

Christopher Lawless

Department of Sociology, Durham University

The Evolution, Devolution and Distribution of UK Biometric Imaginaries

Published online first in *BioSocieties* 5 May 2021

Abstract

This article critically examines UK biometric policymaking by charting the bodies identified by the 2018 Home Office Biometric Strategy as playing key roles in the oversight of biometric data used in law enforcement and other related functions. The article argues that oversight actors are embedded in biometric imaginaries promoted by the UK Home Office and the devolved Scottish administration. By mapping oversight of UK biometrics policy together with developments in Scotland, the article challenges sociotechnical imaginaries studies which assume the power of national governments to project dominant, cohesive and instrumental visions. The article peels away that image to reveal UK biometric policy as located within a patchwork in which embedded commissioners, regulators and advisors challenge biometric imaginaries through interpretive flexibility and standpoint. By identifying technical, operational, legislative and ethical issues, these actors challenge the UK government imaginary and act as channels of critique between it and wider stakeholder communities. The article further challenges assumptions concerning the cohesion of national imaginaries by highlighting a diverging approach to biometric governance in Scotland. The article uses these observations to sketch a means to further characterize the notion of the biometric imaginary and to address biometric policymaking more widely.

Keywords

Biometric data; Forensic science; Sociotechnical Imaginaries; Policy.

Introduction

In July 2019, the House of Commons Science and Technology Select Committee reported on its inquiry into the work of the UK Biometrics Commissioner and the Forensic Science Regulator, the latest in a series of similar inquiries stretching back at least fifteen years (House of Commons, 2005, 2011, 2013, 2015, 2018, 2019, House of Lords, 2019). The Committee strongly criticised the UK Government's 27-page Home Office Biometrics Strategy, claiming it "was not worth the five year wait. Arguably it is not a 'strategy' at all: it lacks a coherent, *forward looking vision* and fails to address the legislative vacuum that the Home Office has allowed to emerge around new biometrics." (House of Commons, 2019: 20, emphasis added). The Committee also expressed deep concern over the status of forensic science, describing an "unstable forensics market which has been on the brink of collapse" (ibid: 20) over which the Government had failed "to show leadership" by not implementing legislation to strengthen oversight.

The Committee's harsh criticisms of the alleged lack of government leadership and foresight on forensics and biometric data systems, which encompass a diversifying, advancing, increasingly seductive yet ethically contentious range of technologies, contrasts with a growing body of literature which has employed the concept of the sociotechnical imaginary to depict how governments project "collectively imagined forms of social life and social order" (Jasanoff and Kim, 2009: 120) through technology policy. Sociotechnical imaginaries have been used to frame how governments seek "to influence technological design, channel public expenditures, and justify the inclusion or exclusion of citizens with respect to the

benefits of technological progress”. (ibid). Sociotechnical imaginaries may thus refer to jurisdictionally specific constructions of relations between technology and desired national futures. Related research has examined how governments acquire control over visions for the future (Delina, 2018, Levidow and Raman, 2020), and how hierarchies between political elites and publics endure via sociotechnical imaginaries (Smith and Tidwell, 2016, Smallman, 2020).

Imaginaries can become embedded in certain spaces among certain actors (Smith and Tidwell, 2016), and actors may become embedded within imaginaries in turn. The standpoints and interpretive flexibility of those embedded in imaginaries hold consequences for how imaginaries are constructed and/or challenged (Lawless, 2020). This article builds on this observation by focusing on biometric policymaking as a means of challenging the cohesion of sociotechnical imaginaries, and to question assumptions concerning the role of political power in shaping the circulation and distribution of these imaginaries within and across jurisdictions.

The article focuses on biometric policy across the UK, including the devolved administration of Scotland. Biometrics broadly relates here to any form of data about bodily or behavioural characteristics which can be used to identify an individual. Much previous discussion has focused on the criminal justice applications of biometric technology and data (Williams et al, 2004, Lynch et al, 2008), while attention has also focused on uses of biometric identification in areas such as migration, border control, citizenship and welfare entitlement (Amoore, 2013, Donovan, 2015, Marko, 2016).

Recent years have seen significant advances in biometric technology, including DNA and facial recognition, which may be augmented in the near future if harnessed to automation, artificial intelligence or big data systems (OBC, 2018). The advent of genetic methods

claimed to infer appearance and biogeographic ancestry, and the use of commercial genealogical services to pursue suspects (as in the ‘Golden State Killer’ case) has received attention in the literature regarding their potential social and ethical implications (Toom et al, 2016, Syndercombe Court, 2018, M’charek and Wade, 2020). A growing body of social science literature has explored the heterogeneous spaces where this technology is evolving, in which scientific deliberations intermingle with ethical concerns, law enforcement considerations and commercial drivers (Wienroth, 2018, 2020, Samuel and Prainsack, 2018, Granja and Machado, 2020). These studies have explored the social and technical complexity which surrounds these emerging biometric technologies through various conceptual resources, including boundary work (Samuel and Prainsack, 2018, Granja and Machado, 2020), anticipatory space (Wienroth, 2018) and ethical moments (Wienroth, 2020). Related commentaries have addressed concerns over the ways in which technologies such as DNA phenotyping may lead to problematic constructions of race in policing contexts (Skinner, 2020, M’charek and Wade, 2020).

Facial recognition has emerged as another prominent but ethically contentious biometric. Facial matching entails comparing an individual’s image with a database of other images, such as the collection of custody photographs stored on the UK-wide Police National Database. It has been revealed that UK police forces had collected approximately 19 million custody images on the database without seeking legal permission (Big Brother Watch, 2018). Methods involving live or automated facial recognition technology scan the faces of individuals in crowds or public spaces in real time, comparing them with an image database or ‘watchlist’ of persons of police concern. It has been argued that such methods are disproportionate and contravene rights to individual privacy, rights to freedom of expression and rights to assembly or association (Big Brother Watch, 2018, Fussey and Murray, 2019). Further concerns relate to the reliability of facial recognition technology. While estimates of

error rates differ, even the more conservative reports suggest a potentially significantly high rate of false positive matches (Big Brother Watch, 2018, Fussey and Murray, 2019). Certain social groups such as women and black, Asian and minority ethnic individuals are regarded as more likely to be falsely identified, possibly due to bias introduced into algorithms used to compare images (BFEG, 2019).

Much recent social research on biometrics has focused directly on scientists and users apprehensions of technology, highlighting how they negotiate the science-ethics nexus (Wienroth, 2018, 2020, Samuel and Prainsack, 2018, Granja and Machado, 2020), and elsewhere how operational contingencies challenge user engagement (Davies et al, 2018, Fussey and Murray, 2019). Broader issues concerning the governance of emerging biometrics have been addressed at the transnational level (Wienroth, 2018), which alludes to the multivalent challenges facing biometric policymaking. Biometric governance at the national level such in as the UK presents no less significant complexities. McCartney and Amoako (2018) and Amankwaa and McCartney (2019) have drawn attention to the challenges facing relevant national-level agencies such as the Forensic Science Regulator and UK Biometrics Commissioner (McCartney and Amoako, 2018, Amankwaa and McCartney, 2019). These studies have focused on individual commissioners and regulators, but national-level research has not yet considered these agencies in concert despite being framed as key to overseeing the Biometrics Strategy (see below). The entanglement of technical, ethical, legal, commercial and operational issues faced by national-level bodies is significant given the association in the UK of biometrics as a means of cementing law and order and securing national borders (Home Office, 2018). By exploring the issues and pressures associated with biometric policymaking across a range of agencies and spaces, this article provides a more holistic picture of the UK biometric policy landscape.

The social and scientific complexity raised in academic literature contrasts markedly with the 2018 Home Office Biometrics Strategy, which painted a harmonized picture of future technical arrangements for biometric data systems for law enforcement and immigration purposes, with a series of confidently expressed aims and objectives (Home Office, 2018). The Biometrics Strategy does little to challenge technology in terms of the underlying scientific robustness of systems like DNA, fingerprints or facial technology, even though by contrast academic research, legal deliberations and public reports have expressed concern and scepticism over these forms of data at various points in their use. Science and Technology Studies (STS) research has long charted the scientific controversies faced by fingerprint analysis, forensic DNA and facial recognition profiling at various points in their history (see for example Cole, 1998, Lynch et al, 2008, Edmond, 2011). This moreover challenges imaginaries studies which portray the exercise of governmental power as instrumental, immutable and inevitable (Kim, 2014, Delina, 2018, Levidow and Raman, 2020).

Donovan (2015) and Marko's (2016) work on 'biometric imaginaries' contrasts with much sociotechnical imaginaries research in the latter respect. Donovan (2015) introduced the framing of the biometric imaginary to examine how biometric technology becomes constructed "as a necessary, suitable and effective means" of achieving standardized administration (Donovan, 2015: 832). The forms of necessity which emerge in Donovan (2015) and Marko's (2016) studies of the introduction of biometric systems in South Africa and South Sudan respectively, point to how biometric imaginaries entangle individual bodies within technological plans and visions to promote national futures and breaks with the past. These studies also however drew attention to the disjuncture between how biometric imaginaries project discourses of necessary national progress and the actual reality on the ground. In these cases the reconfiguration of governmental apparatus around biometric technology was subverted by questions over the reliability and suitability of this technology

to capture citizen's biometric data, allegations of corrupt tendering by technology providers, and whether investment in biometrics for the granting of citizenship masked notably non-biometric practices (Donovan, 2015, Marko, 2016).

This article critically examines UK biometric policymaking through the imaginaries framing, but in turn seeks to challenge some assumptions which can be discerned in some imaginaries literature concerning the cohesion of governmental power. The article maps the UK oversight landscape via the 2018 Home Office Biometrics Strategy but also encompasses key developments elsewhere, notably the evolution of Scottish legislation. This landscape incorporates a variety of existing and emerging actors, charged with overseeing a varied and growing number of biometric data forms. By sketching this landscape, the article challenges the idea of sociotechnical imaginaries, of which biometric imaginaries are considered a subset, as monolithic and monovalent entities. While various actors and technologies have become embedded within UK imaginaries, the spatial and jurisdictional distribution of biometric policy is complicated by the standpoint of these actors and the varying agency and interpretive flexibility they exercise (Pinch and Bijker 1984).

By attending to this oversight landscape the article addresses the following kinds of questions. What are the implications for embedding actors within imaginaries? How does the distribution of an imaginary, across spaces, actors and jurisdictions, affect its cohesiveness and evolution? How are perceptions and interpretations of an imaginary distributed across the latter's spatial reach, and how do these shape an imaginary in turn? Focusing on such questions leads the article to suggest a need for sociotechnical imaginaries studies to take a more granular view toward politics and policy (Dányi, 2020).

The UK Home Office Biometric Strategy

The Home Office Biometrics Strategy was published in June 2018 after repeated delays (House of Commons, 2019). The Biometrics Strategy focuses mainly on three specific forms of biometrics, namely DNA, fingerprints and facial data, but also anticipates other forms of biometric data such as voice data. The Biometrics Strategy describes the Surveillance Camera Commissioner, UK Biometrics Commissioner, Information Commissioner and the Forensic Science Regulator as “*the four key Commissioners and Regulators who oversee our use of biometrics*” (Home Office, 2018:16-17, emphasis added). The document also frames the Biometrics and Forensics Ethics Group (BFEG) as playing a key future role in the oversight of government use of biometrics (Home Office, 2018: 16). The Biometrics Strategy thus positions these agencies at the centre of the Home Office’s vision for biometric governance. The Biometrics Strategy also acknowledges devolved administrations. In 2020 the Scottish Parliament passed legislation which codifies a Scottish Biometrics Commissioner responsible for overseeing police use of biometrics in that jurisdiction.

The Biometrics Strategy states that the Home Office’s aim is:

to draw on improvements in biometric technologies to protect the public, provide modern services and to increase public trust in the way in which it operates. This requires investments in technology, controlled innovation and a culture and regulatory framework that embeds privacy safeguards within a transparent decision-making process. These need to be combined with clear and independent oversight and consideration of the ethical issues associated with their use. (Home Office, 2018: 6).

The Biometrics Strategy “describes the Home Office’s current approach to using biometrics and how these future developments will be managed.” (ibid). This document projects an imaginary of harmonized governance in which biometric innovation, involving a single technical processing platform bringing together various forms of biometric data, proceeds

alongside a carefully designed system of ethical oversight. Notably, matters of ethics are discursively disentangled from questions of technical reliability and validity, which contrasts with critical social scientific accounts of emerging biometric systems (Samuel and Prainsack, 2018, Wienroth, 2020).

The agencies identified by the Biometrics Strategy currently play various roles in overseeing the evolution and use of this technology and resultant data. While some of these roles involve making decisions over relatively well-established forms of data such as DNA, fingerprints and footprints in the case of the UK Biometrics Commissioner, a great deal of these roles involve anticipating how technology will develop. Within the variegated landscape of UK biometrics, actors are anticipating and imagining the evolution of this technology in general terms, but also have to consider the epistemic dimensions of this advance, together with the potential implications and challenges for operational policing, the law, public attitudes and relations between the public and private sectors.

The imaginaries approach is used primarily here, rather than the sociology of expectations perspective which has been used as another means of conceptualizing technology policy (Borup et al, 2006. Much sociology of expectations literature has tended to focus on specific or singular examples of technological development, and often has had the benefit of historically charting the constructions of technology and expectations over relatively substantial time-frames (see for example Hielscher and Kivimaa, 2019). The imaginaries framing is preferred here as a more immediate means of accounting for the diversity and variety of biometric technology and data, which are regarded as having the potential to evolve rapidly in the near future (OBC, 2018, Scottish Parliament, 2019a).

This article identifies and characterizes approaches to biometric policymaking through the examination of a range of documentary resources. These include academic research reports

and articles, official policy statements such as those published by the Home Office and Scottish Parliament, civil society literature and written submissions and transcripts of oral evidence supplied to parliamentary inquiries. Agencies such as the UK Biometrics Commissioner and Forensic Science Regulator have generated notably high quantities of documentary data in the form of Codes of Conduct and Annual Reports, which have expressed some candid views on biometric issues, as do their responses in Parliamentary hearings. Fieldwork involving participation with representatives of stakeholders at a series of conferences also contributed to the analysis.

The article proceeds by focusing on the oversight bodies identified by the 2018 Biometrics Strategy in turn, before moving on to discuss developments in the devolved administration of Scotland.

Mapping the Governance Landscape of the UK Biometric Imaginary

UK Biometrics Commissioner (UKBC)

The UKBC is mandated to address issues concerning the retention of DNA, fingerprints and shoeprints by police forces on national databases. The National DNA Database (NDNAD) evolved through a series of legislative changes to police powers to sample and retain biological material (Williams et al 2004). Earlier legislative interventions were introduced to pursue the imaginary of capturing the “active criminal population” on the NDNAD (Williams et al, 2004: 54). A highly inclusive regime emerged, which at one point allowed police to permanently retain the DNA of anyone arrested by police, regardless of whether they were subsequently charged or convicted. A ruling in a case heard in 2008 by the European Court of Human Rights concluded however that UK laws violated Article 8 of the European Convention on Human Rights (S & Marper, 2008). The UK Government subsequently

introduced the 2012 Protection of Freedoms Act (PoFA) to attempt to provide a more proportionate regime for the retention of biometric data.

PoFA introduced the office of the UK Biometrics Commissioner. Under PoFA the UKBC considers cases where individuals have been arrested in connection with so-called ‘qualifying’ offences of a serious and violent nature, but not subsequently convicted, and who have no previous convictions (UK Parliament, 2012). Police forces can apply to the UKBC to retain the data of such persons for three years, with a possible two-year extension. The UKBC also makes decisions about whether a person’s data should be retained if the individual is considered a threat to national security. The UKBC publishes Annual Reports which provide relevant data on PoFA (OBC, 2018, 2019a).

Implementing PoFA has not been without its challenges. A number of such issues were identified by Amankwaa and McCartney (2019) via a detailed reading of documents including those published by the UKBC (Amankwaa and McCartney, 2019). These issues included limitations to the Police National Computer system regarding the need for manual data entry to drive the ‘automatic’ deletion of profiles from the NDNAD (which is now allowed by PoFA in certain cases), which has led to some “erroneous retention of biometric data” (Amankwaa and McCartney, 2019: 121). Limited engagement with the PoFA system on the part of police forces was also identified as another challenge, with forces making a markedly small number of applications for retention of biometric data. A series of further issues have included continued uncertainty over the effectiveness of the PoFA regime, concerns about database contamination and error rates, inadequate enforcement of PoFA to the separate counter-terrorism DNA database, and limited statutory guidance for new forms of DNA data such as DNA phenotyping or massive parallel sequencing. These issues have all arisen in official reports, and highlight the complexities apparent when *inter alia* technical

assessments, regulatory scope, legal capacities and policing practices become entangled (Amankwaa and McCartney, 2019).

The annual reports published by the UKBC have gone outside the strict legislative mandate in commenting on other emerging developments concerning biometric technology. The UKBC has regularly commented and expressed concern over facial data even though PoFA does not currently legislate for the role to oversee this data (OBC, 2018, 2019a). More recently the UKBC published an opinion on the track and trace system announced by the UK Government to address COVID-19 (OBC, 2020), suggesting a consideration of the retention period for which individual's personal data would be kept. The UKBC has engaged within academic forums, drawing attention to over-confident claims made by the producers of technology and functional over-reach (ESRC Seminar Series, 2017). In annual reports the UKBC has also expressed concern over the extent to which future biometric systems could be harnessed to artificial intelligence and machine learning, and whether such systems could evade judicial scrutiny (OBC, 2018, 2019).

The UKBC has also given evidence in parliamentary inquiries, including the Scottish Parliament inquiry into the Scottish Biometrics Commissioner legislation (Scottish Parliament 2019a). Most notably still, the UKBC is on record in a UK Commons inquiry as having criticised the 2018 Biometrics Strategy:

I thought that that was disappointing. It was a missed opportunity to lay out a strategy (House of Commons, 2019: 12).

The UKBC's statutory remit is partial in terms of the limited forms of data subject to their purview, and the effectiveness and functioning of PoFA has been challenged by a series of technical and operational issues and legislative lacunae. The UKBC's activities have however extended beyond their statutory role to anticipate future technical, operational and

policy developments. Postholders have been critical of government policy in relation to general biometrics issues.

Forensic Science Regulator

The position of Forensic Science Regulator was instituted by the Home Office in 2007 (McCartney and Amoako, 2018). The Forensic Science Regulator is described on its website as ensuring “that the provision of forensic science services across the criminal justice system is subject to an appropriate regime of scientific quality standards” (UK Government, 2020a). In the course of pursuing this aim the Forensic Science Regulator is responsible for supervising and accrediting forensic laboratories; developing, implementing and maintaining quality standards; and developing validation procedures for new technologies (McCartney and Amoako, 2018). The Forensic Science Regulator has published a Code of Practice and Conduct which has been periodically updated (Forensic Science Regulator, 2020). The Regulator has published numerous documents which have addressed a range of specific matters, including crime scene practice, fingerprints, toxicology, blood stain analysis, pathology and DNA. The Regulator works with a wide variety of professional organizations representing different forensic and related specialisms (McCartney and Amoako, 2018).

Regulation of forensic biometrics entails both addressing present challenges and anticipating those posed by emerging technologies (Fieldwork, 2019). Perceived limitations of biometric technology may impact upon its investigative utility. Some current technical platforms such as those which underpin the NDNAD are relatively well-established, while other data forms are currently regarded as having more limited reliability and are thus treated with greater epistemic caution. Biometric data such as voice, gait, genealogical DNA databases or behavioural biometrics (keystrokes, touch-screen gestures etc) are currently less well-established in these terms. Combining biometrics such as for example forensic DNA

phenotyping with facial recognition is a more speculative possibility, but one which has been anticipated as a further challenge for establishing technical standards. Defining the epistemic risk (i.e. assuming certain or probable knowledge from what may be much less certain sources) of these forms has been seen as key to reining in police expectations (or hopes) of these technologies (Lawless, 2016).

Establishing standards for biometrics is therefore regarded as a key challenge for the Forensic Science Regulator in terms of the sheer variety of technological forms and validation challenges. Assessing the efficacy of biometric data in policing contexts also presents numerous challenges in terms of how data is used and interpreted in the course of law enforcement. CCTV is one notable example of regulatory concern as it can be a high-priority source of data for senior police officers involved in serious crime investigation (Fieldwork, 2019). CCTV poses interpretation issues such as uncertainties about measurements.

Estimating the height of persons captured on camera is problematic. Validating the expertise of human users to make such assessments is a major issue. Losing frames within CCTV footage may impact upon how images are interpreted. Image quality is also regarded as an important limiting factor for the effectiveness of facial recognition algorithms.

The Regulator's scope is however limited to forensic providers across England and Wales, although forensic services in Scotland and Northern Ireland voluntarily comply. Concerns have been raised over the alleged lag in compliance with quality standards on the part of some police forces (McCartney and Amoako, 2018). The Regulator currently has limited agency to address non-compliance. A proposed Forensic Science Regulator and Biometric Strategy Bill would grant statutory powers, including the ability to investigate possible breaches with a statutory code of practice and to serve compliance notices (House of Commons, 2020). The current lack of statutory powers for the Regulator, and the alleged

inactivity on the part of Government to bestow them, has been identified as a matter of concern in Parliamentary Inquiries (House of Commons, 2019, House of Lords, 2019).

The Forensic Science Regulator does not conduct economic regulation of the forensic marketplace. The Regulator has however repeatedly drawn attention to the increasing economic vulnerabilities of the forensic marketplace, and associated risks, in Annual Reports. The Regulator has described companies entering administration or ceasing operations entirely, risking the availability of judicial evidence (Forensic Science Regulator, 2018, 2019). The Regulator has also warned of the lack of skilled recruits to the forensic science sector, and the alleged decline in capacity and quality of research and development (House of Commons, 2013, Forensic Science Regulator, 2018).

The Regulator's role addresses a wide and growing variety of methods and data forms and encompasses a notable degree of horizon-scanning activity. Their regulatory remit is however partial, limited to providers in England and Wales, notwithstanding voluntary compliance elsewhere. Moves to establish a statutory basis for the role have been slow in coming, and at time of writing are still not in place. The Regulator does not possess a strictly economic role but has nonetheless warned of threats to the forensic marketplace with increasing urgency (House of Commons, 2018, 2019).

Information Commissioner (ICO)

The role of Information Commissioner has its roots in the 1998 Data Protection Act, which was later replaced by the General Data Protection Regulations and the 2018 Data Protection Act (ICO, 2020). The Information Commissioner's Office (ICO) website describes itself as the "UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals" (ICO, 2020).

According to the 2018 Biometrics Strategy the ICO issues “guidance, advice and can carry out enforcement action” (Home Office, 2018: 17) where data protection laws have been breached. In written evidence to the Commons Science and Technology Select Committee, the ICO stated that biometric data “is afforded an additional level of protection”, through Part 3 of the 2018 Data Protection Act, which applies to the processing of personal data “in the context of law enforcement” (ICO, 2019a).

The ICO has submitted and published statements concerning facial data. In the same written submission to the 2019 Commons Inquiry, the ICO expressed concern over the ongoing retention of custody images of individuals not subsequently convicted of an offence (ICO, 2019a). The 2017 Custody Image Review led to such individuals being allowed to request deletion of these images. The ICO stated that “it is unclear how those individuals would know that they could make a request and we are aware that there have not been a significant number of requests, indicating a lack of awareness.” (ICO, 2019a). Retention of such images, the ICO claimed, had ‘no clear basis in law’ (ibid). The failure to implement an automated deletion system was viewed as breaching the 2018 Data Protection Act (House of Commons, 2019).

The Information Commissioner issued an opinion on the use of live facial recognition by law enforcement in October 2019. This opinion claimed that data protection law “applies to the whole process...from consideration about the necessity and proportionality for deployment, the compilation of watchlists, the processing of the biometric data through to the retention and deletion of that data”, whether “for a trial or routine operational deployment” (ICO, 2019b: 2). The Information Commissioner further opined that the use of such technology constitutes “sensitive processing” under the terms of the 2018 Data Protection Act “as it involves the processing of biometric data for the purpose of uniquely identifying an individual”, and that this category applies to all facial images captured and analysed by

software (ibid). The Commissioner expressed a view to work toward a binding code of practice, possibly building upon that of the Surveillance Camera Code (see below), but with “a clear and specific focus on law enforcement use of [live facial recognition] and other biometric technology”, applicable to both current and future technology (ibid). Without such a code, the Commissioner opined that “we are likely to continue to see inconsistency across police forces and other law enforcement organisations in terms of necessity and proportionality determinations relating to the processing of personal data” (ibid: 10).

The ICO has statutory powers and an enforcement capacity and has played a key role in defining the legal status of biometric systems. While the ICO has drawn attention to issues relating to the retention of facial data, this has been in a responsive mode and it remains to be seen precisely how the ICO might go about addressing possible data protection breaches regarding biometric data use by law enforcement. The ICO’s opinion on facial recognition has not stopped it being deployed in England and Wales, notwithstanding subsequently successful legal challenges (Bridges, 2020)

Surveillance Camera Commissioner (SCC)

According to the Home Office Biometric Strategy, the Surveillance Camera Commissioner’s role is “to encourage compliance with the Surveillance Camera Code of Practice” (Home Office, 2018: 17). The SCC was created under PoFA, as was the requirement for the Code of Practice. According to the Code:

The commissioner should provide advice and information to the public and system operators about the effective, appropriate, proportionate and transparent use of surveillance camera systems and should consider how best to make that information available. Such advice should complement the content of this code, and may for

example provide additional detail on good practice...or on the proportionate application of any new technological developments in surveillance camera systems. (SCC, 2019: 2).

The SCC published a guidance document on police use of automated facial recognition systems with surveillance cameras in March 2019. In this document the SCC “*does not give legal advice* and nothing within this document should be construed or otherwise interpreted as amounting to such.” (SCC, 2019: 3, emphasis added). This document relates itself to existing legal frameworks (SCC, 2019: 4), mentioning PoFA, the 2000 Regulation of Investigatory Powers Act, the 1998 Human Rights Act and the 2018 Data Protection Act. In this document the SCC stated that “any use of facial recognition or other biometric characteristic recognition systems needs to be clearly justified and proportionate in meeting the stated purpose and be suitably validated” (SCC, 2019: 6). The SCC delegates this validation to the Forensic Science Regulator’s Codes of Practice and Conduct. With regard to ethical guidance, the SCC also delegates to a notable extent to the Biometrics and Forensics Ethics Group (BFEG) (SCC, 2019: 12).

The SCC has “no powers of inspection, audit or compliance and his role is simply advisory.” (SCC 2019: 3). The SCC instead works with “relevant authorities” (defined by PoFA as including Chief Officers of Police and Police and Crime Commissioners) to have regard to the code. The SCC is also limited to encouraging voluntary adoption of the code by other operators of surveillance camera systems. The SCC has however issued opinions on issues such as the Appeal to the *Bridges* case (SCC, 2020). The civil rights groups Liberty supported the case *R v Bridges*, which challenged the use of facial recognition technology by South Wales Police. The High Court in Cardiff rejected Bridges’ claim that the technology was unlawfully used against him, but a subsequent hearing in the Appeal Court ruled in favour of Bridges. The SCC welcomed the Appeal Court’s acknowledgement of his role, but

was also sharply critical of the Home Office who he accused of failing to update the relevant Code of Practice, and viewing them and the Home Secretary as having been ‘asleep on watch’ (SCC, 2020).

Biometrics and Forensic Ethics Group (BFEG)

The Biometrics and Forensics Ethics Group was first established as the DNA Database Ethics Group in 2007. Sponsored by the Home Office, BFEG is described on its website as providing ‘independent ethical advice to Home Office ministers on issues related to the use of biometrics and forensics.’ (UK Government, 2020b). Its remit is described as including:

“consideration of the ethical impact on society, groups and individuals of the capture, retention and use of human samples and biometric identifiers for purposes which fall within the purview of the Home Office, including the differentiation between, or identification of, individuals” (ibid).

This remit reflects the expansion in July 2017 of the group beyond the NDNAD to address a wide range of biometric technology, both current and potential. The minutes of quarterly BFEG meetings reflect this expansion in scope and a future-scanning function, including consideration of new data forms relating to DNA phenotyping and other emerging exploitations of DNA such Y-STR testing and genealogical analysis (see for example BFEG, 2018b). In June 2018 BFEG published a set of broad ethical principles (BFEG, 2018a). In February 2019 some BFEG members published ethical guidelines specifically for the use of automated facial recognition in law enforcement (BFEG Facial Recognition Working Group, 2019). BFEG membership contains a high proportion of academics and legal professionals (UK Government, 2020c).

The 2018 Home Office Biometrics Strategy refers to BFEG as a source of “governance” for certain forms of data, namely fingerprints, DNA and facial analysis (Home Office, 2018: 16). BFEG currently however has no statutory powers, and no new legislation was proposed in the Biometrics Strategy to re-shape BFEG from an advisory body. While BFEG members have issued ethical guidelines for the use of facial recognition, it is unclear to what extent forces such as the Metropolitan Police or South Wales Police have transparently followed such principles (Fussey and Murray 2018; Davies et al 2018, Big Brother Watch 2018).

A Devolved Imaginary? The 2020 Scottish Biometrics Commissioner Act

Biometric data in Scotland is subject to a separate legal system. In 2016 Her Majesty’s Inspectorate of the Constabulary Scotland (HMICS) “identified a need for improved legislation and better independent oversight around the police use of biometrics in Scotland” (HMICS, 2016: 8). The HMICS proposed a Scottish Biometrics Commissioner (SBC) be established to independently oversee biometric databases and records held in Scotland, and to anticipate future technological developments (HMICS, 2016). The Scottish Government convened an Independent Advisory Group (IAG), including representatives from the legal system, policy and academia, to consider the use and retention of biometric data in general, and to establish an “ethical and human rights based framework” which could be applied to “existing, emerging and future biometrics” (Scottish Government, 2018: 4). The IAG reported in March 2018 and made nine recommendations including the establishment of a Scottish Biometrics Commissioner and a Code of Practice to govern police use of biometrics. This was viewed by the IAG as a means of responding reflexively to the potentially fast-moving development of biometric technology without having to constantly legislate for these developments (Scottish Government, 2018: 10).

The Scottish Biometrics Commissioner (SBC) Act was passed by the Scottish Parliament in March 2020 with 110 votes in favour and none against. The Act compels police to comply with a Code of Practice produced by the SBC. When drafting the Code, the latter is legally obliged to consult with a series of representatives of Scottish government, law and policing, as well as the Information Commissioner, Scottish Human Rights Commission, and the Commissioner for Children and Young People in Scotland (Scottish Parliament 2020b: Subsection 10(1)). At least for the time being, the Code applies only to police agencies, and does not extend in scope to other users of biometric systems such as local authorities, private actors, or the Scottish Prison Service, where the private provision of biometric systems was made evident during an earlier Parliamentary inquiry into the legislation (Scottish Parliament, 2019a). During this inquiry some interlocutors argued for a more all-encompassing privacy commissioner rather than the SBC (Scottish Parliament, 2019c). The place of private sector producers, recognised as a key source of biometric innovation during Committee hearings (Scottish Parliament, 2019b), is less clear in the legislation. The Act enables the SBC to consult with “such other persons” they consider “appropriate” in the formation of the Code (Scottish Parliament 2020b: 10(1)). This would allow but not compel the SBC to engage with the private sector, and the latter are not directly obligated to comply with the Code. Police, if they were to contract out biometrics provision, may be ultimately responsible for compliance. In addition, the issue was raised over the collection of biometric data by UK-wide bodies such as the British Transport Police. The UKBC raised the issue of whether the latter body would follow Scottish legislation when operating in Scotland regarding collecting biological material from arrestees, even though that material would be sent to England (Scottish Parliament 2019a: 11).

During the Scottish Parliamentary inquiry process it was debated whether the IAG’s own draft Code could form the basis of one put directly into legislation and which could be

scrutinized by Parliament. Other views claimed that this would prevent the Act from being sufficiently responsive and flexible to rapidly evolving technological developments, if constant changes to the Code had to be amended through Parliamentary procedure (Scottish Parliament 2019a: 30-32, 2019d). This latter view largely prevailed, although some key considerations for preparing the Code are included in the Act (Scottish Parliament, 2020b: Section 8). The legislation is however less clear on mechanisms for reviewing the Code. The Act does not provide for any formal procedure, other than that the Code be revised “from time to time” (Scottish Parliament, 2020b: Subsection 7(1)). An advisory group was made a statutory requirement. At time of writing, details of the precise role and selection criteria for this group have yet to be made public, although the Scottish Justice Secretary expressed a strong preference for a diverse group, rather than populating it with academics, which he contrasted with the composition of BFEG (Scottish Parliament 2019d: 17).

In earlier deliberations prior to the final draft legislation, the SBC role was envisaged as “identifying systemic deficiencies” (quoted in Scottish Parliament, 2019d: 18), but the final Act provides for a formal complaints procedure regarding police (mis)use of biometrics. Public engagement matters have seldom featured in UK governmental discourses (Scottish Parliament, 2019b), although it is stated as a responsibility for the SBC. The precise nature of such public engagement activity, while discussed in Scottish Parliamentary settings, remains to be seen (Scottish Parliament, 2020a).

An emergent Scottish biometric imaginary can nonetheless be discerned involving anticipatory legislation led more by *a priori* principles rather than technological developments. This contrasts with the rest of the UK, which has largely justified biometric policymaking in retroactive terms, referring to existing pieces of legislation (House of Commons, 2019, SCC, 2019). In adopting a broad definition of biometrics, this Scottish imaginary appears to make far less assumptions about how technology will develop – just

that it will. The kind of negotiated expectations related to the Scottish imaginary have been less directly technology-focused, but more closely concerned with the effectiveness of the SBC role and the attendant framework including the Code of Practice. The SBC Act is however notably police-focused, and it remains to be seen how far the SBC could go to engage with other stakeholders, such as private authorities employing surveillance cameras, private providers of biometrics, or the Scottish Prison Service. This may reflect a potential issue with adopting such a broad definition of biometrics as it may create difficulties anticipating exactly what kind of coalitions certain technologies might emerge within, and thus namely with whom the SBC should consult.

Discussion

This article began by taking the 2018 Home Office Biometrics Strategy as a starting point to examine biometric policymaking across the UK. That document adopts an assured tone concerning future plans for the oversight and use of biometrics in law enforcement and other functions. This article has contrasted that harmonized rendering of biometric policymaking with the distributed complexity of agencies cited by that document as playing key roles in biometric oversight, and the array of technical, legal, legislative and operational challenges they face, together with a consideration of interventions they have made. The article also examined developments in the devolved administration of Scotland, in which a separate and distinct imaginary is emerging in the form of the Scottish Biometrics Commissioner. Scotland may be joined by other devolved imaginaries in the near future. In July 2020 the Northern Ireland Justice Minister announced a consultation for its own Biometrics Commissioner (Northern Ireland Executive, 2020).

In contrast with imaginaries studies which portray national governments as harnessing resources in a cohesive and instrumental way to project futures, this article has peeled away that image to reveal the oversight landscape of UK biometric policy as marked by lacunae between codified roles and agency, together with varying distributions of power. Rather than resting within a monolithic governmental structure, UK biometric policy is located within a patchwork of oversight (which in some ways has emerged reactively) in which diverging biometric imaginaries can be discerned. Scotland is pursuing a distinct approach involving anticipatory legislation, in contrast with the UK government which has often justified its policies in relation to a series of existing pieces of legislation (with the possible and only partial exception of the proposed Forensic Science Regulator and Biometrics Strategy Bill).

The 2018 Biometrics Strategy embeds a number of commissioners, regulators and advisors into a biometric imaginary. This document however does not reflect the significant degree of interpretive flexibility arising from these actor's standpoints, relating to how they view their respective role and agencies, and how they perceive challenges to biometric policy and implementation. These standpoints are reflected in various interventions made by them. Some of these have cautioned against the status of biometric technologies, drawing attention to the challenges of standardizing and validating new biometric systems and of applying them in law enforcement and juridical contexts. Other statements by incumbents have challenged biometric policy in wider terms and have even questioned the status of their own role.

The Forensic Science Regulator has for example repeatedly called for statutory powers in Parliamentary inquiries and expressed concern over the state of the forensic marketplace. The current UKBC has commented on his purview being limited to DNA, fingerprints and footprints, commented on the UK government's COVID-19 track and trace system, has given evidence on the Scottish Biometrics Commissioner role and has strongly criticised the Biometrics Strategy. The ICO has been critical of policies regarding custody image retention

and the legality of these policies. The SCC published a statement responding to the *Bridges* Appeal verdict which welcomed the acknowledgement of their role, but which was also critical of the Home Office (SCC, 2020). While embedded in a UK Government imaginary, these actors are positioned in such a way to problematize biometric policy (which itself has been partially responsively shaped via external contingencies such as the S & Marper case for example), to align with external challenges such as court rulings, and to criticise government in parliamentary inquiries. The standpoints of these actors are also shaped by the issues they face in the course of their roles. These include the challenges of implementing PoFA faced by the UKBC and expressed future concerns about the impact of technology on legal scrutiny of biometrics, the legal issues identified by the ICO, and the operational and validation challenges to current and emerging biometrics identified by the Forensic Science Regulator, together with the technical, operational and ethical issues raised by BFEG and the SCC. The anticipation of these challenges by these actors serve to problematize the dominant imaginary in which they are embedded, and they suggest ways in which this imaginary could be re-shaped by future operational issues or legal challenges.

While recent Scottish legislation appears to be more future-oriented, the Scottish Biometrics Commissioner Act leaves a series of issues currently open including: how the Code of Practice will evolve (including what kind of scope will develop to address technical standards alongside interrelated ethical issues and police practices) and through what process it will be revised; precisely who the postholders will consult with other than Scottish police representatives; and how postholders will work with UK commissioners and regulators. A certain room for manoeuvre exists within the Scottish Biometrics Commissioner Act and with it the potential for individual agency to shape this devolved imaginary.

Civil society should also be acknowledged as challenging imaginaries. For some time, various non-governmental organizations have questioned the use and deployment of

biometric data in law enforcement. For example the group Genewatch UK has addressed ethical concerns over the spread of DNA databases in the UK and internationally (Genewatch, 2020). Facial recognition technology has been challenged by groups such as Big Brother Watch, who have published reports and surveys critical of the use of facial recognition by police forces (Big Brother Watch, 2018, Ada Lovelace Institute, 2019). On numerous occasions these groups have been able to engage with oversight actors (Fieldwork, 2019, Scottish Parliament, 2019b, 2020a).

One should not overestimate the capacity of political elites such as leaders and ministers to promote visions of biometric policymaking. The UK Government has been constrained by decisions from the European Court of Human Rights which have helped shaped the current governance landscape by leading to the introduction of the UKBC. A more recent European ruling in the *Gaughran* case has further challenged UK law concerning the permanent retention of biometric data from convicted persons (Gaughran v United Kingdom, 2020). The recent outcome of the *Bridges* appeal case indicates how UK courts can themselves intervene (the role of law courts in shaping imaginaries has largely been overlooked, even though the impact of court cases has been well-covered in other strands of STS research).

This article has also indicated how devolution dilutes the power of UK Government to push through sociotechnical visions across the whole of the country. Yet even the devolved Scottish Government, currently a minority administration, was dependent on cross-party support to pass the Scottish Biometrics Commissioner Act, following a consultation process which brought the Scottish Government and Parliament into contact with a variety of stakeholders who contributed to shaping this legislation. This all highlights how imaginaries researchers need to further problematize the agency of national governments, and to not underplay complexities and contingencies within and across polities. Only recently has STS

begun to explicitly recognise the need to address political processes and policymaking with the same granularity it has accorded to science (Dányi, 2020).

This article has found that governmental biometric imaginaries embed actors who differentially experience them from various standpoints, and who have capacity to identify and raise issues of significant detail. In being tasked with overseeing imaginaries, these actors deal with the interpretive work of deciding whether biometric data is being retained appropriately and ethically, whether codes are being followed or if technology is being used lawfully. They also anticipate future problems concerning ethical decision-making, complex technical and operational standard-setting, and who they should consult with in the course of fulfilling their roles. Oversight actors can be regarded as possible obligatory passage points (Callon, 1986) who mediate between governmental imaginaries and wider milieux encompassing scientists, researchers, police, lawyers, technology producers, and publics, enmeshed with technology and data, who may feed back and challenge these imaginaries, possibly through statements made by these oversight actors. These oversight actors function as conduits, located at key interstices of governmental imaginaries, through which a host of perspectives, possibilities and problems are channelled. In Scotland, the 2020 SBC Act could be said to partially formalize such a relation through the requirement for the SBC to consult with certain figures in the drafting of their Code of Practice (Scottish Parliament 2020b: Subsection 10(1)). This article thus advocates that understanding the (re)configuration of state structures through biometric technology (Donovan, 2015) requires us to pay more detailed attention to these figures as part of the recent turn in STS toward more sustained examination of politics and policymaking (Dányi, 2020).

The article however acknowledges a tension between the standpoint of these actors embedded within UK biometric policymaking and the imposition of agency based on the presence or absence of, for example, statutory powers and resourcing (many of these bodies involve part-

time roles with limited personnel support). A countering question is whether the delegation of roles among UK bodies, with the differential and possibly selective distribution of (non)statutory powers, responsibilities and resources, contributes to scientific and ethical complexities being filtered out of policymaking (Smallman, 2020). Or does the problematic detail, identified by oversight bodies and conveyed through public statements and stakeholder gatherings, feed back into channels such as parliamentary inquiries or legal challenges in a meaningful way? A further question is whether such feedback may extend to influencing policy and legislation in other jurisdictional spaces, such as Scotland for example. The emergence of the Scottish Biometrics Commissioner provides a future opportunity to compare how the distribution or centralization of powers in numerous roles or one role shape whether (and how) biometric imaginaries are rendered more or less complex or problematic – and how and to whom that complexity is communicated. Might devolved administrations be able to better apprehend and address the complexities of biometric policymaking? Do we need to pay attention to possible variance among governmental imaginaries in terms of how they may more or less problematize technology, how that subsequently shapes the evolution of biometric governance, and the implications for perceptions of ‘good’ biometric governance? If so, this article has indicated a path of future research to help flesh out further the concept of the biometric imaginary, and to contribute more broadly to sociotechnical imaginaries studies.

Conflict of Interest

On behalf of all authors, the corresponding author states that there is no conflict of interest.

Bibliography

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

Amankwaa, A.O. and McCartney, C. (2019) The UK National DNA Database: Implementation of the Protection of Freedoms Act 2012. *Forensic Science International* 284: 117-128.

Amoore, L. (2013) *The Politics of Possibility: Risk and Security Beyond Probability*. Durham, NC: Duke University Press.

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

Biometrics Commissioner (2018) Biometrics Commissioner's response to the Home Office Biometrics Strategy, 28 June 2018. <https://www.gov.uk/government/news/biometrics-commissioners-response-to-the-home-office-biometrics-strategy>, accessed 19 December 2019.

Biometrics and Forensics Ethics Group (2018a) *Ethical Principles* April 2018. London: Home Office.

Biometrics and Forensics Ethics Group (2018b) Note of the 6th meeting held on 3rd December 2018 at Home Office, 2 Marsham Street, Westminster, London, SW1P 4DF. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/837704/BFEG_minutes_-_03_December_2018.pdf, accessed 3 October 2020.

Biometrics and Forensics Ethics Group Facial Recognition Working Group (2019) Ethical Issues Arising From The Police Use of Live Facial Recognition Technology. London: Home Office.

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

Bridges, R (on application of) v. Chief Constable of South Wales Police [2020] EWHC 2341 (Admin). Accessed 3 October 2020.

Callon, M. (1986) Elements of a sociology of translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. In: J. Law (ed.) *Power, Action and Belief: A New Sociology of Knowledge?* London: Routledge, pp.196-233.

Cole, S.A. (1998) Witnessing identification: Latent fingerprint evidence and expert knowledge. *Social Studies of Science* 28(5-6): 687-712.

Dànyi, E. (2020) The insides and outsides of parliamentary politics: Introduction to a special issue of *Social Studies of Science* on parliamentary practices. *Social Studies of Science*. 50(2): 245-251.

Davies, B., Innes, M. & Dawson, A. (2018) An Evaluation of South Wales Police's Use of Automated Facial Recognition. Universities' Police Science Institute & Crime & Security Research Institute, University of Cardiff. September 2018.

Delina, L.L. (2018) Whose and what futures? Navigating the contested coproduction 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(4): 815-833.

Edmond, G. (2011) The building blocks of forensic science and law: Recent work on DNA profiling (and photo comparison). *Social Studies of Science* 41(1): 127-152.

ESRC Seminar Series (2017) Securitization and forensic genetics. Northumbria University 24 March 2017. <https://www.ncl.ac.uk/peals/research/forensicgenetics/#seminar5>, accessed 3 October 2020.

Forensic Science Regulator (2018) Annual Report November 2016-November 2017.

Birmingham: Forensic Science Regulator.

Forensic Science Regulator (2019) Annual Report 17 November 2017-16 November 2018.

Birmingham: Forensic Science Regulator.

Forensic Science Regulator (2020) Codes of practice and conduct for forensic science providers and practitioners in the criminal justice system issue 5. Birmingham: Forensic Science Regulator.

Fussey, P. and Murray, D. (2019) Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. Human Rights Centre, University of Essex. July 2019.

Gaughran v United Kingdom (2020) European Court of Human Rights 13 February 2020 ECHR 45245/15.

Genewatch (2020) Forensic Genetics Policy Initiative. <http://www.genewatch.org/sub-572921>, accessed 5 October 2020.

Granja, R. and Machado, H. (2020) Forensic DNA phenotyping and its politics of legitimization and contestation: Views of forensic geneticists in Europe, *Social Studies of Science* advance online publication, July 30, 2020,

<https://doi.org/10.1177/0306312720945033>

Her Majesty's Inspectorate of the Constabulary in Scotland (HMICS) (2016) Audit and Assurance Review of the use of the Facial Search functionality within the UK Police National Database (PND) by Police Scotland. Edinburgh: HMICS.

Hielscher, S. and Kivimaa, P. (2019) Governance through expectations: Examining the long-term policy relevance of smart meters in the United Kingdom. *Futures* 109: 153-169.

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

House of Commons (2020) Forensic Science Regulator and Biometrics Strategy Bill. London: House of Commons.

House of Commons Science and Technology Select Committee (2005) Forensic Science on Trial: Seventh Report of Session 2004-5. London: Her Majesty's Stationery Office.

House of Commons Science and Technology Select Committee (2011) The Forensic Science Service: Seventh Report of Session 2010-12. London: Her Majesty's Stationery Office.

House of Commons Science and Technology Select Committee (2013) Forensic Science: Second Report of Session 2013-14. London: Her Majesty's Stationery Office.

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 Lords Science and Technology Committee (2019) *Forensic Science and the Criminal Justice System: A Blueprint*. London: House of Lords, 3rd Report of Session 2017-19, London: Her Majesty's Stationery Office.

Information Commissioner's Office (2019a) *Written evidence submitted by Steve Wood, Deputy Commissioner for Policy. Written evidence to House of Commons Select Committee Inquiry The Work of the Biometrics Commissioner and The Forensic Science Regulator March 2019 (WBC0008)*.

Information Commissioner's Office (2019b) *Information Commissioner's opinion: The use of live facial recognition technology by law enforcement in public places*. 31 October 2019.

Information Commissioner's Office (2020) *ICO Homepage*. <https://ico.org.uk>, accessed 3 October 2020.

Jasanoff, S. and Kim, S-H. (2009) *Containing the atom: Sociotechnical imaginaries and nuclear regulation in the US and South Korea*. *Minerva* 47(2): 119-146.

Kim, S-H. (2014) *The politics of human embryonic stem cell research in South Korea: Contesting national sociotechnical imaginaries*. *Science as Culture* 23(3): 293-319.

Lawless, C.J. (2016) *Forensic Science: A Sociological Introduction*. London, New York: Routledge.

Lawless, C.J. (2020) *Assembling airspace: The Single European Sky and contested transnationalities of European air traffic management*. *Social Studies of Science* 50(4): 680-704.

Levidow, L. and Raman, S. (2020) Sociotechnical imaginaries of low-carbon waste-energy futures: UK techno-market fixes displacing public accountability. *Social Studies of Science* 50(4): 609-641.

Lynch, M., Cole, S.A., McNally, R. and Jordan, K. (2008) *Truth Machine: The Contentious History of DNA Fingerprinting*. Chicago: Chicago University Press.

McCartney, C. and Amoako, E.N. (2018) The UK forensic science regulator: A model for forensic science regulation? *Georgia State University Law Review* 34(4): 945-981.

Markó, F.D. (2016) “We are not a failed State, we make the best passports”: South Sudan and biometric modernity. *African Studies Review* 59(2): 113-132.

M’charek, A. & Wade, P. (2020) Doing the individual and the collective in forensic genetics: Governance, race and restitution. *BioSocieties*. 15(3): 317-328.

Northern Ireland Executive Department of Justice (2020) Long announces consultation on biometric proposals. <https://www.justice-ni.gov.uk/news/long-announces-consultation-biometric-proposals> Published 3 July 2020

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

Office of the Biometrics Commissioner (OBC) (2019a) *Commissioner for the Retention and Use of Biometric Material: Annual Report 2018*. London: Her Majesty’s Stationery Office.

Office of the Biometrics Commissioner (OBC) (2020) *Biometrics Commissioner statement on the use of symptom tracking applications 21 April 2020*. <https://www.gov.uk/government/news/biometrics-commissioner-statement-on-the-use-of-symptom-tracking-applications>. Accessed 3 October 2020.

Pinch, T.J. and Bijker, W.E. (1984) The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science* 14(3): 399-441.

S & Marper v United Kingdom (2008) European Court of Human Rights, 4 December ECHR 1581.

Samuel, G. and Prainsack, B. (2018) Forensic DNA phenotyping in Europe: Views “on the ground” from those who have a professional stake in the technology. *New Genetics & Society* 38(2): 119-141.

Scottish Government (2018) Independent Advisory Group on the Use of Biometric Data in Scotland. Edinburgh: Scottish Government.

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

Scottish Parliament (2019b) Justice Committee Official Report 24 September 2019.

Scottish Parliament (2019c) Justice Committee Official Report 1 October 2019.

Scottish Parliament (2019d) Justice Committee Official Report 12 November 2019.

Scottish Parliament (2020a) Justice Sub-committee on policing. Facial recognition: How policing in Scotland makes use of this technology. Edinburgh: Scottish Parliament.

Scottish Parliament (2020b) Scottish Biometrics Commissioner Act.

Skinner, D. (2020) Forensic genetics and the prediction of race: What is the problem? *BioSocieties* 15(3): 329-349.

Smallman, M. (2020) 'Nothing to do with the science': How an elite sociotechnical imaginary cements policy resistance to public perspectives on science and technology through the machinery of government. *Social Studies of Science* 50(4): 589-608.

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(6): 327-350.

Surveillance Camera Commissioner (2019) *The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems*. London: Her Majesty's Stationery Office.

Surveillance Camera Commissioner (2020) *Surveillance Camera Commissioner's Statement: Court of Appeal Judgment (R) Bridges v South Wales Police – Automated Facial Recognition*, 11 August 2020.

<https://www.gov.uk/government/speeches/surveillance-camera-commissioners-statement-court-of-appeal-judgment-r-bridges-v-south-wales-police-automated-facial-recognition>, accessed 25 September 2020.

Syndercombe Court, D. (2018) Forensic genealogy: Some serious concerns. *Forensic Science International: Genetics*. 36: 203-204.

Toom, V., Wienroth, M., M'Charek, A., Prainsack, B., Williams, R., Duster, T., Heinemann, T., Kruse, C., Machado, H and Murphy, E. (2016) Approaching ethical, legal and social issues of emerging forensic DNA phenotyping (FDP) technologies comprehensively: Reply to 'Forensic DNA phenotyping: Predicting human appearance from crime scene material for investigative purposes' by Manfred Kayser', *Forensic Science International: Genetics*. 22: E1-E4.

UK Government (2020a) Forensic Science Regulator.

<https://www.gov.uk/government/organisations/forensic-science-regulator>, accessed 3 October 2020.

UK Government (2020b) Biometrics and Forensics Ethics Group.

<https://www.gov.uk/government/organisations/biometrics-and-forensics-ethics-group>, accessed 3 October 2020.

UK Government (2020c) Biometrics and Forensics Ethics Group: Membership

<https://www.gov.uk/government/organisations/biometrics-and-forensics-ethics-group/about/membership>, accessed 3 October 2020.

UK Parliament (2012) The Protection of Freedoms Act. UK Parliament Website.

<https://services.parliament.uk/bills/2010-11/protectionoffreedoms.html>, accessed 19 December 2019.

Wienroth, M. (2018) Governing anticipatory technology practices. Forensic DNA phenotyping and the forensic genetics community in Europe. *New Genetics & Society*. 37(2): 137-152.

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(1): 28-45.

Williams, R. Johnson, P. and Martin, P. (2004) Genetic Information and Crime Investigation. Social, Ethical and Public Policy Aspects of the Establishment, Expansion and Police Use of the National DNA Database. Durham: Durham University, School of Applied Social Sciences.

