Civil Society in an Age of Surveillance: Beyond techno-legal solutionism?

As many recent revelations – from the Snowden leaks to WikiLeaks' Vault7 files – have shown, the monitoring and analysis of data traffic is now an integral part of government and corporate practice. The sources of data range from online communication, social media activity and mobile phone locations through to 'smart' household devices, health trackers, and sensors in 'smart' cities. The 'datafication' of our lives, i.e. the collection and processing of communication, health, location, etc. as data points, has increased the traceability and visibility of citizens and advanced the ability for a range of different institutions to monitor us. While this has implications for citizens in general, it presents particular challenges for civil society actors who are actively engaged in advancing and shaping social and political change. In an age of data-driven surveillance, how is civil society impacted? And how have activists sought to resist it?

With rapid technological development, both the means of collection and the uses of data are expanding rapidly. Vast amounts of personal data are now collected and shared across social media and digital platforms, smart homes detect our presence and movements, and smart TVs can listen to our conversations. Such data is collected and analysed by companies, shared and sold by the data industry, and used by state agencies. Citizens are increasingly categorized and profiled according to data assemblages, for example through data scores used in the criminal justice system or by social credit scores, as developed in China. The purpose of such scores is to predict future behaviour and allocate resources and eligibility for services (or punishment) accordingly. Data analysis thus denotes a particular mode of governance, one in which the prevailing logic is to predict human behaviour as a means to both manage populations and produce revenue - an information order described as 'surveillance capitalism.'

The transformation towards data-based governance, and the historic moment of the Snowden leaks, have highlighted key challenges for the protection of citizens in a datafied environment. Policies pertaining to data collection, however, have hardly kept pace with technological change and have often empowered business and the state rather than the citizen. While data protection was strengthened in the US, with the USA Freedom Act, and in the European Union through the General Data Protection Regulation, surveillance capabilities of the state were expanded in countries like France, Germany and the UK. In the UK, particularly, the Investigatory Powers Act of 2016 makes the state's surveillance capabilities more transparent, but it allows for a wider range of data collection and analysis than before and, arguably, than anywhere else in the Western world.

While the Snowden revelations and the increasing use of 'smart' technologies point to the *mass* collection of data and thus to the implications for all citizens, certain groups and actors remain particularly vulnerable in a surveillance-based society. Unsurprisingly, this includes key parts of civil society engaged in political activism, both in institutionalised form and more broadly. Documents from the Snowden revelations showed that US and UK intelligence agencies spied on international organisations such as Medecins Du Monde (Doctors of the World), UNICEF, Amnesty International and Human Rights Watch, members of Anonymous, and anyone politically engaged enough to visit websites such as Wikileaks. Both law enforcement and corporations now routinely use social media to collect information about activists and protesters, and we are increasingly moving towards a mode of governance based on trying to pre-empt certain activities from happening or from groups getting together.

A key consequence of this may be a so-called 'chilling effect' that stifles the possibilities for challenging institutions of power and advocating for social change. Although the theory of 'chilling effects' has been difficult to prove empirically, it is widely recognised that people may be deterred from engaging in certain legal (or even desirable) activities if they fear they are under observation. A

study by the PEN American Center, for example, found that writers were engaging in self-censorship as a result of the Snowden revelations. Other 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, a decline in page views of Wikipedia articles relating to terrorism, and a 'spiral of silence' in surveillance debates on social media. For activists and civil society campaigners who express dissent and fight for social and political change, pervasive surveillance may lead to concerns for their own privacy and security, but also has practical implications for their efforts of organizing and mobilizing. In the words of Glenn Greenwald, in a culture of pervasive surveillance, 'merely organizing movements of dissent becomes difficult when the government is watching everything people are doing.' Beyond such practical concerns, surveillance fundamentally shifts the power balance between activists and the state (as well as large businesses) by providing the latter with powerful tools to monitor and target potential adversaries.

The sheer ubiquity of surveillance infrastructures and their embeddedness in ordinary aspects of social, political and cultural participation make it difficult for citizens to think they can be challenged, despite prevalent unease and concerns with the current system. The institutional and discursive normalisation of data collection across everyday life often leads to a widespread resignation to status quo, partly driven by a sense of pragmatism and a perceived lack of alternatives. We have referred to this as a condition of surveillance realism (drawing on Mark Fisher's concept of capitalist realism) in which the normalisation of surveillance limits the possibilities of imagining another way of organising society. This also extends to politically-active members of society. In carrying out research with activist groups, we found that even amongst civil society organizations there is a relative acceptance and expectation of pervasive monitoring. Some groups negotiate the risk of this in relation to their own activities and the level of threat they think they pose to the state, finding safety in operating within an accepted mainstream framework. In that sense, a 'chilling effect' is certainly evident within civil society.

Of course, whilst these feelings of disempowerment have stifled opposition, we have also seen a growing effort amongst particular pockets of civil society to directly confront and challenge the existing surveillance regime. Digital rights groups and technology activists have jointly advanced key points of advocacy and resistance. The development and dissemination of privacy-enhancing tools such as the TOR browser, the GPG email encryption system and the encrypted phone and text messaging software Signal have picked up since the Snowden revelations and provide mechanisms of secure online communication for, among others, civil society groups. 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' and the Tactical Tech Collective's 'Security in a 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. Technical solutions to surveillance have included, furthermore, the development of self-organised communications infrastructures as alternatives to corporate services such as Google and Facebook. Groups like Riseup.net, amongst others, have offered mailing lists, blog platforms and collaborative online workspaces that protect user privacy and are hosted on the groups' own secure servers.

Alongside this, challenges advanced by digital rights and civil liberties groups have targeted 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 surveillance, 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 has combined some of this advocacy work towards a common campaign. Their voice has been significant

in the specialized discourses around, for example, the draft Investigatory Powers Act. Some campaign organizations have been involved in litigation, for example by challenging British surveillance practices at the Investigatory Powers Tribunal (IPT) and the European Court of Justice.

Digital rights activists and civil society-based technological developers have been influential in all these venues. But in an atmosphere of surveillance realism, the terms upon which they have had to engage with the issue of surveillance have also been limited. They have struggled to go beyond individualised responses, a specialized discourse and a constituency of experts. Anonymization and encryption tools put the onus on the individual to secure their own privacy. Policy reform advocacy may move beyond individual users but maintains a focus on the specific audience of policymakers, based on issue-specific expertise and discourse. Meanwhile, concerns with data-driven surveillance remain marginalized in public perceptions and practices, including amongst political activists, partly because of a continued dependency on insecure communication platforms that are perceived to be more accessible and have a wider reach.

Part of the challenge in the civil society resistance to surveillance and the consequences of datafication lies in overcoming the techno-legal solutionism that has dominated much of the debate and, instead, feed into a broader political movement on the role and nature of 'big data' and other technical artefacts (AI, IoT etc.) in society. This means framing the debate beyond concerns with individual privacy and engaging different parts of civil society with the issue. Highlighting broader societal implications and power relations that emerge from datafication leads, we believe, to an understanding of what we refer to as 'data justice' that addresses the intricate relationship between datafication and social justice. We see this as a growing response within civil society, as it becomes increasingly clear how the ubiquitous collection and processing of data across social life not just erodes privacy, but can come to marginalise, discriminate, suppress and exploit individuals and communities in new and challenging ways. Such developments demand collectivist responses that engage a broad range of stakeholders, across civil society, in order to break through surveillance realism and begin to imagine alternative ways of organising society and articulate new deals on data.

Lina Dencik and Arne Hintz are Senior Lecturers at Cardiff University's School of Journalism, Media and Cultural Studies where they serve as Co-Directors of the Data Justice Lab.