Granja, R., and Machado, H. (2020) 'Forensic DNA Phenotyping and Its Politics of Legitimation and Contestation: Views of Forensic Geneticists in Europe', *Social Studies of Science*, 1–19.

Granja, R., Machado, H., and Queiros, F. (2020) 'The (De)materialization of Criminal Bodies in Forensic DNA Phenotyping', *Body & Society*, 27: 60–84.

Gunnarsdottir, K., and Rommetweit, K. (2017) 'The Biometric Imaginary: (Dis)trust in a Policy Vacuum', *Public Understanding of Science*, 26: 195–211.

Hamidi, F., Scheuerman, K. M., and Branham, S. M. (2018) 'Gender Recognition or Gender Reductionism? The Social Implications of Automatic Gender Recognition Systems', in *Computer Human Interaction 2018 Conference*, April 21–26, 2018. Montreal Canada.

Hawkins, I., and Scherr, K. (2017) 'Engaging the CSI Effect: The Influences of Experience-taking, Type of Evidence, and Viewing Frequency on Juror Decision-making', *Journal of Criminal Justice*, 49: 45–52.

Hilscher, S., and Kivimaa, P. (2019) 'Governance through Expectations: Examining the Long-term Policy Relevance of Smart Meters in the United Kingdom', *Futures*, 109: 153–69.

Hockenhull, M., and Cohn, M. (2021) 'Hot Air and Corporate Sociotechnical Imaginaries: Performing and Translating Digital Futures in the Danish Tech Scene', *New Media & Society*, 23: 302–21.

Home Office. (2018) *Biometrics Strategy: Better Public Services Maintaining Public Trust*. London: Home Office.

Hopman, R., and M'charek, A. (2020) 'Facing the Unknown Suspect: Forensic DNA Phenotyping and the Oscillation between the Individual and the Collective', *BioSocieties*, 15: 438–62.

Hopman, R., van Oorschot, I., and M'charek, A. (2020) 'From Promise to Practice: Anticipatory Work and the Adoption of Massive Parallel Sequencing in Forensics', in V. Toom, M. Wienroth, and A. M'charek (eds.) *Law, Practice and Politics of Forensic DNA Profiling: Forensic Genetics and Their Technolegal Worlds*, pp. 93–110. Abingdon, NY: Routledge.

House of Commons Science and Technology Select Committee. (2015) *Current and Future Uses of Biometric Data and Technologies: Sixth Report of Session 2014-15*. London: Her Majesty's Stationery Office.

House of Commons Science and Technology Select Committee. (2018) *Biometric Strategy and Forensic Services: Fifth Report of Session 2017-19*. London: Her Majesty's Stationery Office.

House of Commons Science and Technology Select Committee. (2019) *The Work of the Biometrics Commissioner and the Forensic Science Regulator*. London: Her Majesty's Stationery Office.

House of Commons Science and Technology Select Committee. (2021) *Oral Evidence: Biometrics and Forensics: Follow-up*. London: Her Majesty's Stationery Office.

House of Lords Justice and Home Affairs Committee. (2021a) 'Formal Meeting (Oral Evidence Session) 19 October 2021', https://committees.parliament.uk/oralevidence/2882/pdf/, Accessed 13 Dec. 2022.

House of Lords Justice and Home Affairs Committee. (2021b) 'Formal Meeting (Oral Evidence Session) 23 November 2021', https://committees.parliament.uk/oralevidence/3077/pdf/, Accessed 13 Dec. 2022.

House of Lords Justice and Home Affairs Committee. (2022) 'Formal Meeting (Oral Evidence Session) 12 January 2022', https://committees.parliament.uk/oralevidence/3287/pdf/, Accessed 13 Dec. 2022.

House of Lords Science and Technology Committee. (2019) *Forensic Science and the Criminal Justice System: A Blueprint*. 3rd Report of Session 2017-19. HL Paper 333. London: House of Lords.

Huey, L. (2010) '"I've Seen This on CSI": Criminal Investigators' Perceptions about the Management of Public Expectations in the Field', *Crime, Media, Culture: An International Journal*, 6: 49–68.

Jasanoff, S. (2004) *States of Knowledge: The Co-production of Science and the Social Order*. London: Routledge.

Jasanoff, S., and Kim, S.-H. (2009) 'Containing the Atom: Sociotechnical Imaginaries and Nuclear Regulation in the US and South Korea', *Minerva*, 47: 119–46.

Kaunert, C., and Leonard, S. (2012) 'The European Union Asylum Policy after the Treaty of Lisbon and the Stockholm Programme: Toward Supranational Governance in a Common Area of Protection?', *Refugee Survey Quarterly*, 31: 1–20.

Kim, S.-H. (2014) 'The Politics of Human Embryonic Stem Cell Research in South Korea: Contesting National Sociotechnical Imaginaries', *Science as Culture*, 23: 293–319.

Koops, B.-J. (2021) 'The Concept of Function Creep', *Law, Innovation and Technology*, 13: 29–56.

Korsnes, M. (2016) 'Ambition and Ambiguity: Expectations and Imaginaries Developing Offshore Wind in China', *Technological Forecasting and Social Change*, 107: 50–8.

Lawless, C. J. (2013) 'The Low-template DNA Profiling Controversy: Biolegality and Boundary Work among Forensic Scientists', *Social Studies of Science*, 43: 191–214.

Lawless, C. J. (2020) 'Assembling Airspace: The Single European Sky and Contested Transnationalities of European Air Traffic Management', *Social Studies of Science*, 50: 680–704.

Levin, S. (2017) 'LGBT Groups Denounce "Dangerous" AI That Uses Your Face to Guess Sexuality', *The Guardian*. https://www.theguardian.com/world/2017/sep/08/ai-gay-gaydar-algorithm-facial-recognition-criticism-stanford, Accessed 17 Aug. 2017.

London Policing Ethics Panel. (2019) *Final Report on Facial Recognition*. London: London Policing Ethics Panel.

Lynch, M. (2009) 'Science as a Vacation: Deficits, Surfeits, PUSS, and Doing Your Own Job', *Organization*, 16: 101–19.

Machado, H., and Granja, R. (2019) 'Risks and Benefits of Transnational Exchange of Forensic DNA Data in the EU: The Views of Professionals Operating the Prüm System', *Journal of Forensic and Legal Medicine*, 68: 1–7.

Madianou, M. (2022) 'Technological Futures as Colonial Debris: "Tech for Good" as Technocolonialism', in J. Zylinska and G. Media (eds.) *The Future of Media*, pp. 281–96. London: Goldsmiths Press.

Markó, F. D. (2016) '"We Are Not a Failed State, We Make the Best Passports": South Sudan and Biometric Modernity', *African Studies Review*, 59: 113–32.

Metropolitan Police Service. (2021) *Written Evidence to House of Lords Justice and Home Affairs Committee Inquiry: New Technologies and the Application of the Law (NTL0031)*. London: Metropolitan Police Service.

Michael, M. (2002) 'Comprehension, Apprehension, Prehension: Heterogeneity and the Public Understanding of Science', *Science, Technology & Human Values*, 27: 357–78.

Miller, S. (2001) 'Public Understanding of Science at the Crossroads', *Public Understanding of Science*, 10: 115–20.

Nordmann, A. (2009) 'European Experiments', *Osiris*, 24: 278–302.

Office of the Biometrics Commissioner. (2018) *Commissioner for the Retention and Use of Biometric Material: Annual Report 2017*. London: Her Majesty's Stationery Office.

O'Neill, C. et al. (2022) 'The Faces of the Child in Facial Recognition Industry Discourse: Biometric Capture between Innocence and Recalcitrance', *Information, Communication and Society*, 25: 752–67.

Paterson, T., and Hanley, L. (2020) 'Political Warfare in the Digital Age: Cyber Subversion, Information Operations and "Deep Fakes"', *Australian Journal of International Affairs*, 74: 439–54.

Samuel, G., and Prainsack, B. (2019) 'Forensic DNA Phenotyping in Europe: Views "On the Ground" from Those Who Have a Professional Stake in the Technology', *New Genetics and Society*, 38: 119–41.

Scottish Parliament. (2019) *Scottish Biometrics Commissioner Bill Stage 1 Report*. Edinburgh: Scottish Parliament.

Scottish Parliament. (2020a) Scottish Biometrics Commissioner Act.

Scottish Parliament. (2020b) *Facial Recognition: How Policing in Scotland Makes Use of This Technology*. Justice Sub-committee on Policing. 1st Report (Session 5). Edinburgh: Scottish Parliament.

Scottish Police Federation. (2019) *Written Submission to Scottish Parliament Justice Sub-committee on Policing Inquiry: Facial Recognition: How Policing in Scotland Makes Use of This Technology*. Glasgow: Scottish Police Federation.

Singler, S. (2021) 'Biometric Statehood, Transnational Solutionism and Security Devices: The Performative Dimensions of the IOM's MIDAS', *Theoretical Criminology*, 25: 454–73.

Skinner, D. (2020) 'Forensic Genetics and the Prediction of Race: What Is the Problem?', *BioSocieties*, 15: 329–49.

Smith, J. M., and Tidwell, A. S. D. (2016) 'The Everyday Lives of Energy Transitions: Contested Sociotechnical Imaginaries in the American West', *Social Studies of Science*, 43: 327–50.

Strittmatter, K. (2019) *We Have Been Harmonized*. London: Old Street Publishing.

Wang, Y., and Kosinski, M. (2018) 'Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images', *Journal of Personality and Social Psychology*, 114: 246–57.

Wienroth, M. (2018) 'Governing Anticipatory Technology Practices: Forensic DNA Phenotyping and the Forensic Genetics Community in Europe', *New Genetics and Society*, 37: 137–52.

Wienroth, M. (2020) 'Socio-technical Disagreements as Ethical Fora: Parabon NanoLab's Forensic DNA Snapshot™ Service at the Intersection of Discourses around Robust Science, Technology Validation, and Commerce', *BioSocieties*, 15: 28–45.

Wienroth, M., McCormack, P., and Joyce, T. J. (2014) 'Precaution, Governance and the Failure of Medical Implants: The ASR^{TM} Hip in the UK', *Life Sciences, Society and Policy*, 10: 1–16.

Williams, R. (2004) *The Management of Crime Scene Examination in Relation to the Investigation of Burglary and Volume Crime*. Home Office Online Report. London: The Home Office.

Williams, R. (2008) 'Policing and Forensic Science', in T. Newburn (ed.) *Handbook of Policing*, pp. 760–93. Cullompton: Willan.

Williams, R., and Johnson, P. (2004) '"Wonderment and Dread": Representations of DNA in Ethical Disputes about DNA Databases', *New Genetics and Society*, 23: 205–23.

Wu, X., and Zhang, X. (2016) 'Automated Inference on Criminality Using Face Images', arXiv. https://arxiv.org/pdf/1611.04135v1.pdf, Accessed 4 Aug. 2021.

Wynne, B. E. (1996) 'May the Sheep Safely Graze? A Reflexive View of the Expert-Lay Knowledge Divide', in S. Lash, B. Szerszynski, and B. Wynne (eds.) *Risk, Environment and Modernity: Toward a New Ecology*, pp. 44–83. London: Sage.