Section A The fields in this section are mandatory.

Institution: Durham University

Unit of Assessment: 14 Geography and Environmental Sciences

Title of case study: Biometric data in the age of algorithms

Period when the underpinning research was undertaken: Between 2006 and 2020

Details of staff conducting the underpinning research from the submitting unit:

Name(s):	Role(s) (e.g. job title):	Period(s) employed by submitting HEI:
Professor Louise Amoore	Professor of Human Geography	September 2005 to present
Dr Volha Piotukh	Postdoctoral Research Associate	January 2013 to December 2015

Period when the claimed impact occurred: Between September 2014 and December 2020

Is this case study continued from a case study submitted in 2014? N

Section B

1. Summary of the impact

From biometric data captured in borders and immigration systems, to the police deployment of facial recognition technologies in UK cities, the use of algorithms in the processing of biometric data has become central to contemporary security. Durham University research has advised and held to account UK public authorities in their formulation and implementation of algorithmic biometric technologies. As a direct result of Amoore's research-based evidence on the ethical implications of algorithms for a UK government review and a parliamentary select committee, she serves on the only ethics committee within the UK Home Office, the Biometrics and Forensics Ethics Group (BFEG). The BFEG is responsible for the scrutiny and oversight of biometrics and data analytics technologies. Through the BFEG, Amoore's research has directly shaped accountability regarding the ethical considerations of the use of algorithmic biometric technologies in public spaces.

2. Underpinning research

Durham University research has pioneered the understanding of how biometric data are transformed through algorithmic techniques. Biometric data are a special category of personal data related to a person's physical or behavioural characteristics, and merit special treatment under current data protection law. Novel forms of algorithmic processing and analysis have important social and political consequences because of how they assemble and use those data in new ways. Public accountability and scrutiny of algorithmic biometrics is, however, constrained by the complexity of computer models used to analyse the data. Existing societal mechanisms – data protection, privacy, transparency – are not sufficient because they have not kept pace with this technological transformation. Research led by Amoore has identified the novel forms of algorithmic analysis of biometric data that are deployed for security, policing, and border control, and has advanced a unique body of knowledge of the implications of this analysis for public accountability and oversight.

The research has defined the state-of-the-art knowledge of how biometric data have been transformed through machine learning algorithms, cloud data storage, and digital analytics. Amoore's approach has been underpinned by a novel conceptualisation of algorithms as iteratively constituted through their relations with the world (reference **R1**). Coupled with pioneering methods for 'following the algorithm' as part of an iterative socio-technical system (**R1**), this conceptualisation allows for an extension of what can count as an algorithmic decision system, and necessitates close, sustained engagement with governments, borders and policing authorities, algorithm designers, commercial software organisations, and NGOs (**R1**, **R2**, **R4**).

Through this longstanding engagement, the research has generated substantive empirical evidence of the processes of algorithmic biometrics, extending from the design and training of algorithmic models to their deployment by frontline authorities (**R1**, **R4**). Evidence has included how algorithmic biometrics are deployed in a range of pre-emptive security interventions (**R2**, **R6**). The research also anticipated and tracked how new forms of biometric analysis, such as facial recognition and gait recognition, were beginning to be used in the securing of public space (**R1**). 'Data derivatives' produced from aggregated data become decoupled from the individual subject and attached instead to a profile of attributes (**R5**). The research analysed why and how biometric

data are thus rendered linkable to other forms of behavioural data (**R3**). In this way, associations are generated across data elements, inferences are drawn about the probability of specific behaviours, and security interventions are justified and deployed (**R1**, **R3**).

Amoore's research has explored the ethical implications of this transformative shift from biometrics as 'one-to-one' identifiers of individuals to biometrics as data elements in a broader 'big data' world (**R1**, **R4**). The research has specified the issues for public accountability and oversight of the algorithmic analysis of biometric data, focusing on: automation and algorithmic decisions; the processing and analysis of multi-modal data that combine biometrics and behaviour; and the limits of privacy and data protection as regulatory and juridical principles (**R1**). Existing legislative and regulatory approaches are undercut and superseded by algorithmic methods that decouple biometric data from their context and combine them with other types of big data, allowing governments and commercial authorities to overlook the deep potential harms that can result (**R1**, **R3**). The research has also identified the ethical challenges for governing emerging biometric technologies such as emotion detection, voice recognition, and sentiment analysis. Such emerging biometrics are not effectively governed by simply restricting access to personal data because they are often generated as a reusable by-product of other forms of big data, such as social media images or CCTV video (**R1**).

The research proposes that new societal, ethical, and regulatory responses are required (**R1**). In response, Amoore has developed a substantive new approach to ethics in the age of algorithms and cloud computing (**R1**). This goes beyond ethical codes designed to govern biometric identity, proposing that the algorithm itself has ethical bias, assumptions and values, and embracing the principle that every interaction with the algorithm is of potential ethical significance. The research has explained why existing ethical approaches that attempt to grapple with the challenges of algorithmic biometrics – such as 'ethical AI' or 'algorithmic accountability' - are unable to account for the inequalities and discrimination resulting from the interactions of data and models in their training, trials, and deployment (**R1**). Instead, Amoore has proposed ethical approaches that redefine what is at stake with biometric data, shifting the emphasis from identifying individuals to the expanded questions of discrimination, bias, and injustice involved in iterative human and algorithmic decision-making.

3. References to the research

Note: underline indicates Durham employee during the research and/or at the time of publication. Citation data are from Google Scholar, updated 1 Sept 2020.

R1: Amoore, L. (2020) *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*. Durham, Duke University Press, doi:10.2307/j.ctv11g97wm. *(Returned to REF2021; 24 citations)* (PDF available from Durham)

R2: Amoore, L. (2006) Biometric borders: governing mobilities in the war on terror. *Political Geography* 25, 336-351, doi:10.1016/j.polgeo.2006.02.001. *(Returned to RAE2008; 1115 citations)*

R3: Amoore, L. (2018) Cloud geographies: computing, data, sovereignty. *Progress in Human Geography* 42, 4-24, doi:10.1177/0309132516662147. *(99 citations)*

R4: Amoore, L. (2013) *The Politics of Possibility: Risk and Security Beyond Probability* Durham NC, Duke University Press. *(Returned to REF2014; 615 citations)* (PDF available from Durham)

R5: Amoore, L. (2011) Data derivatives: on the emergence of a security risk calculus for our times. *Theory, Culture & Society* 28, 24-43, doi: 10.1177/0263276411417430. *(Returned to REF2014; 389 citations)*

R6: Amoore, L. (2009) Algorithmic war: everyday geographies of the war on terror. *Antipode: A Radical Journal of Geography* 41, 49-69, doi: 10.1111/j.1467-8330.2008.00655.x. *(Returned to REF2014; 304 citations)*

4. Details of the impact

The impact of the body of work described in Section 2 has been to advise and hold to account the UK public authorities who design, implement and deploy algorithmic biometric technologies. The impact has developed from extensive engagement over a 14-year period with international public authorities, commercial organisations, and NGOs. This activity developed knowledge about the intersection of biometric data and algorithms, for example through the International Air Transport Association's Passenger Risk Assessment Study (2014) based on an ESRC-funded knowledge exchange placement. While we do not claim impact from that activity here, it shaped the context and content of Amoore's impact on the governance of biometric data and algorithms in UK public life. As a direct consequence of research findings presented to three public bodies, Amoore was appointed to the Home Office's Biometric and Forensic Ethics Group, which emerged in response to evidence provided by Amoore and others of a governance gap in relation to biometric data and the implications for security and public life. We describe this sequence of impacts in turn.

In 2014, Amoore and Piotukh provided written evidence to the Ministry of Justice's *'Review of the Balance of Competences between the United Kingdom and the European Union Information Rights'* (evidence source **E1**), published in December 2014. Durham research was cited extensively in the final report, specifically in relation to questions of data protection and accountability that follow from new forms of data and data processing. The Durham evidence was cited in the context of the fundamental right to data protection (**E1**, Paragraph 1.75), the inadequacies of current transatlantic approaches to safeguarding personal data (**E1**, Paragraph 2.52), and the interconnectedness of the movement of data and the movement of things and people (**E1**, Paragraph 2.102). In particular, the evidence informed the report's discussion of 'concerns' with the control of data in cloud computing (**E1**, Paragraph 3.25) and the need for trust in cloud computing: *'Durham University also cautioned about the lack of transparency about the relationship of responsibilities and processes within the Cloud'* (**E1**, Paragraph 3.26).

Amoore provided written and oral evidence in November 2014 to the House of Commons Science and Technology Committee on 'Current and future uses of biometric data and technologies'. The evidence was the only social science submission to detail how biometric data have become newly analysable and linkable with algorithmic techniques. Amoore highlighted the implications for public transparency and accountability that follow from the use of biometric data in algorithmic analytics. Her testimony informed three key areas of the committee's report (**E2**), published in March 2015. First, the committee identified trends in the use of biometric data, specifically the move towards linking different types of biometric data with other data through *'advanced algorithmic analytics'* (**E2**, Paragraphs 21-23). Second, the report discussed the problems posed by biometric data, with Amoore's testimony demonstrating that the issue is not only with the underlying science of biometrics, but also with how biometric data are put to use in machine learning algorithms (**E2**, Paragraph 47). Third, Amoore's testimony highlighted the inadequacy of current regulatory approaches to biometrics and biometric systems, and the need for greater transparency, public scrutiny, and accountability (**E2**, Paragraphs 47, 66, 81, 83). The government response to the report, published in September 2015, noted the concerns and stated that the government was considering whether to apply ethical oversight to biometric data (**E3**).

Amoore subsequently provided written and oral evidence to the Science and Technology Committee's evidence session on 'Algorithms in decision making' in November 2017. This evidence again informed several key areas of the committee's report (**E4**), published in May 2018. Her testimony was cited in support of the framing argument that algorithms can be used to identify patterns in big data (**E4**, Paragraph 2), and critically underpinned the view that some form of bias is '*intrinsic to the algorithm*' (**E4**, Paragraph 32), supporting the committee's conclusion that '*[a]lgorithms, like humans, can produce bias in their result, even if unintentional*' (**E4**, Paragraph 44). Finally, Amoore pointed out that algorithms based on machine learning may not be fully transparent and understandable in their functioning, even to their writers (**E4**, Paragraph 59). This view, and others, informed the committee's view that transparency about an algorithm's '*inner workings*' should be accompanied by an explanation of how it works (**E4**, Paragraph 66).

In sum, Amoore's evidence and testimony to three separate bodies helped to establish the need for new forms of public accountability that are appropriate to how biometric data are being used and combined through algorithms. In response to the governance gap in biometric data and technologies identified by Amoore and others and noted by the government in **E3**, the Home Office established a non-departmental advisory public body – the Biometrics and Forensics Ethics Group (BFEG). The BFEG is the only formally accountable ethics committee within the Home Office. Its members are ministerial appointees whose role is to provide independent ethical advice to Home Office ministers and the Science Secretariat on the ethical impact of the capture, retention, and use of human identification data on society, groups, and individuals. It replaced the National DNA Database Ethics Group, whose sole focus was on DNA in relation to Home Office activity. Amoore was appointed to the BFEG in December 2017. The former Chair of the BFEG (2017-2019) confirms that *'[a]t the point of her appointment, Louise's research findings had led her to make some substantial contributions to the public debates about the ethics of biometrics*' (**E5**), citing the aforementioned testimony and evidence to the Science and Technology Committee, including the identification of a governance gap, the need for public accountability, and the use of biometric identifiers becoming big data inputs for subsequent machine learning (**E5**).

The first area where Amoore made what the former Chair describes as a *'major contribution'* (**E5**) to the work of the BFEG was in relation to live facial recognition technologies. In March 2018 (**E6**, p.6) a BFEG Facial Recognition Working Group was set up to consider the police use of facial recognition systems. The Working Group conducted an inquiry into the use of automated facial recognition systems in public places, such as transportation hubs and urban areas (**E7**). The implementation of such algorithmic biometric systems mirrors exactly the scenarios Amoore cautioned against in her evidence to the Science and Technology Committee (**E2**, **E4**), wherein machine learning algorithms learn from biometric and transaction data in order to identify patterns in human behaviour. The former Chair of the BFEG summarises Amoore's role in the inquiry: *'Overall, and in the context of the team of diverse specialisms within BFEG, Louise has drawn on her research knowledge to provide expertise on the ethics of novel biometrics such as facial recognition, gait and voice recognition'* (**E5**). Amoore co-authored the Working Group report on facial recognition (**E7**), published in February 2019, which recommended that trials and deployments of facial recognition technologies cease until such time as a legislative framework is in place (**E5**, **E7**). It detailed the ethical principles that should govern decisions on future uses of such algorithmic biometrics. As a direct result of the report, public trials and policing deployments of facial recognition technologies that were planned for February 2019 ceased. A meeting took place between the Working Group and the Metropolitan Police Service in March 2019, conveying specific advice and guidance on the ethical design of scientific trials in public spaces. As a result of the Working Group's intervention, facial recognition technology will now not be trialed using the data of members of the public (**E5**, **E8**).

The Facial Recognition Working Group, chaired by Amoore, was subsequently commissioned by the Home Office Science Secretariat to report on the sharing of biometric data and algorithms across public and private authorities. The resulting briefing note (**E9**), whose publication was delayed to January 2021, advises government ministers and policing authorities on the ethical aspects of sharing digital biometric data with private entities such as shopping centres. Following widespread public concern amid the sharing of facial biometric data between the Metropolitan Police and the Kings Cross property developer Argent, the briefing note provides the first public recommendations for ethical oversight of public-private biometric data sharing. The briefing note finds that the police and private companies are sharing biometric data, as well as the algorithms and cloud platforms used to store, combine, and analyse them, in an unregulated way. It cautions that the advent of public-private collaborations in algorithmic biometrics '*has the potential to exacerbate discrimination and bias, particularly in cases where a public authority does not scrutinize the private entity's training dataset and algorithm testing*' (**E9**). It recommends that all new collaborations in biometric data and algorithm sharing must be subject to independent review and scrutiny, with '*proposed deployments*' subject to review and '*monitored at regular intervals during their operation*' (**E9**).

In April 2019 the remit of the BFEG was expanded to four working groups with '*broad thematic relevance to the use of biometrics, forensics and large and complex data sets in the Home Office'* (**E8**). Beyond her work on facial recognition, Amoore is currently centrally involved in two further streams of BFEG work (**E5**). First, she is a member of a working group focusing on the ethics of large and complex datasets and machine learning in immigration workstreams. Second, she is involved in a project developing a data ethics framework to integrate the work done by the BFEG into guidance for government. Within these groups, Amoore has advised cross-departmental projects considering the use of machine learning and biometric data, providing guidance to government data scientists on the ethical issues of discrimination, transparency, fairness, and human and algorithmic decision making. For example, following Amoore's advice that existing data protection impact assessments (DPIAs) for biometric and algorithmic systems did not take new technologies such as cloud storage into account, improvements have been made to future DPIA templates for Home Office projects. In line with Amoore's research findings that ethical concerns extend beyond the source code of the algorithm and into every interaction between the algorithm and people (**R1**), the DPIA template now extends to processes of trialing, testing and recalibrating the system. This change is significant because the DPIA is both a legal requirement and a primary mechanism for public transparency and accountability. In her announcement to the House of Commons in May 2020, the Minister of State, Home Office, thanked BFEG for '*its strategic advice … on the development and testing of new biometric technologies*', and put before Parliament '*recommendations covering the testing and use of live facial recognition technologies by police forces*' and '*the design and implementation of DPIAs with the Home Office*' (**E10**).

In summary, Amoore's research has made a substantial contribution in connecting the issues of algorithmic technologies and biometric data, and advising public bodies on the range of significant new ethical issues surrounding novel algorithmic biometrics, including *'enabling the Home Office to better understand the ethical implications of the choices presented by advances in technology and helping it develop the tools to manage technological develop [sic] in a way which respects individual rights while enhancing public safety'* (**E5**).

5. Sources to corroborate the impact (indicative maximum of ten references)

E1: UK Government, Ministry of Justice (2014) *Review of the Balance of Competences between the United Kingdom and the European Union - Information Rights.*

E2: House of Commons Science and Technology Committee, Sixth Report of Session 2014-2015 on *Current and Future Uses of Biometric Data and Technologies*, HC734, March 2015.

E3: Government Response to the House of Commons Science and Technology Committee Sixth Report of Session 2014-15, HC455, September 2015.

E4: House of Commons Science and Technology Committee, Fourth Report of Session 2017-2019 on *Algorithms in Decision Making*, HC351, May 2018.

E5: Testimony from former chair of the Biometrics and Forensics Ethics Group, 18 February 2020.

E6: Biometrics and Forensics Ethics Group, Notes of the Third Meeting held on 19 March 2018 at the Home Office, London.

E7: Interim report of the Biometrics and Forensics Ethics Group Facial Recognition Working Group, *Ethical issues arising from the police use of live facial recognition technology*, February 2019.

E8: Confidential letter from Data and Identity Directorate policy sponsor detailing participation in and purpose of expanded BFEG working groups, April 2019.

E9: *Briefing note on the ethical issues arising from public-private collaboration in the use of live facial recognition technology*, Biometrics and Forensics Ethics Group Facial Recognition Working Group, January 2021.

E10: Written statement from the Minister of State, Home Office, Hansard, 5 May 2020.