

---

## “Coded Inequity” and the Undercover Policing Inquiry

A Review of Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code*, Polity Press, 2019. 285 pp. £14.99 (PB). ISBN-13: 978-1-5095-2640-6

*patriciatuitt.com*

---

“Codes...operate within powerful systems of meaning that render some things visible, others invisible, and create a vast array of distortions and dangers” (Ruha Benjamin 2019, p. 7).

### *Focus of this review*

Questions of racial justice have played a defining role in the period of UK undercover policing which, since 2015, has been the subject of a judge-led public inquiry. In January 2019, the inquiry found that the justice campaign which followed the death by gun-shot wounds of a 21 year old black man, Colin Roach, in Stoke Newington Police Station was one of the first campaigns “...upon which there was any significant...reporting...” (see Inquiry Transcript, 31.1.2019, p. 21) by an undercover policing unit, the Special Demonstration Squad (SDS), which has since been disbanded. And it was an earlier finding that the same unit had infiltrated an even more prominent black justice campaign - the Stephen Lawrence family justice campaign - that led to the establishment of the current inquiry by the then Home Secretary, Theresa May.

In June 2020, the inquiry will begin to hold public hearings relating to the activities of SDS managers and officers. With this event in mind, this review draws on Ruha Benjamin’s *Race After Technology* in support of the argument that the inquiry’s management of the data it holds (which documents the surveillance methods used against thousands of private citizens who were spied upon by undercover officers) is likely to undermine its stated aim of “getting to the truth of undercover policing”. Focusing on two categories of inquiry decisions made over an approximate two-year period, the review highlights the ways in which the inquiry has reproduced aspects of the very techniques that undercover policing units deployed against private individuals involved in anti-racist/anti-capitalist and family justice campaigns.

The inquiry decisions at issue here relate to applications by former undercover officers for orders restricting the release of their real and/or cover names (anonymity orders), and requests from those spied upon for release of the intelligence reports compiled on them.

In Benjamin's work, "technologies" are equated with all things that are capable of being "coded", and 'names' are accorded special significance. The name "...that is most *ours* is also out of our hands" says Benjamin (2019, p. 3). The inquiry's controversial decision to allow many of the former SDS officers to retain full or partial anonymity by giving evidence through the use of a cypher (a word which denotes many forms of code) establishes the validity of Benjamin's statement. The decision cannot but serve to remind those whose lives were infiltrated by undercover officers who used false names to facilitate their covert operations that "...some people, by virtue of their social position, are given more license to experiment with unique names" (Benjamin 2019, p. 5).

### *About the book*

A wide range of campaigns, not merely those in pursuit of racial justice, were infiltrated by the SDS, and the double-meaning of the main title to Benjamin's book encourages her readers to reflect on the way the *race after technology* in pursuit of the 'quick fixes' which technological use promises has negatively impacted upon people experiencing marginalisation due to many forms of social construct, such as disability, sexual orientation and gender, as well as race. Similarly, her analysis of the "...symbiotic relationship between technology and society..." (Benjamin 2019, p. 41) covers a number of spheres, including education, health and finance as well as the criminal justice sphere about which her book is principally concerned. However, throughout her examination and critique of the "...social dimensions of technology..." (Benjamin 2019, p. 11), Benjamin makes clear that in all of these different but interlocking arenas the lived experiences of black people is key; this because "[t]he plight of Black people has consistently been a harbinger of wider processes...which then get rolled out on an even wider scale" (Benjamin, 2019: p. 32). To apply Benjamin's insights to the undercover policing context, we might say that the appearance of SDS officers during the Colin Roach campaign for justice attests to the fact that what is often presented as *new* practices of so-called "[pre-emptive policing]" may well be new to *some* communities but is entirely "... consistent with the long history of racial surveillance endured by Black people" (Benjamin, 2019: p. 121).

Benjamin's statement that "...in many ways Black people *already* live in the future" (2019: p. 32) provides the powerful framework of a book that will almost certainly become a major point of reference.

### 3. “Coded Inequity” and the Undercover Policing Inquiry

That this future need not be a bleak one is clear from Benjamin’s discussion of how the plight of black people has provided the impetus for the development of “...technology with an emancipatory ethos...” (Benjamin 2019, p. 163). Two of the examples of what she refers to as a “...race conscious orientation to emerging technology...” (Benjamin 2019, p. 35) warrant attention. The first example given is an app called Appolition which allows owners of the app to convert change from their daily shopping “... into bail money to free black people” (Benjamin 2019, p. 161). For Benjamin, Appolition represents a “...tool of solidarity that directs resources to getting people literally free” (Benjamin 2019, p. 163). The second example given is that of the White-Collar Early Warning System, which “...flips the script by creating a heat map that flags city blocks where financial crimes are likely to occur” (Benjamin 2019, p. 196), thereby challenging “...the narrative of what we consider to be a crime and of whom we consider to be a criminal....(Benjamin 2019, p. 197).

*Race After Technology* aims to expose the “...social bias embedded in technical artifacts...” (Benjamin 2019, p. 53). Such biases are embedded in apparently simple ‘codes’, such as names, which are always “...interacting with numerous technologies, like airport screening systems and police risk assessments, as forms of data (Benjamin 2019, p.1). Social biases are also embedded in more elaborate ‘legal codes’ which offer ostensible protection to individuals against the invasive/abusive use of data and technology but which, from the example of the European Union’s General Data Protection Regulation (GDPR), invariably contain provisions which allow “...a wide latitude for government officials to revoke data rights in an instant...[w]hat looks like an expansion of data rights for individuals rests on the ability of governments to revoke those rights from anyone deemed a public threat” (Benjamin 2019, p. 188).

The technical artifacts discussed in the book are diverse in form, and include facial recognition tools which have proved time and again that “[s]ome technologies fail to see Blackness, while others render Black people hypervisible and expose them to systems of racial surveillance” (Benjamin 2019, p. 99), electronic monitoring systems which “...function is to create vertical realities - surveillance and control for some, security and freedom for others” (Benjamin 2019, p. 158), and ancestry testing tools (increasingly deployed in the management of asylum applications), which, in the case of the UK (see Benjamin 2019, p. 128-132) have proved highly controversial - even in the context of a “...broader push toward privatization where efforts to cut costs and maximise profits, often at the expense of other human needs, is a guiding rationale for public and private sectors alike” (Benjamin 2019, p. 30).

Overall, the author aims to show how even when technical artifacts and data are used for ostensibly emancipatory purposes (for example, in order to uncover the truth behind past oppressive practices - as in the case of the undercover policing inquiry) their use inevitably “...reflect and reproduce existing inequalities that are promoted and perceived as more objective or progressive than the discriminatory systems of a previous era” (Benjamin 2019, p. 5/6 - original emphasis removed). This practice of reproduction is what the author refers to as “coded inequity” - a concept I examine further in the context of the undercover policing inquiry in the next section of this review. To conclude this part, whilst the subtitle of the book immediately situates it within the civil rights/justice landscape of America, *Race After Technology* will nonetheless appeal to a broad audience of readers concerned to address questions of social justice through an emerging academic field, which the author designates as “... race critical code studies...” (Benjamin 2019, p. 34) .

### *“Coded inequity” and the undercover policing inquiry*

“Coded inequity” is used by the author as a generic term which encapsulates the books several themes and supporting examples. At its most exact, “coded inequity” is “...the practice of codifying existing social prejudices into a technical system...” (Benjamin 2019, p. 96), but it is important to understand that Benjamin’s task is precisely to render less distinct so-called ‘technical’, ‘social’ and ‘cultural’ spheres. Understood in this way, I found Benjamin’s notion of “coded inequity” to be a productive one for analysing the effects of two distinct categories of decisions which have been made in the course of the undercover policing inquiry’s preliminary investigations. These are decisions on applications by former undercover officers for orders restricting the disclosure of their real and/or cover names, and decisions on requests by non-state core participants to the inquiry for the release of intelligence reports in which they have been named or otherwise identified.

For Benjamin, “coded inequity” is a particularly troubling practice where the purpose of the system design is benign, or, as in the case of an inquiry, avowedly transformative. Whilst the precise scale of undercover police reporting on private individuals is not yet known, conservative assessments suggest that the practice was extensive. In April 2019, in the first of two Statements on Data Protection and Privacy (ISDPP), the inquiry chair stated that “...tens of thousands of intelligence reports produced by undercover officers...” (ISDPP, 11 April 2019, p. 1) are currently being processed. This translates into approximately 67,400 documents (ISDPP, 11 April 2019, p. 1). In short, the inquiry is in possession of vast amounts of data, and the harnessing and processing of this data has presented it with significant challenges. It need hardly be said that such challenges are being met in part by the design and implementation of sophisticated

data processing and other technical systems., including a “secure computer system” (ISDPP, 11 April 2019, p. 1) which will have been designed to ensure, among other things, that the cyphers used by those undercover officers to whom the inquiry has granted partial or complete anonymity cannot be easily “decoded”.

I move now to the first of the two sets of decisions made in the course of the inquiry’s preliminary investigations which we might better comprehend through the theoretical frameworks which Benjamin provides in *Race After Technology*. For approximately twelve to eighteen months, a significant part of the inquiry’s work was devoted to processing and deciding upon anonymity applications - the majority of which were from former undercover police officers. Some particularly wide-reaching decisions were made in the period between 21 November 2017 and 7 August 2018. If we take the inquiry public facing records of these decisions at face value, we might suppose that it was legal rules - specifically Article 8 of the European Convention on Human Rights (ECHR), which covers the right to family and private life - which constrained the chair’s decisions on these anonymity applications. However, if we follow Benjamin, we might instead conclude that the real constraining force was no more nor less than the oppressive and improper histories of undercover policing. Setting out the aims of her book, Benjamin is at pains to stress that “[t]his is not simply a story of ‘then’ versus ‘now.’ It is about how historical processes make the present possible...” (Benjamin 2019, p. 147). It is because undercover officers engaged in elaborate subterfuge while they were serving officers - thereby exploiting the social positions that enabled them to “experiment with unique names” (Benjamin 2019, p. 5) - that the inquiry chair has been able to find sufficient evidence of the unjustified interference in the right to respect for private and family life that would result from the revelation of the real and/or cover of names of a number of the former undercover officers who sought anonymity. The “historical process” of undercover policing during which undercover officers were given licence to experiment with names is under scrutiny by the inquiry. Yet, per Benjamin, it is that same “historical process” which made it possible for the inquiry chair to use *his* special social position in a way which continues the name experiment into the upcoming inquiry evidence hearings.

The second set of decisions concern requests by non-state core participants for the release of intelligence reports in which they have been named or otherwise identified. The inquiry protocol governing release of intelligence reports is summarised in two ISDPPs published in April and August 2019. However, the protocol is informed by two public hearings (31.1.2019 and 25.3.2019) at which consideration was given to the requirements of the GDPR.

In essence, the protocol that has been established to deal with such requests is that unredacted versions of intelligence reports (ISDPP, 21 August 2019, p. 2) will be disclosed *after* the officers who collated the reports have had the opportunity to review them and comment on the circumstances in which they were produced (ISDPP, 11 April 2019, p. 2-5), and subject to the individual to whom disclosure is made being placed under a legal duty of confidentiality in respect to what she/he has gleaned from the reports, ((ISDPP, 21 August 2019, p. 3).

We now know that the vast majority of these intelligence reports are comprised of mixed personal data. This means, for example, that information relating to one non-state core participant will, in most cases, be mixed in with information relating to other inquiry participants, Moreover, the reports include ‘special category’ information, relating to health, sex life, criminal convictions and other especially sensitive matters. The ISDPP protocol allows for some redaction of intelligence reports (and other documents, such as witness statements from former undercover police officers) where ‘special category’ information is present, but “... [i]t is anticipated that the net result will be that almost all personal data, including special category personal data, will not normally be restricted from disclosure to a witness from whom evidence is sought” (ISDPP, 21 August 2019, p. 3).

Many members of the public would have come to learn of the undercover policing inquiry because of publicity surrounding a particularly abhorrent covert policing strategy. The strategy was one in which women members of political campaign organisations were deceived into intimate relationships with undercover officers so that the officers could more easily gain intelligence on the campaign organisation’s *lawful* activities. Here the historical processes that , per Benjamin, make the present possible is clear. The deceitful infiltration of personal lives by undercover officers assumed a largely unfettered licence to override the rights to privacy and bodily integrity of the individuals who were spied upon. And it is that history which today renders the data privacy rights of those who were spied upon vulnerable - even against the GDPR regime which was designed precisely to secure such rights. Indeed, to the extent that they are unable to avoid being recipients of disclosures about others from unredacted intelligence reports, those who have yet to fully deal with the social and psychological effects of having been spied upon by undercover police officers are placed in an intolerable position where they are required to ‘covertly’ absorb potentially highly sensitive information pertaining to other anti-racist/capitalist campaigners.

### *Conclusion: wider themes*

“Demanding more data about subjects that we already know much about is, in my estimation, a perversion of knowledge. The *datafication of injustice*...in which the hunt for more and more data is a barrier to acting on what we already know” (Benjamin 2019, p. 116).

I have chosen to focus this review on a public inquiry concerning a matter of importance in the UK. However, I would be doing less than justice to the eclectic mix of theories, situated examples and contexts on which *Race After Technology* relies if I do not conclude this review with an intimation of at least one other UK context in which scholars and policy-makers would benefit from Ruha Benjamin’s extremely lucid analysis. When I first read the quotation from the book with which this concluding part begins, I was inclined to orient the review toward the higher education context. In the UK at least, higher education is more and more wedded to the use of algorithms and other technical processes to ‘fix’ a number of ills - some real, others, like degree grade inflation, largely imagined. The most pernicious example of what Benjamin refers to as the “datafication of injustice” (2019, p. 116) is evident in the response of government bodies and universities to the attainment gap between black and minority ethnic (BAME) students and white students. I fear that such data collecting exercises - whatever their intention - will do more than simply defer any real action on the problem: for they will provide the content of a modern colonial archive of ostensibly ‘objective’ data about BAME students (and staff), which, as Benjamin’s analysis of “coded inequity” informs us, can only be used in ways which underscores their marginality.

## References

Undercover Policing Inquiry, Chairman’s Statement of Data Protection and Privacy, 11 April 2019.

[https://www.ucpi.org.uk/wp-content/uploads/2019/04/20190411-Chairmans\\_Statement\\_on\\_Data\\_Protection\\_and\\_Privacy.pdf](https://www.ucpi.org.uk/wp-content/uploads/2019/04/20190411-Chairmans_Statement_on_Data_Protection_and_Privacy.pdf)

Undercover Policing Inquiry, Chairman’s Second Statement of Data Protection and Privacy: Disclosure to Non-Police, Non-State Core Participants and Civilian Witnesses, 21 August 2019.

[https://www.ucpi.org.uk/wp-content/uploads/2019/08/20190821-chairmans\\_second\\_statement\\_on\\_data\\_protection\\_and\\_privacy\\_san.pdf](https://www.ucpi.org.uk/wp-content/uploads/2019/08/20190821-chairmans_second_statement_on_data_protection_and_privacy_san.pdf)

Undercover Policing Inquiry, Transcript of Hearing, 31 January 2019.

[https://www.ucpi.org.uk/wp-content/uploads/2019/01/20190131-transcript-Privacy\\_hearing.pdf](https://www.ucpi.org.uk/wp-content/uploads/2019/01/20190131-transcript-Privacy_hearing.pdf)