9

TOWARDS DATA JUSTICE

Bridging anti-surveillance and social justice activism[1]

Lina Dencik, Arne Hintz and Jonathan Cable

The Snowden leaks provided unprecedented insights into the operations of state-corporate surveillance and highlighted the indiscriminate nature of large-scale data collection across communication networks and platforms in Western democracies, most notably the US National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ). The documents illustrated the intricate ways in which everyday communication is integrated into an extensive regime of surveillance that relies considerably on the "data-fication" of many aspects of social life. Ordinary users' social activities are "sucked up as data, quantified and classified, making possible real-time tracking and monitoring" (Lyon 2014, 4). This information infrastructure characterizes a particular mode of governance, one that is rooted in a political economy in which the prevailing logic is to predict and modify human behaviour as a means to produce revenue and market control; what Zuboff (2015) has described as "surveillance capitalism". Such data-driven forms of social organization have significant implications for citizenship (cf., Hintz, Dencik and Wahl-Jorgensen 2018; Isin and Ruppert 2015) and particularly for how citizens might intervene, challenge and resist this form of governance. As part of the interplay between data and politics, resistance can take several forms. Much onus has been on the collection and use of data, and prominence has been placed on the use of counter-surveillance technologies such as encryption or anonymisation tools along with a focus on advocacy pertaining to privacy and data protection amongst digital rights groups. This has provided windows of opportunity for technological developments and legislative changes that speak particularly to concerns with the implications of surveillance programmes for secure communication infrastructures and individual privacy (Hintz and Brown 2017; Rogers and Eden 2017). However, the degree to which such strategies and concerns have expanded towards the broader range of politically-active and interested

publics is less clear. Moreover, a common agenda around an engagement with the politics of or in data in which data is seen as "generative of new forms of power relations and politics at different and interconnected scales" (Ruppert, Isin and Bigo 2017, 2) is difficult to identify.

In this chapter we explore the relationship between these broader concerns and data by analysing responses to the Snowden leaks amongst political activists in the UK.[2] The chapter draws from a series of in-depth interviews with UK-based activists engaged in a range of social justice concerns, exploring attitudes and practices in relation to mass data collection and digital surveillance. Based on this research, we develop the concept of "data justice" as a way of reframing prominent understandings of data politics.

The chapter starts by outlining the implications of the Snowden leaks for political activists before discussing how resistance to data-driven surveillance has predominantly emerged in their aftermath. We argue that resistance in the datafied society post-Snowden has tended to focus on techno-legal responses relating to the development and use of encryption and policy advocacy around privacy and data protection. This presents a particular way of framing and engaging with data politics. In light of this, we examine how these types of practices are negotiated amongst political activists and outline the extent to which the activists we interviewed view such resistance as part of their social justice agendas. We observe a significant level of ambiguity around technological resistance strategies, while policy responses to the Snowden leaks have largely been confined within particular expert communities. In the final part of the chapter, we therefore propose a (re)conceptualization of resistance to data collection and use that can address the implications of this data-driven form of governance in relation to broader social justice agendas. To that end, we introduce the notion of data justice which, we argue, would help contextualize datafication, connect it to social and economic justice concerns, and thereby contribute to transforming the role of data politics in current civil society practice and, potentially, public debate. This is particularly significant in light of the central role of data-driven processes in contemporary capitalism.

The Snowden leaks and political activism

The revelations of programmes designed to "bulk" collect data on citizen engagement with digital infrastructures[3] indicate the extent to which contemporary forms of governance are increasingly based on the ability to monitor, track and potentially predict the behaviour of entire populations. This is part of a broader emphasis on the role of "big data" in current societies (Kitchin 2014) that highlights the surveillance implications of the "big data" discourse. As Lyon (2015) has argued, surveillance culture came prominently into view simultaneously with the intensified security-discourse following 9/11 and the so-called war on terror. In particular, the uncertainty of the form and nature of potential threats in such a political climate provides an apparent necessity and justification for limitless measures to be taken to

ward off any such possible dangers. The focus, therefore, moves to the operationalization of how to perceive of these potential threats, in which the apparatuses of surveillance play an integral role (Massumi 2015). In such circumstance, the rise of "surveillance society" marks a social context characterized by an increasing amount of surveillance taking place alongside an explosion in the possible methods and means for observing and monitoring people's behaviour (Lyon 2001).

A central concern for Snowden and others has been the extent to which extensive forms of monitoring lead to a "chilling effect" in society that stifles the possibilities for challenging institutions of power and advocating for social change. Although the theory of "chilling effects" has historically been difficult to empirically prove and remains controversial, the debate on it following the Snowden leaks concerned the extent to which government surveillance may deter people from engaging in certain legal (or even desirable) online activities because they fear punishment or criminal sanction, and do not trust the legal system to protect their innocence (Penney 2016). Such surveillance "effects" were documented in a survey carried out by the PEN American Center in the immediate aftermath of the Snowden leaks in which they found that writers are engaging in self-censorship as a result (PEN 2013). Further studies have shown a reluctance amongst citizens to engage with politically sensitive topics online, such as a decline in "privacy-sensitive" search terms on Google (Marthews and Tucker 2015), a decline in page views of Wikipedia articles relating to terrorism (Penney 2016), and a "spiral of silence" in surveillance debates on social media (Hampton et al. 2014). As Greenwald claims:

> Merely organizing movements of dissent becomes difficult when the government is watching everything people are doing. But mass surveillance kills dissent in a deeper and more important place as well: in the mind, where the individual trains him- or herself to think only in line with what is expected and demanded.
>
> *(2014, 177–178)*

Furthermore, the Snowden leaks revealed the expansive notion of "target" that has come to be operationalized in such a mode of governance, going far beyond what may be obvious misconduct or wrong-doing. Greenwald points out:

> The perception that invasive surveillance is confined only to a marginalized and deserving group of those "doing wrong" – the bad people – ensures that the majority acquiesces to the abuse of power or even cheers it on. But that view radically misunderstands what goals drive all institutions of authority. "Doing something wrong" in the eyes of such institutions encompasses far more than illegal acts, violent behavior and terrorist plots. It typically extends to meaningful dissent and any genuine challenge. It is the nature of authority to equate dissent with wrongdoing, or at least with a threat.
>
> *(Greenwald 2014, 183)*

The Snowden leaks provided substantial evidence for the ways in which a wide range of politically active citizens are under scrutiny in this ever-expanding threat environment. For example, documents showed that government agencies in both the US and the UK have actively been engaging in the monitoring of political groups with a "watchlist" including international organisations such as Medecins Du Monde (Doctors of the World), UNICEF, Amnesty International and Human Rights Watch, as well as prominent individuals such as Ahmad Muaffaq Zaidan (Al-Jazeera's Pakistan Bureau Chief), Agha Saeed (a former political science professor who advocates for Muslim civil liberties and Palestinians rights), and groups such as Anonymous (Harding 2014; Privacy International and Amnesty International, 2015). State surveillance practices have also extended to the monitoring of politically-interested citizens with programmes such as the one carried out by GCHQ in the aftermath of the "Cablegate" publications which sought to track any visitor to the Wikileaks site by tapping into fibre-optic cables and collecting IP addresses of visitors to the site as well as the search terms used to reach the site (Greenwald and Gallagher 2014).

These disclosures build on previous and continued practices of surveillance of activist groups and dissenting voices. In the UK, revelations of undercover police officers infiltrating a range of activist groups over a longer period of time, including environmental and animal rights activists, have illustrated the invasive tactics used to monitor and suppress protest and dissent (Lubbers 2015). This is alongside other documented forms of managing and containing resistance, tracking activities and intercepting planned actions, whether by corporate agencies or state bodies (cf. Lubbers 2012; Smith and Chamberlain 2015; Uldam 2016). The navigation and circumvention of surveillance is therefore a fully integrated and long-standing tradition in some activist circles (della Porta 1996; Earl 2003; Leistert 2013). However, with the emergence of big data-driven surveillance programmes, regimes of governance and control have increasingly been based on digital infrastructures that facilitate "dataveillance" – a form of continuous surveillance through the use of (meta)data (Raley 2013). These regimes are rooted in the economic logic of "surveillance capitalism" in which accumulation is pursued through the ability to extract, monitor, personalize, and experiment based on the pervasive and continuous recording of digital transactions (Varian 2014; Zuboff 2015). Not only does the entrenchment of this logic within everyday communication technologies cement a fundamentally asymmetrical power relation between activists and those wishing to carry out surveillance on them (Leistert 2012), but the nature of these, often invisible, infrastructures also carries with it central pertinence and significance for activists seeking to challenge existing power relations and mobilize social change. As Lovink and Rossiter (2015) have argued, a politics of the "postdigital" in which the digital has become so omnipresent that it has been pushed to the background and become naturalized, demands of activism to focus on the network architectures at the centre of power in order to pursue genuine social justice and emancipatory ideals.

Anti-surveillance and techno-legal resistance

Efforts to resist data-extractive technologies have taken several forms, particularly in relation to surveillance. As Mann and Ferenbok (2013) have argued, multiple types of "veillance" intersect, undermine and challenge each other in the monitoring of modern societies. Surveillance – veillance in which the viewer is in a position of power over the subject – is often met with efforts to revert or 'equalize' such power. Mann has placed emphasis on the advent of "sousveillance" in this regard, where the subject is gazing back at power "from below", exemplified by technologies such as wearable cameras and other efforts to capture, process, store, recall and transmit human-centered sensory information (Mann 2005, 636). However, as Bakir (2015) points out, modes of resistance to surveillance also include counterveillance and univeillance that speak more to the sabotaging and blocking of surveillance as well as ways of making intelligence services more accountable.

Much resistance to surveillance following the Snowden leaks has centred on these latter strategies – particularly on developing and "mainstreaming" alternative technologies alongside campaigns for tighter policies on the protection of personal data. To start with, forums to provide secure digital infrastructures to activists have proliferated, with "numerous digital rights and internet freedom initiatives seizing the moment to propose new communication methods for activists (and everyday citizens) that are strengthened through encryption". (Aouragh et al. 2015, 213). These have included renewed focus on privacy-enhancing tools such as the TOR browser, the GPG email encryption system and the encrypted phone and text messaging software Signal. An increasing number of websites now support the more secure https protocol rather than the standard http, and a growing number of internet users have downloaded tools such as "https everywhere" that connect to those more secure websites. Privacy guides such as the Electronic Frontier Foundation's "Surveillance Self-Defense" (https://ssd.eff.org/en) and the Tactical Tech Collective's "Security in a Box" (https://tacticaltech.org/projects/security-box) explain the use of privacy-enhancing tools and offer advice on secure online communication. "Crypto-parties" have brought necessary training in such tools to towns and cities worldwide (O'Neill 2015).

Technical solutions to mass data collection have included, furthermore, the development of self-organized communications infrastructures as alternatives to corporate services such as Google and Facebook. Groups such as Riseup.net, Autistici and Sindomino have offered mailing lists, blog platforms and collaborative online workspaces that protect user privacy and are hosted on the groups' own secure servers. Indymedia, arguably the first social media platform, was run by activists in the same manner, and attempts to create other non-commercial and privacy-enhancing social networks have continued. The development of technological alternatives that reinforce autonomous and civil society-based media infrastructure has been a key part of anti-surveillance activism (Hintz and Milan, 2013). Their adoption by activist communities may have grown since the Snowden leaks began but remains limited, so far, as the vast resources available to

large corporate providers and the ease of use of their products – from Gmail to YouTube to Facebook – have meant a far more widespread uptake (Askanius and Uldam 2011; Terranova and Donovan 2013).

However, following the Snowden leaks internet companies have had to address customer concerns regarding data security, too. While they mostly enjoyed friendly relations with, in particular, the US government in pre-Snowden times, divisions between the industry sector and the state emerged after Snowden as criticism of these companies' data practices grew (Wizner, 2017). The confrontation between the FBI and Apple in early 2016 crystallized this new and troubled relation (even if momentarily), in which Apple managed to appear as protector of user interests against state intrusions. The introduction of end-to-end encryption by services such as WhatsApp demonstrated a new trend which aligned, to a degree, with the efforts of non-commercial tech activists. Campaign projects such as "Ranking Digital Rights" (https://rankingdigitalrights.org/) have advanced the focus on corporate policies by, for example, creating an "Accountability Index" that measures company commitment to user privacy and freedom of expression.

While the focus on infrastructure providers and technological development has been prominent, many digital rights campaigns have addressed the state and sought policy reform. In the UK, organisations such as Privacy International, the Open Rights Group, Big Brother Watch, Article 19 and Liberty have regularly issued statements regarding their concerns about mass data collection, have organized public debates and have lobbied legislators. As an immediate response to the Snowden leaks, these groups and others formed a coalition – Don't Spy On Us – which combined some of this advocacy work towards a common campaign. Their voice was significant in the specialized discourses around, for example, the Investigatory Powers Act – the main post-Snowden piece of UK legislative reform. They have formulated fundamental critiques of surveillance practices, but they have also, increasingly, been recognized as a legitimate participant in policy debates that holds relevant expertise. As one anti-surveillance campaigner noted: "Previously NGOs would have fought just to kill a new law and probably been unsuccessful in doing so; now they can say: here's how we can genuinely improve it and have a proper conversation with the Home Office" (quoted in Hintz and Brown 2017).

Litigation has emerged as a key strategy of policy advocacy. Campaign organisations such as Privacy International, Liberty and Amnesty International challenged GCHQ's data collection practices at the Investigatory Powers Tribunal (IPT) which decided that some of the agency's activities were unlawful. Others, such as the Open Rights Group, Big Brother Watch and Human Rights Watch brought cases against the British government before the European Court of Human Rights and the European Court of Justice. While the results of legal challenges have been mixed, they have forced governments to admit to previously secret practices and have thereby opened up avenues for policy reform (Hintz and Brown 2017).

At the intersection between policy and technology, civil society activists have also contributed to the work of institutions that define and regulate the standards and protocols of digital communication. In some of these bodies, such as the

Internet Engineering Task Force (IETF), they participate in individual capacity and based on their personal expertise, next to experts from industry and government. In others, such as the Internet Corporation for Assigned Names and Numbers (ICANN), they form specific caucuses, for example the Non-commercial User Constituency (NCUC). As technical standards and protocols typically allow some actions and disallow others, and enable some uses and restrict others, their development constitutes a latent and invisible form of policymaking and therefore places standards organisations in both a highly influential and slightly obscure position (cf., DeNardis 2009; Lessig 1999). In response to the Snowden leaks, several of these bodies started to address the vulnerabilities exposed in the revelations by setting up working groups, developing proposals on how to incorporate privacy in standards, and, in some cases, agreeing that these concerns should become a priority of standards development (Rogers and Eden 2017).

Digital rights activists and civil society-based technological developers have been influential in all these venues. Yet their efforts have largely remained within a specialized discourse and a constituency of experts. Our goal with this research was to explore to what extent activists concerned with other social justice issues have engaged with these agendas, and whether there is scope for linking these (possibly) divergent concerns.

Resistance to datafication amongst political activists

In the rest of this chapter, we therefore explore the extent to which such resistance to digital surveillance features in broader activist practices and how concerns with data are understood. This research is based on a number of semi-structured interviews carried out with political activists in the UK as part of the larger project "Digital Citizenship and Surveillance Society: UK State-Media-Citizen Relations After the Snowden Leaks". These interviews were conducted with a range of political activists, both from big NGOs as well as smaller community and grassroots organisations based in the UK, that were not specifically engaged with digital rights or technology activism, and individuals within those groups who were not specifically responsible for technical infrastructures of communication. These groups were chosen on the basis of having a more or less adversarial relationship with the state, covering a range of causes, and predominantly out of an existing network of contacts. They therefore cover a relatively wide spectrum of civil society activity. The sample consisted of 11 interviews (see Table 9.1) carried out in person (8) or on Skype (3) during March–June 2015, lasting on average 60 minutes and focused on the following themes: a) understanding and experience of surveillance; b) knowledge and opinions of the Snowden leaks; c) attitudes towards state surveillance; d) online behaviour and practices; e) changes and responses to the Snowden leaks.

In the context of the above discussion, this chapter is particularly concerned with the extent to which resistance to digital surveillance features in activist practices and agendas and how data politics more broadly is understood. We extracted prominent themes from our interviews around these issues, based on a thematic analysis that

TABLE 9.1 List of Interviews

Organization	*Orientation*
Global Justice Now (GJN)	Economic justice
Campaign Against Arms Trade (CAAT)	Anti-arms
CAGE	Anti-discrimination
Muslim Association of Britain (MAB)	Community integration
Greenpeace	Environmentalism
Stop the War Coalition (STWC)	Anti-war
Muslim Council of Wales (MCoW)	Community integration
Trade Union Congress (TUC)	Workers' rights
Anti-fracking activist	Environmentalism
ACORN	Community organizing (housing)
People's Assembly Against Austerity (PAAA)	Anti-austerity

focused on understandings of surveillance, uses of encryption software, changes in communication practices following the Snowden leaks, and attitudes towards digital rights advocacy. Below we outline key themes emerging from our interviews in relation to how anti-surveillance and data politics is situated in activist practices. In the first part we discuss general understandings of surveillance, data collection, and responses to the Snowden leaks. In the second part we move on to discuss how resistance to mass data collection in terms of encryption and advocacy around digital rights is understood and practiced amongst the activists we interviewed.

Responses to Snowden

To start with, the interviews demonstrated that the issue of state surveillance is very familiar amongst political activists in the UK, particularly due to a troublesome history of police infiltration into activist groups. Many of the activists we spoke with had either direct experiences of police infiltrating groups they were part of or they knew someone who had experienced infiltration. Digital surveillance and big data surveillance of the kind revealed in the Snowden leaks was less prominent and salient in initial descriptions of surveillance. However, many of the activists we interviewed expressed a general awareness and expectation that these activities are going on, from either corporations or state, or a combination of both. Several activists pointed to specific experiences that might demonstrate the monitoring of online activities:

> I think there's been instances where the police have turned up to our meetings or rung ahead of venues we've been using and warned the venues not to allow us to have a meeting (. . .) they're obviously keeping tabs on our Facebook activities but then that's public so you totally expect that. Similarly with Twitter . . . we're pretty sure that there's a police presence on something called Basecamp which is where we organize online.
>
> *(Anti-fracking activist)*

What was revealed in the Snowden leaks, therefore, came as little surprise to the majority of our interviewees although the scale of the surveillance programmes revealed in the documents did exceed expectation for many activists:

> I think, kind of like most people my impression is there has been a hell of a lot more going on than anyone has known about. The capabilities of the security services are much greater than anyone suspected but there is much less political and judicial oversight of this, and indeed some of this is done on a dubious legal basis.
>
> *(TUC activist)*

The lack of surprise, or the widespread expectation, of what the Snowden leaks revealed therefore also muted any direct reaction to the Snowden leaks amongst most of the activists we interviewed. With the exception of Greenpeace who reviewed and revised their communication infrastructure as an immediate and direct result of the Snowden leaks, our interviewees expressed little, if any, direct response to the revelations.[4] Rather, awareness and continued negotiation with the realities of surveillance has developed over time and the Snowden leaks fit into this longer-term consciousness instead of being transformative in and of themselves:

> I think it's about being always aware of the general threat. I don't think in fact that Snowden in particular has had an impact on a single aspect of how we work . . . In a sense he confirmed what was the sort of thing people suspected was happening anyway, but I don't think that revelation has changed anything we do.
>
> *(CAAT activist)*

Of course, this does not mean that precautions are not taken against digital surveillance as part of activist practice. Some of the people we interviewed spoke of tactics employed to circumvent different forms of digital surveillance, such as using anonymisation tools (e.g. a VPN) for researching targets, preferring face-to-face meetings for organizing actions, and using encrypted emails for sharing personal data. This also highlights how circumvention of data collection is more prominent for particular kinds of activities (e.g. internal organizational use). Overwhelmingly, however, our interviews illustrate the extent to which the dependence on digital communications, and mainstream social media in particular, for pursuing activist agendas undermines efforts to actively circumvent or resist data-driven surveillance. Activist groups use digital infrastructures that are subject to large-scale data collection for several aspects of their activities, including general awareness-raising, advocacy, mobilizing, organizing and expanding their actions and membership base, using programmes and tools integrated into social media interfaces. They do so because of the perceived reach that social media platforms afford and because activists themselves rely on the "datafication"

of social relations in order to collect data and extend networks of connections, both for organization and mobilization of activities:

> [NationBuilder] is a programme which is designed for campaign organisations. Obama used it in his campaign. Labour are using it. It basically integrates your website with a database and social media as well so sucks in social media profiles out of Facebook and Twitter and things like that.
>
> *(ACORN activist)*

> You start off by setting up a Facebook event and then the activists learn tools like the invite all app where you don't have to keep on inviting individual friends, it invites 500 at a time. So we will then spread that all around people so then you can drive the invites up to 5 or 6 thousand very quickly.
>
> *(PAAA activist)*

Such dependency on this kind of digital infrastructure in conjunction with a general awareness that communication is being monitored and stored in turn manifests itself by forms of self-regulating online behaviour. Despite their widespread use of mainstream platforms, activists noted they are cautious about not saying anything "too controversial" on social media, or choose to withdraw entirely from using social media to discuss politics:

> My advice to our people, our community, is just be careful before saying anything, before making a statement . . . and think about it, what the repercussions would be and how it could be misconstrued. So prevention is better.
>
> *(MCoW activist)*

> It can get picked up and used in a court or, partly in a court case or possibly liable. I think people are worried about liable.
>
> *(STWC activist)*

These types of concerns speak partly to the "chilling effect" mentioned above in which some online activities and communication are deterred out of a fear of the repercussions and mistrust towards the system.

Resisting data collection

Despite such concerns being expressed, the active circumvention of data-extracting technologies such as widespread uptake of encryption or anonymisation tools remained limited to just a few of the groups we interviewed, with Greenpeace expressing the most extensive and comprehensive secure communication infrastructure. Predominantly, the activists we interviewed did not use encryption or anonymisation tools as an integrated part of their communication practices. In reasoning this, we can see a number of themes emerge. Firstly, several interviewees

spoke of a perceived "lack of knowledge", insufficient technical ability and not being able to "afford" to implement alternative communication practices. These kinds of perceptions are often also combined with notions of convenience in which mainstream platforms are favoured for their familiarity and ease of use:

> We just want ease of access to be honest. Actually, I can send an email to a few thousand people and do a few other things and I don't need to spend days or weeks actually learning how to do it because I'm not very technically minded.
> *(ACORN activist)*

The question of convenience is linked to a second significant theme that emerged on this topic. Activists feel that using encryption strides against their ambitions of being an "open" and "inclusive" group or organization. Several of our interviewees emphasized the transparent nature of their activities, including also the legality of their tactics, and their wish to be a "public" movement. In positioning their response in this way, we can identify an important perception of encryption as being linked to "hidden" practices or "exclusive" forms of communication. In contrast to understanding encryption according to its established purpose as a means of security and protection, and as an enabler of both privacy and freedom of expression (Kaye 2015), the strong role of a popular "nothing to hide" discourse is evident even among activists. A number of interviewees understood such tools as contradicting or undermining their self-identification:

> We've got nothing to hide, we're not doing anything illegal and we're not doing anything that's not defendable. So you know . . . if the security services want to challenge what we're doing then we'll have that debate out in public. And anyway, I suppose at the back of our minds is that it probably wouldn't work anyway is my guess. Without spending huge amounts of time or resources.
> *(STWC activist)*

> We're having to campaign all of the time, we're not secret organisations, or organisations of tight-knit groups of people campaigning together. We are mass movements, and we are open. For us social media is great because it makes communication easy and of course we know people look at social media but our messages are not hard to get.
> *(TUC activist)*

The point here is not the choice of tactics that these groups use. Rather, the attitude expressed here demonstrates that privacy-enhancing technology is seen to be pertinent to only a particular strand of political activism and directly undermines another. Indeed, there was a prevalent sentiment in several of our interviews that being part of "mainstream" groups reduced the need for concern with digital surveillance practices. That is, resisting or circumventing data collection as an activist practice is predominantly confined to those engaging in "radical" political activism.

Consequently, this might also deter those "in the middle" from becoming more "radical", making "people more cautious" (ACORN activist), and thereby keep the mainstream "in check". This sentiment is reasoned not just in terms of the legality of tactics that different activist groups employ, but also in terms of the perception of their own influence and the extent to which they see themselves as adversarial to the state (our sample includes a variation of activists in this regard). In this sense, only activists who understand themselves as being sufficiently of interest to the state feel the need to concern themselves with data-driven surveillance as an issue or integrate secure technologies into their practices.

Such perceptions also extend to activists' engagement with advocacy on legislation relating to privacy or digital rights issues more broadly. Although solidarity and support of the cause was expressed across the board, most activists we interviewed did not see themselves or the organisations and groups they are part of as being actively engaged with issues relating to digital rights, such as privacy or data protection. Rather, despite mentions of some informal links with organizations such as Privacy International and Statewatch[5], most of the activists we interviewed made a distinction between their own activist work and that of technology activists and digital rights groups:

> Some people focus on things like surveillance and some people focus on the workplace, some people do community things.
>
> *(ACORN activist)*

> I think there are organisations that are doing that work already and it's for us to be knowledgeable and a bit of a step ahead of the game, but I don't think it's for us to campaign on surveillance.
>
> *(Anti-fracking activist)*

Despite a general critique of mass data collection, resisting it actively does not feature in activists' own agendas and is instead "out-sourced" to expert communities. In this sense also, resistance to data collection was not seen as providing a base for a broader movement, but rather an issue in which you need to "specialize" (PAAA activist).

"Data justice" and the bridging of activism(s)

Our interviews with activists illustrate that a general awareness and expectation of surveillance is prevalent amongst activist communities in the UK, but concerns with data-driven surveillance of the kind revealed in the Snowden leaks remain somewhat marginalized in activist perceptions and practices. Rather, the entrenched dependency on mainstream communication platforms that are predominantly insecure provide an environment for activist practices in which it is seen as difficult and problematic to engage in resistance to data collection either through technological means or in terms of protest and advocacy for

greater privacy and data protection. More generally, we can identify a "disconnect" between concerns with data-driven surveillance and other (broader) social justice concerns.

How, then, might we address this disconnect? Aouragh et al. (2015) argue that the "division of labour" between what they label "tech justice" and "social justice" activists emerges partly from the socio-technical practices that have been advanced in secure communication campaigns in which there is a distinct user-developer dichotomy that places the onus on the (individual) "user" to protect themselves (identifying risks using "threat modeling") with tools provided by the "developer". Similarly, Kazansky (2016) found, based on her experience with providing information security training for human rights activists, that training is often designed towards the individual user rather than as a collective project that considers the enabling social structures needed for secure communication to become an integrated activist practice. This speaks to the shortcomings identified by Ruppert, Isin and Bigo (2017), with the common atomism prevalent in views on data politics and the onus on immediacy that pervades responses. That is, the view of the internet as addressed to atomized individuals who then need to protect themselves against the immediacy of a threat engendered. This view, they argue, is based on the ontological premise of "hyper-individualism" in which the addressee is "the atomized subject whose data is individualized rather than understood as a product of collective relations with other subjects and technologies" (Ruppert, Isin and Bigo 2017, 3) Policy reform advocacy, meanwhile, does not address individual users but, nevertheless, the specific audience of policymakers and thereby erects different boundaries, based on issue-specific expertise and discourse (Hintz and Brown 2017).

Such approaches, Aouragh et al. contend, configure modes of delegation that actually come to negate possibilities for overlaps between different justice claims and reproduce "a perhaps unintended hierarchy based on traditional models of production" (2015, 216). Drawing on their research with "tech justice" activists, they therefore argue for connecting security engineers with the language of collective action within a political project and, more broadly, for dissolving the perceived divisions of justice claims that persist between these activist camps.

Building on this ambition, we want to further advance the debate based on our research with "social justice" activists by suggesting a broader framework that may allow us to develop a more integrated understanding of data collection in relation to social justice agendas. As outlined above, the terms upon which resistance to surveillance has predominantly been approached have placed data debates within the parameters of particular expert communities, namely technology activists and digital rights groups. This techno-legal framing of resistance, although partly dictated by the activist opportunity structures currently available, limits our understanding of the implications of these data-driven practices that underpin contemporary surveillance and dilutes their politicized nature. The consequences of this limitation include, for example, a relatively uncritical perspective among digital rights advocacy communities on "targeted" surveillance which is often seen as a benign alternative to

indiscriminate "mass" surveillance but abstracts from the experiences of minority communities and political activists as typically targeted groups (Gürses, Kundnani and Van Hoboken 2016). Further, this limited perspective may lead to a perception of industry surveillance as largely politically benevolent and the turn to the tech companies of Silicon Valley as our "protectors" in the counter-surveillance struggle, armed with PR-friendly encryption tools. Moreover, a techno-legal framing of the issue risks masking the struggles through which people come to be governed by data (Ruppert, Isin and Bigo 2017). As Gürses, Kundnani and Van Hoboken (2016) suggest, these problematic positions point to the need for a political analysis as our starting point for countering the systems of data collection and use that have been developed; one that simultaneously broadens the discussion beyond the narrow confines of techno-legal parameters and speaks to the concerns of activists across technology and social justice camps.

As part of such an analysis, we advance the notion of "data justice" as a way to highlight the place of data-driven surveillance, and related big data decision-making and governance, in conceptions of social justice. Whilst recognizing the procedural inference in the term "justice", by data justice we are referring to the implications that data-driven processes at the core of surveillance capitalism have for the pursuit of substantive social and economic justice claims. This, we suggest, encompasses both the targeting of surveillance against activists leading to repression, self-censorship and chilling-effects in the organization, mobilization, and pursuit of social justice as well as the role of data collection in (new) forms of governance that shape society in line with particular political and economic agendas. As Andrejevic (2015) has outlined, the nature of the surveillance programmes revealed in the Snowden leaks are intimately linked to a system of economics and a state-corporate interest not necessarily in individual people, but in detecting and predicting patterns, profiling and sorting groups. Big data surveillance brings up issues not just of privacy, but also of social sorting and preemption (Lyon 2014) and is generative of new power relations and politics (Ruppert, Isin and Bigo 2017). Although much more difficult to ascertain in concrete terms, this has significant implications for people's lives and the society they will live in. Data justice as a framework is intended to guide a research trajectory and types of activity that bring out and underscore this politics of data and the implications of these practices for substantive social justice claims. This is obviously a bigger task beyond our current scope, but here we can highlight some questions that have already planted the seeds for further illumination and advancement of our understanding of resistance to datafication in this regard.

Whilst "data justice" as a concept and framework is still in nascent form, different interpretations are being advanced that share a concern with outlining data in relation to structural inequality and social (in)justice (Heeks 2017; Heeks and Renken 2016; Hintz, Dencik and Wahl-Jorgensen 2018; Newman 2015; Taylor 2017). Grassroots groups and social justice campaigns have started to apply this more comprehensive approach to datafication and, in some cases, have done so within a "data justice" framework. For example, the Detroit Digital

Justice Coalition (http://detroitdjc.org) has worked with local residents in identifying potential social harms that may emerge through the collection of citizen data by public institutions. In particular, they are concerned with the criminalization and surveillance of low-income communities, people of colour and other targeted groups. As a result, they have developed a set of guidelines for equitable practices in collecting, disseminating and using data in relation to social and historical context. The US/Canadian Environmental Data & Governance Initiative, EDGI (https://envirodatagov.org/), has preserved vulnerable scientific data in the aftermath of the US election of Trump in 2016 and, in the process, has developed a deeper understanding of the politics, generation, ownership and uses of environmental data. Their perspective on "environmental data justice" "brings together the concerns of the emergent area of data justice with the long-standing principles of environmental justice" (https://envirodatagov.org/towards-edj-statement/). The local administration in Barcelona, meanwhile, has been actively developing alternative infrastructures, with an emphasis on decentralized technologies that are designed for more citizen-led and participatory platforms and where ownership of data belongs to the citizens. Such ideas are also prevalent in the growing "platform cooperativism" movement that sets out to challenge the dominance of contemporary platform capitalism in order to create a fairer future of work in a digital economy by building on the values of cooperativism.

These sorts of initiatives speak partly to the framework we are proposing here by reframing data debates to consider how digital infrastructures and data-driven processes have implications for broader society beyond individual privacy. We want to further progress this agenda by suggesting that "data justice" can provide a conceptual foundation for exploring how mass data collection implicates different understandings of social justice as well as a potential action-building tool for addressing such implications. This requires us to further examine the ideological basis of data-driven processes, situating this form of governance within a political agenda that extends to particular conceptions of society and the demarcation of "good" and "bad" citizens. Furthermore, it leads us to scrutinize the interests and power relations at play in 'datafied' societies that enfranchise some and disenfranchise others, highlighting also forms of exclusion and discrimination. Moreover, it requires us to stipulate how society is and ought to be organized in relation to digital infrastructures – on social, political, economic, cultural and ecological terms – that can consider and develop the meaning of justice in this context. This includes questions of how to think about notions such as security, autonomy, dignity, fairness and sustainability in a data-driven society and make us ask what, for example, the implications are for community cohesion and discrimination; for welfare and inequality; for workers' rights; or for the environment, for poverty, and for conflict. Most importantly, advancing this agenda transforms data-driven processes from a special-interest "issue" into a core dimension of social, political, cultural, ecological and economic justice, and thus responds to the central position of data in contemporary capitalism.

By advancing the framework of "data justice" our point is to illustrate how the relationship between political activism and surveillance is not one in which activists are only at risk for expressing dissent, but one in which the very infrastructures of surveillance (big data) have direct consequences for the social justice claims they are seeking to make. Data justice integrates the concerns with the collection, use and analysis of data with activists' agendas, not just to protect themselves, but also to achieve the social change they want to make. As such, this may offer an opportunity to bridge the current "disconnect" we have found in anti-surveillance resistance and provide resources for a political and social movement that can engage with data debates beyond techno-legal solutionism. It may also contribute to the call for a conception of data subjects more in relation to rights-claiming citizens (Ruppert, Isin and Bigo 2017). This, we would argue, is urgently needed in the shift towards data-driven forms of governance rooted in surveillance capitalism.

Conclusion

The need to engage with data politics in a way that situates concerns with data-driven processes within a broader framework of social justice is becoming increasingly prevalent, and is being approached from a number of different angles.[6] In this chapter we have addressed this topic by looking specifically at attitudes and practices pertaining to resisting data-driven surveillance. The Snowden leaks constitute an important moment for exploring these questions as they provided substantial evidence for the extent of the collection and use of digitally-generated data (or big data) and illustrated the intricate relationship between the infrastructures of our everyday technologies and emerging forms of governance and control. Pertinent debate, activity and advocacy has flourished in response to the Snowden leaks, opening up opportunities for many existing technology- and digital rights-concerned communities to mobilize, expand and influence political processes and social attitudes. However, due to the dominant political culture and opportunity structures available to active participants in the resistance against surveillance, debates on data collection and use, and critical engagement with data politics more broadly, have struggled to move beyond the participation of particular expert communities. A concern with digital surveillance, in this context, has come to be viewed as a "specialist" issue in which achieving "tech justice" is predominantly centred on technical and legal solutions relating to privacy and data protection. We have seen this in our research on attitudes and practices amongst political activists engaged in broader social justice issues, from environmentalism to labour justice to anti-discrimination, who have predominantly come to view data-driven surveillance as an issue that does not substantially feature on their agenda.

Rather, what emerges in the broader ecology of civil society pursuits of justice, is a kind of "disconnect" between those concerned with technology issues and those concerned with social justice issues as two separate camps. Of course, we recognize that this comes partly from the necessity to set priorities and focus on particular

topics when activist energies and resources are frequently limited. However, we argue that the nature of surveillance revealed in the Snowden leaks speaks to an urgent need to broaden the parameters for how data collection and use has been understood and discussed that implicates activists across the tech and social justice camps, collectively. The ability to monitor, record and store digital transactions on a massive scale creates an environment that substantially limits the possibilities for dissent and protest, whether through self-censorship, chilling-effects or active repression. Moreover, however, it constitutes a form of governance that is rooted in and simultaneously advances particular social, economic, and political agendas that enfranchise some whilst disenfranchising others, and prioritizes certain ways of organizing society at the expense of others.

By introducing the notion of "data justice" in this chapter we want to contribute to the shift and broadening of our understanding of the role of data-driven processes in contemporary society. By advancing data justice as a framework for debate and research, we want to set the parameters for a discussion on datafication that can illuminate the implications for social justice, both in terms of the conditions for communicating autonomously and practicing dissent as well as the social and economic (in)justices that are produced by this form of governance (and, therefore, what might be the possible alternatives). Referring to "data justice" recognizes the political economy of the system that underpins the possibilities for extensive data collection and use, whilst drawing attention to the political agenda that is driving its implementation. This, we argue, comes to impact on political activists and their pursuits of social justice in significant ways and provides an impetus for a broad collective movement to engage in pertinent data-related debates. Such a collective approach is needed, we suggest, in light of a shift to surveillance capitalism in which the collection, use and analysis of our data increasingly comes to shape the opportunities and possibilities available to us and the kind of society we live in.

Notes

The research for this chapter was funded by the Economic and Social Research Council as part of the project "Digital Citizenship and Surveillance Society: UK State-Media-Citizen relations after the Snowden leaks".

1 Note that a version of this was originally published in *Big Data & Society*.
2 The chapter is based on research carried out for the collaborative research project "Digital Citizenship and Surveillance Society: UK State-Media-Citizen relations after the Snowden leaks" at Cardiff University funded by the Economic and Social Research Council, the first comprehensive review of the implications of the Snowden revelations from a UK perspective.
3 Details of the revelations can be found at The Snowden Archive: http://www.cjfe.org/snowden
4 We were later informed that CAGE has also significantly changed their communication infrastructure, but this development happened after our interview period.
5 Interestingly, also, CAGE participated for the first time in the large hacker convention Chaos Communication Congress in December 2015.
6 See, for example, the 'Data Justice Conference' that took place in Cardiff in the United Kingdom in May 2018: https://datajusticelab.org/data-justice-conference/

References

Andrejevic, M. 2015. Keynote plenary at the conference 'Surveillance and Citizenship', Cardiff, 19 June.

Aouragh, M., Gürses, S., Rocha, J. and Snelting, F. 2015. Let's first get things done! On division of labour and techno-political practices of delegation in times of crisis. *The Fibreculture Journal*, 26: 208–235.

Askanius, T. and Uldam, J. 2011. Online social media for radical politics: climate change activism on YouTube. *International Journal of Electronic Governance (IJEG)*, 4(1/2): 69–84.

Bakir, V. 2015. Veillant panoptic assemblage: Mutual watching and resistance to mass surveillance after Snowden. *Media and Communication*, 3(3): 12–25.

della Porta, D. 1996. Social Movements and the State: Thoughts on the Policing of Protest. In D. McAdam, J. McCarthy, and M. N. Zald (eds.), *Comparative Perspectives on Social Movements. Political Opportunities, Mobilizing Structures, and Cultural Framing*. Cambridge/New York: Cambridge University Press, 62–92.

DeNardis, L. 2009. *Protocol Politics: The Globalization of Internet Governance*. Cambridge: MIT Press.

Earl, J. 2003 Tanks, tear gas, and taxes: Toward a theory of movement repression, *Sociological Theory*, 21(1): 44–68.

Greenwald, G. 2014. *No Place to Hide: Edward Snowden, the NSA and the surveillance state*. London: Hamish Hamilton.

Greenwald, G. & Gallagher, R. 2014. Snowden documents reveal covert surveillance and pressure tactics aimed at WikiLeaks and its supporters, The Intercept, February 18, available at: https://theintercept.com/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/ (last accessed March 7th, 2016).

Gürses, S., Kundnani, A. and Van Hoboken, J. 2016. Crypto and empire: the contradictions of counter-surveillance advocacy. *Media, Culture & Society*, DOI: 10.1177/0163443716643006.

Hampton, K.N., Rainie, L., Lu, W., Dwyer, M., Shin, I., and Purcell, K. 2014. 'Social media and the 'spiral of silence''. Pew Research Center, Washington, DC. Retrieved from http://www.pewinternet.org/files/2014/08/PI_Social-networks-and-debate_082614.pdf.

Harding, L. 2014. Edward Snowden: US government spied on human rights workers, *The Guardian*, April 8.

Heeks, R. and Renken, J. 2016. Data justice for development: what would it mean? *Information Development*. Available at: https://doi.org/10.1177/0266666916678282.

Heeks, R. 2017. A structural model and manifesto for data justice for international development. *Development Informatics Working Paper Series*, No. 69.

Hintz, A. and Brown, I. 2017. Enabling digital citizenship? The reshaping of surveillance policy after Snowden. *International Journal of Communication*, 11: 782-801.

Hintz, A., Dencik, L. and Wahl-Jorgensen, K. 2018. *Digital Citizenship in a Datafied Society*. Cambridge: Polity Press.

Hintz, A. and Milan, S. 2013. Networked collective action and the institutionalised policy debate: Bringing cyberactivism to the policy arena? *Policy & Internet*, 5(1): 7–26.

Kaye, D. 2015. Report on encryption, anonymity, and the human rights framework. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. 22 May 2015. Available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

Kazansky, B. 2016. Digital security in context: Learning how human rights defenders adopt digital security practices. Project report. Available at: https://secresearch.tacticaltech.org/media/pages/pdfs/original/DigitalSecurityInContext.pdf?1459444650 (last accessed 21 May 2016).

Kitchin, R. 2014. *The Data Revolution*. London: Sage.
Leistert, O. 2012. Resistance against cyber-surveillance within social movements and how surveillance adapts, *Surveillance & Society*, 9(4): 441–456.
Leistert, O. 2013. *From Protest to Surveillance – The Political Rationality of Mobile Media*. Frankfurt Am Main: Peter Lang.
Lessig, L. 1999. *Code and other Laws of Cyberspace*. New York: Basic Books.
Lovink, G and Rossiter, N. 2015 Network Cultures and the Architecture of Decision. In Dencik, L. & Leistert, O. (eds.) *Critical Perspectives on Social Media and Protest: Between Control and Emancipation*. London: Rowman & Littlefield International: 219–232.
Lubbers, E. 2012. *Secret Manoeuvers in the Dark: Corporate and Police Spying on Activists*. London: Pluto Press.
Lubbers, E. 2015. Undercover Research: Corporate and police spying on activists. An introduction to activist intelligence as a new field of surveillance. *Surveillance & Society*, 13(3/4): 338–353.
Lyon, D. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham and Philadelphia: Open University Press.
Lyon, D. 2014. Survellance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, July–December: 1–13.
Lyon, D. 2015. *Surveillance After Snowden*. Cambridge and Malden, MA: Polity Press.
Mann S 2005. Sousveillance and cyberglogs: A 30-year empirical voyage through ethical, legal and policy issues. *Presence: Teleoperators and Virtual Environments*, 14(6): 625–646.
Mann, S. and Ferenbok, J. (2013) New Media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance & Society*, 11(1/2): 18–34.
Marthews, A. and Tucker, C. 2015. Government surveillance and internet search behaviour. *Available at SSRN:* http://ssrn.com/abstract=2412564.
Massumi, B. 2015. *Ontopower: War, Powers, and the State of Perception*. Durham and London: Duke University Press.
Newman, N. (2015) Data Justice: Taking on Big Data as an Economic Justice Issue. Report. Available at: http://www.datajustice.org/blog/data-justice-report-taking-big-data-economic-justice-issue
O'Neill, P. H. 2015. The state of encryption tools, 2 years after Snowden leaks, *The Daily Dot*, 20 June. Available at: http://www.dailydot.com/layer8/encryption-since-snowden-trending-up/ (last accessed 4 September 2016).
PEN. 2013. *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*. New York: PEN American Center, available at: http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf (last accessed 7 March 2016).
Penney, J. 2016. Chilling effects: Online surveillance Wikipedia use. *Berkeley Technology Law Journal*, Available at SSRN: http://ssrn.com/abstract=2769645.
Privacy International & Amnesty International. 2015. Two years after Snowden: Protecting human rights in an age of mass surveillance. Report, available at: https://www.privacyinternational.org/sites/default/files/Two%20Years%20After%20Snowden_Final%20Report_EN_0.pdf (last accessed 7 March 2016).
Raley, R. 2013. Dataveillance and Countervailance. In: Gitelman, L. (ed.) *'Raw Data' is an Oxymoron*. Cambridge, MA: MIT Press: 121–146.
Rogers, M. and Eden, G. 2017. The Snowden disclosures, technical standards and the making of surveillance infrastructures. *International Journal of Communication*, 11: 802–823.
Isin, E. and Ruppert, E. 2015. *Becoming Digital Citizens*. Lanham: Rowman & Littlefield.
Ruppert, E., Isin, E. and Bigo, D. 2017. Data politics. *Big Data & Society*. July– December: 1–7.
Smith, D. and Chamberlain, P. 2015. *Blacklisted: The Secret War Between Big Business and Union Activists*. Oxford: New Internationalist.

Taylor, L. 2017. What is data justice? The case for connecting digital rights and freedoms. *Big Data & Society*, 4(2).

Terranova, T. and Donovan, J. 2013. "Occupy Social Networks: The Paradoxes of Corporate Social Media for Networked Social Movements." In Lovink, G. and Rash, M. (eds.) *Unlike Us Reader: Social Media Monopolies and Their Alternatives*. Amsterdam: Institute of Network Cultures, 296–311.

Uldam, J. 2016. Corporate management of visibility and the fantasy of the post-political: Social media and surveillance, *New Media & Society*, 18(2): 201–219.

Varian, H. R. 2014. Beyond Big Data, *Business Economics*, 49(1): 27–31.

Wizner, B. 2017. What changed after Snowden? A US perspective. *International Joutnal of Communication*, 11: 897–901.

Zuboff, S. 2015. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30: 75–89