

one's European history right is not the magic formula that will solve the problems of historical change in the non-Western world.' On this issue, especially, William H. Sewell, Jr's measured (but again, brief) commentary on the historiography of the bourgeois revolutions functions as a good mediator by emphasising that perhaps the best way to 'provincialize Europe' is to insist that it, too, consists of a number of provinces, nations and histories.

On the final issue, regarding Chibber's only proposal for an adequate form of social theory, several of the symposium papers criticise the appeal to a modified analytic Marxism espoused by Chibber; the prominent term of derision here being 'rational choice Marxism'. The rather bombastic call in *PTSC* for a twofold 'universal history' – a history of capital and one of worker struggles read as the expression of a struggle for the fulfillment of basic needs and rationally-comprehensible interests – wasn't fully worked out therein, nor was it of course intended to be (although if his recent article 'Rescuing Class from the Cultural Turn', is anything to go by, this is a task he will take on in time to come). But the claim that there is an unbridgeable gulf between postcolonial theory and Marxism (or, between identity politics and class struggle) is one we've heard before; Ahmad's 1992 book is a case in point.

The current volume does much to elucidate the terms of this 'debate' but little to push the stakes further. The exception is the final (and by far the longest) essay by Viren Murthy. Here, the limitation that one faces when insisting on either side of a dichotomy between postcolonial theory and Marxism is skilfully sidestepped in an immanent critique of both Chibber and Chakrabarty that interrogates their respective conceptions of capitalism by way of value-form theorist Moishe Postone. Unfortunately, as a whole however, if the criteria of assessment for intellectual debates should go beyond leaving either side with a sense of having been both misunderstood and right all along, the Chibber debate offers, in the end, only a limited contribution.

**Marie Louise Krogh**

## Remain in light

Finn Brunton and Helen Nissenbaum, *Obfuscation: A User's Guide for Privacy and Protest* (Cambridge, MA: MIT Press, 2015). 136pp., £16.95 hb., 978 0 26202 973 5

Since the beginnings of Enlightenment era struggles against absolutism, one of the most prominent concerns of progressive politics has been to tear away the veils concealing the operation of power. Publicity and openness have long been the overriding values in Western democracies and, although they do not necessarily take a liberal form, such ideals are now deeply ingrained. Political discourse constantly references the importance of 'transparency', while suspicious publics are ever vigilant with regard to the secret machinations of their representatives. At the same time, a competing tendency, according to which progressives and radicals strove to protect privacy and foster secrecy, has been equally important but arguably less prominent. In the early days of Enlightenment, those with unorthodox ideas needed to be sheltered from scrutiny; thinking against the grain required the space to do so. Thus, Habermas has described how in the eighteenth century it was from within the private space of the family that the bourgeoisie set out into the newly formed public sphere. Perhaps the most striking example of this strand of opacity is the way Masonic lodges promoted equality and Enlightenment partly through ritualised secrecy, helping to undermine the status quo from Bavaria to Haiti as they did so. Rather than ever-increasing illumination, then, modern struggles for liberty and progress began with a combination of transparency *and* obstruction.

Contemporary conditions appear to call with increasing urgency for a renewal of the latter part of this equation. The Snowden revelations concerning the extent of government surveillance capabilities and, at a more mundane level, the unprecedented capacity for corporate giants such as Facebook and Google to harvest our data are well known. Awareness is one thing, however, knowing how to respond quite another. Many are not concerned at all – shock-

ing as the Snowden revelations were, 'if you've done nothing wrong, you have nothing to fear' is the easiest response. It is easier still to surrender 'our' data as we access social media or shop online. In keeping with the more obvious appeal of publicity and popular determination to see behind the veil, perceived obfuscation and mendacity by elites incur far greater popular ire than these incursions on our privacy.

As Finn Brunton and Helen Nissenbaum point out, the problem is that when it comes to the politics of knowledge most of us are on the wrong side of a massive epistemic asymmetry. Our relative lack of power arises not only, or even predominantly, from the way information is concealed, but also from the fact that the data we produce as we shop, socialise, travel and work – as we do just about anything, in fact – is collected and analysed using methods and in pursuit of ends which remain mysterious to all but a few experts. Complex algorithms use data harvested from everyday activity to determine our access to insurance, credit, housing, healthcare. As the authors put it: "‘They’ know much about us, and we know little about them or what they can do.’ We know even less about the uses to which this data might be put in the future by actors who may not yet exist. In many respects, as the authors point out, the result is a prison from which it is hard to see any possibility of escape. There is little prospect of grand acts of resistance, and ‘opting out’ is, for most, simply not realistic. We seem to have little choice but to allow ourselves to be subjected to constant scrutiny using methods which we cannot hope to understand – a fact which perhaps explains the apathetic reaction of many to invasions of privacy.

If we are to retain our dignity and autonomy under these conditions, Brunton and Nissenbaum argue, we must look to ‘weapons of the weak’. The forms of resistance most easily adopted, and therefore most likely to prove effective, are ‘foot-dragging, slowdowns, feigned ignorance, deliberate stupidity, and the pretence of compliance.’ A significant source of such humble but revolutionary – and, as the book shows, frequently ingenious – action lies in ‘obfuscation’, the essence of which is ‘getting overlooked and adding to the cost, trouble, and difficulty of doing the looking’. This is the quintessential tactic of

those who cannot avoid being observed.

The first part of this ‘user’s guide’ provides examples of obfuscation drawn from nature, military strategy, espionage and technology. It opens with a description of World War II planes using ‘chaff’ to confuse radar: an Allied plane could not avoid being detected, but by dropping hundreds of pieces of foil it could become one dot among many on a Nazi radar screen. In the natural world, the orb-weaving spider must spin a large web if it is to eat but in doing so exposes itself to attack from predatory wasps. Its response is not to fight or to build shelter, but the more efficient solution of creating decoy spiders from silk and leaves. Like the plane or the spider, we cannot avoid exposing ourselves to surveillance. Like them, however, we are in a position to make life difficult for those watching us. In the context of gross epistemic asymmetry, data obfuscation represents a realistic means of defending privacy. Through obfuscation we can retain some dignity and autonomy, along with some hope of expressing dissent or concealing resistance. Nissenbaum herself has designed the TrackMeNot browser extension, which obfuscates in the face of attempts to observe the user’s search history or mine it for data. Rather than relying on encryption or concealment, the program generates a stream of random searches in which the genuine are lost. Other examples include FaceCloak, which hides genuine social connections from Facebook by producing a plausible ‘non-person’, and Anonymouth, a tool for anonymous authors to avoiding stylometric identification by producing ‘statistically bland prose.’

Part II of the guide deals with the implementation and justification of obfuscation. Chapter three describes our contemporary informational asymmetry, whilst drawing on James C. Scott’s account of power relations in a Malaysian village to explain why obfuscation is necessary. The authors are rightly careful not to push the comparison too far, but use Scott to support their claim that in the face of power asymmetries the weak must often rely on modest forms of resistance. The book’s fifth chapter presents a series of questions through which potential users might determine what kind of obfuscation they need. In keeping with the practical purposes of the book,

Brunton and Nissenbaum emphasise that successful obfuscation must be highly sensitive to context and purpose: do you want to buy time, cover your tracks or conceal your identity? Your answer to such questions should shape the tools you employ.

The most complex questions are addressed in chapter four, which considers how obfuscation can be justified. The authors' primary aim is clearly to provide those practicing and designing obfuscation with a ready means of responding to objections that they are engaged in antisocial, destructive behaviour through free-riding on online communities or using up valuable bandwidth. Rawls' maximin principle provides a neat response to such criticisms: in assessing data practices we should favour those which maximise the position of the worst off; the status quo clearly does not meet this requirement and obfuscation is therefore justified. Perhaps more insightful, however, is the suggestion that informational asymmetry involves a violation of autonomy of the kind described by Philip Petit in his account of republican freedom. On this view, obfuscation is justified because we are currently subjected to the arbitrary will of those who control data collection and analysis and, as a result, are not truly free.

Perhaps because of the concern to be concise and practical, the book rarely ventures beyond the possessive and distributive epistemology that has come to represent an article of information age common sense. Knowing involves holding information and transmitting it from actor to actor, and obfuscation appears as a strategic move in a field structured by the circulation of data. This is, of course, an at least partly true representation of our current predicament. However, it risks marginalising those aspects of obfuscation which might involve the assertion of a fundamentally different subjectivity to that imposed by the data-harvesters. The power asymmetries identified in the book are not simply a matter of the possession and control of information; they relate to the very nature of the subjectivity available to us. Before information can circulate, be fought over or distributed, individuals must be moulded into the right kinds of actors and their relationships, actions and preferences rendered into fungible data – into exchange values. This occurs at

the cost of their autonomy, individuality and spontaneity. Obfuscation is potentially an act of resistance in the face of this process, rather than a strategic move on the pre-existing terrain of information. The dangers of pursuing obfuscation in the absence of such considerations are apparent in Brunton and Nissenbaum's concern that Anonymouth's 'statistically bland prose' would prevent the emergence of a modern Tom Paine. Nevertheless, by reviving a tradition of progressive opacity, *Obfuscation's* call to throw sand in the gears shows the degree to which we can turn systems of data-mining against themselves and begin to exercise the autonomy which they serve to suppress.

Matthew Fluck

## Blinded by surveillance

Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Durham, NC and London: Duke University Press, 2015). ix+213pp., £70.00 hb., £19.99 pb., 978 0 82235 919 7 hb., 978 0 82235 938 8 pb.

Surveillance is not blind. Massive, generalised and indiscriminate surveillance might nowadays be pervasive, but the blanket nature of some surveillance practices should not make us forget that they are governed by specific purposes, and that they produce distinct impacts in relation to race and gender. Surveillance is not fortuitous, and its technologies are not neutral, undiscerning or colourless. Simone Browne's *Dark Matters: On the Surveillance of Blackness* documents the non-blindness of surveillance with vibrant detail. It bridges the (cosmic) gap between the fields of surveillance and black studies, guided by a cultural studies' will to embrace potentially anything as a source of edifying light. Bringing into her discussion heterogeneous historical records, contemporary art and Hollywood blockbusters, the book travels through the history of black lives under surveillance, so illuminating its connections with anti-black racism. Indeed, *Dark Matters* connects the roots of surveillance itself with the transatlantic