Our digitally mediated society

Robin Mansell[1]

This article focuses on how we imagine our digitally mediated society and on whether alternative worlds or pathways are possible (Mansell, 2012). What is happening to the public's right to access information, to the right of citizens to be free from surveillance, and to their privacy, as a result of the growing technical ability to track, analyse and act on data? Have dominant trends in digitally mediated surveillance, power and practice congealed, or, can they be better aligned with citizen interests in social democracy and a good society? What algorithms are, who or what governs them, and what values are embedded in them, are questions that are crucial to answer. Research on algorithms, artificial intelligence and their applications is a growth industry and is attracting a lot of research funding. Researchers treat algorithms as a sensitising concept, as active agents, or as black boxes that need to be unpacked. Some work is focusing on the consequences of algorithms for social sorting and discrimination, on whether users are aware of them and on whether they are politically accountable through governance measures.

It is essential to locate these questions in the context of what kind of society is desirable and for whom. Surveillance using today's networks and algorithms is obviously connected with power relationships. These relationships are understood differently by algorithm makers and their corporate and state overseers, as compared to many social science scholars and internet users. Common to many perspectives on the growing use of

[1] An earlier version of this essay was presented as a keynote at the International Communication Association Conference, Fukoka, 13th June 2016 and published in modified form at openDemocracy, 20th July 2016 (https://www.opendemocracy.net/digitaliberties/robin-mansell/surveillance-power-and-communication)

algorithms is a core societal problem. This is an increasing fascination with – and attachment to – the quantifiable. Even when the algorithm is treated as a sensitising concept, research is often very algorithm-centric, and it is at risk of forgetting why questions about power, surveillance and algorithms matter. They matter because of their relation to very big social, political and economic problems.

Wittgenstein said that 'we cannot [...] say what we cannot think' and in this sense algorithms are both effective and unfathomable. Most people, most of the time, do not think about what is happening when they go online and algorithms are at work. Bucher's (2016) work shows that we can imagine that something is happening, but that it is almost impossible for us to think about what choices are being made for us and by whom. For algorithm makers, however, algorithmic computation is mainly about patterns of data. The problems are about prediction, with the aim of rubbing out the foibles of human beings, and of optimising the quantification of behaviour.

A society mediated by algorithms

Algorithms make digitally mediated surveillance, or watching over us, technically very easy. Applications can support and mitigate the damage of disasters, they can help protect people in public spaces, they can help signal health risks and, in that sense, they combat disease. They also help in monitoring climate change. Algorithms are being used to help companies to boost profits and countries are (in some cases) experiencing economic growth as a result – a claim that can be verified. Algorithms also support surveillance or undersight, as Mann (2003) and others call it; and so algorithmic based watching from below can support a radical politics of resistance.

The digitised world is becoming more inclusive by some measures. Some 914 million people have at least one international connection on social media such as Facebook, Twitter, LinkedIn and WeChat and most are using it for electronic commerce. Global data flows raised the world's GDP by more than 10 per cent to USD 7.8 trillion in 2014. Small businesses can become 'micro-multinationals' and around 12 per cent of global goods trade is done via electronic commerce on platforms like Alibaba, Amazon, eBay, Flipkart, and Rakuten. Company platforms and automated processes are operating at hyperscale and, thanks to Airbnb, Agoda and TripAdvisor, data analytics-driven decision-making is the order of the day. The Internet of Things is feeding this and companies are investing to improve productivity, innovation and customer retention.

Digital services are becoming central to the majority of people's lives in the Global North. Global flows of data are becoming more inclusive of people in the Global South, although McKinsey notes that lagging countries are catching up extremely slowly (Manyika et al., 2016). Some six billion people do not have high speed broadband, some four billion do not have Internet access at all, and some two billion do not have a mobile phone. With the growth of the big data ecology, new types of risk are commanding public attention, but data processing using algorithms is expected to come to the rescue if power grids fail, financial crises worsen, or there are information leaks. For McKinsey and some other corporate analysts, the biggest sources of vulnerability for society are disgruntled employees, criminals, political activists, and other countries, not the algorithms themselves.

The rate of inclusion and the penetration of digital technology and statistics on gaps cannot be the sole criteria for deciding whether the pathway towards an algorithmic society is a good one. Alongside the spread of algorithms, inequality is growing within countries, even as digital divides start to close. Countries are facing economic instability, bubbles and financial crashes. Poverty, lack of housing and poor water sanitation and asylum seeking, are all too visible. For some, these are symptoms of calculable risks that can be managed by relying on algorithms and data analytics.

We have a society that increasingly privileges quantification. We encounter big data and algorithmic computing as if it is novel in a way that is similar to the way we responded several decades ago to the birth of the digital revolution and the information society. We encounter it as new partly because debate about big data and algorithms is being hyped by powerful actors as a solution to big social problems. There is no co-ordinated or organised conspiracy, but there is a campaign to assure people that, whatever the functions of today's algorithms, they are designed to keep us safe, happy, and make us wealthier. Attention in the media to the role of the state in war, migration and terrorism threats is bringing digital monitoring and algorithms more prominently into the public eye. This, to some extent, is deflecting citizens' attention away from threats to their privacy and their rights to freedom of expression – at least for a while.

The catch phrase, 'big data', is new, but data processing itself is not. What is new to the public realm is the move into behavioural analytics and learning algorithms where the analytics may occur beyond the knowledge of the algorithm makers. It is this possibility, which is deepening the fascination with the quantification of everyday life. MIT's new AI-based Cyber Threat Analysis Framework, for example, aims to ramp up the speed and accuracy of analytics to find threats in the Dark Web by scanning for malware releases and ransom-ware tools. The technology is intended to be used to identify new threats and observe the activities of hackers, but some experts question both the effectiveness and the human rights implications of the algorithm-driven techniques – they are not a 'silver bullet'. The digital communications skills gap generally is big and there is much debate about deskilling and up-skilling. Few people have the knowledge to understand what an algorithm is or what it means to do data analytics. Skilled people in areas like artificial intelligence, data management, data quality control, and data visualisation are short in supply, but debate about what to do about this is not new and solutions continue to fall short of aspirations especially for the general population.

We are moving ever more rapidly towards a computational theocracy as Ian Bogost suggests in the US *The Atlantic* 2015. The cathedral or temple of computation is a societal issue that is becoming more problematic alongside growing social and economic inequality. The challenge isn't only whether digital communication – based on algorithmic computation – is exploitative *or* liberating, inclusive or excluding. It is to keep in mind that, although it may seem as if algorithms are the drivers of society and that these developments are negating human agency, human agency still matters. All these developments are influenced by norms and rules of governance and these are humanly constituted.

Governing computational black boxes

The term governance is often used loosely, but it refers to the rules, norms, and practices that are accepted or resisted in a given society. Governance influences the kind of world that is being borne; it is about the fundamentals of life, the quality of people's lives, and whether, by any measure, societies aspire to be good societies – societies that are inclusive, respectful, and enabling. Governance involves legislation and policy and it is needed to make sure that the algorithms that are currently signposting Twitter tends and the most read press articles or supporting surveillance by the police are as transparent as possible. It would be useful to understand computational biases, who or what algorithms hide, and when they are successful and when they fail. But governance is also about more subtle issues. Algorithms involve networked information assemblages – 'institutionally situated code, practices, and norms with the power to create, sustain, and signify relationships among people and data through minimally observable, semi-autonomous action' (Ananny, 2016: 93). In this sense, algorithms can govern by structuring future possibilities. When the results they produce are treated as if they are certain, our capacity to think about alternative worlds and development pathways is discouraged because these assemblages are disciplining technologies and they discipline the mind.

If governance is the 'the ensemble of techniques and procedures put into place to direct the conduct of men and women and to take account of the probabilities of their action and their relations' (Lazzarato, 2009: 114), then we need to understand why it is acceptable to so many that machine learning or algorithmic computation are set to become an even greater part of our lives in the future. Algorithmic 'calculative practices are established as legitimate (or true)' (Introna, 2016: 39) increasingly, and they are being internalised. But, while they may be more effective in producing self-governing subjects than earlier technologies, they are not 100 percent effective. We need to remember that algorithms do not make a society. It is human beings in their institutional settings who make the world. The biggest governance challenge today in this area is not so much the algorithm itself, but the assumption that human conduct is predictable enough to allow human beings to defer to machine-driven decisions. When such decisions exacerbate inequality, unfairness, and discrimination, we are not on a pathway aligned with most people's ideas of a good society.

Resistance to the algorithmic computational drama, as it has been called, is definitely needed. The black box that needs unpacking is not the inner workings of an algorithm – although this is a nice theoretical challenge. A different black box should be the principal concern. In digitalisation's earlier history, a Stanford University economist who studied technological innovation said that researchers should look inside the black box of technology (Rosenberg, 1982), but he meant research should focus on points of economic or political power and control. This means that instrumental social science treatments of algorithmic black boxed power need to be challenged with the aim of understanding how the velocity, volume, and value of data are increasingly encouraging us to bow to the cathedral of computation and quantification.

Data derivatives – the combinations of data traces left by people – are being used with probabilistic techniques to yield correlations and new possible risks in the surveillance and security field (Amoore, 2011). These risks are acted upon, but who has the power to act and which companies, states or social movement groups can and do respond? Empirical analysis of who has the power to act is needed to examine which data analytic results are privileged. Power asymmetries in the digital ecology are framed by global capitalism and we should not forget this. But when the present and future are visualised as risk maps, scores or flags based on sophisticated computations, someone – a human – takes a decision to act. Designers and engineers choose algorithms based on how quickly they return results or on their computational elegance, but this should not be the main determinant of actions that are taken.

The shift from data analysis and patterns to action is a gateway or control point through which power is exercised. This is the control point we should focus on – who can and does take action? The algorithmic world negates the vast majority of people's agency, but some retain the power to make choices for us. Citizens who rely on the Cloud, self-managed bioteams, avatars or Facebook have little chance of mastery. They have few resources to take action. But for others, such as the military and big companies, choices and actions are leading to judgements about the use, for example, of aerial surveillance and drones or geo-mapping, and the targeting 'persons of concern'. These actions reinforce inequalities and they expose marginalised populations. Those who interpret, make choices and act on data analytics results can be questioned and formal governance arrangements could be devised to hold them to account, at least in societies that respect the fundamental rights of citizens. Unfortunately, growing captivation by a computational theocracy means that relatively little research is focusing on how the people who act on data can be held to account more effectively. This is different than seeking to hold the algorithmic code itself to account or the individual algorithm designers.

A seductive computational theocracy

A computational theocracy is very attractive because a reification of a calculated future is taking hold. An example comes from social computing, a field that brings computing science together with engineering and social science. Social machines are being built with the aim of achieving a web based social and technical system for 'the mechanistic realisation of system-level processes' (Smart & Shadbolt, 2014). The goal is the 'web-extended mind', which can participate in the mental states of human beings. Developers aim to give equal weight to the technological and the social. But how do the social machine makers understand social issues?

They draw from business and management studies in which desirable behaviour is anything that helps to exploit economic returns. The digital platforms supporting algorithm-based services are seen as neutral conduits for data transmission. Algorithms are likely to be seen self-organising agents in a system that 'creates itself out of itself' and selects the fittest (Arthur, 2009). The human being is seen as an object to be predicted as a rational agent. Values are not neglected, but justice linked to how well resources are allocated using rational choice procedural models and transparency is a property of the technical system. In relation to policy requirements such as privacy, the goal is to make digital records of behaviour automatically and to accurately predict personal attributes. Rational expectations models are preferred because they help with the coding of human behaviour, and uncertainty and emotion are not yet reliably codable. The aim is to develop an axiomatised computational logic in order to formalise values such as fairness and equity (Pitt et al., 2013).

For decades the ultimate aim has been to build a unified theory of artificial intelligence. This involves solving the problem of making inferences about the internal structure of a system when all that is known about that system is the input and output signals. The aim is to automate human intelligence by creating 'an all-powerful executive homunculus whose duties require almost Godlike omniscience' (Dennett, 1978: 164). Examples of technologies moving in this direction are driverless cars, the augmented soldier and the digitally enabled consumer. The semiconductor manufacturer, Qualcomm, is working on neuroprocessing engines for smart phones and many more artificial intelligence developments are starting to come out of the laboratory. In summary, for scientists and engineers, despite a commitment to working with social scientists, algorithms are understood to 'reason' about reliability and honesty and they are expected to facilitate good behaviour.

The computational goal is, 'changing what it means to be human' (Rheingold, 2002) and there is resistance to a calculable good life in other areas of the social sciences. Some scholars understand, for example, that the internet is radically incomplete and so is the development of algorithms. But relatively few researchers are asking fundamental questions about what it means to be human and about whether a different pathway is possible. Algorithmic techniques can 'rule out, [and] render invisible, other potential futures' (Amoore, 2011: 38), but when it comes to big social problems – policing, migration, climate change or inequality and poverty – what alternatives are being concealed by the gleam of risk-based algorithmic solutions? Even if algorithms operate at speeds and scales beyond the threshold of human perception, this doesn't mean we should give up on governing the control points where the algorithmic results are translated into action.

Conclusion

What alternative pathways are there? Much more attention needs to be given to the control points of surveillance, power and action. This is where choices are made and action is taken by relatively limited numbers of human beings who are setting the pathway for social, economic and political development. Governance is needed, not so much of individual algorithm developers, but of states and companies who finance their work. Governance using conventional approaches to privacy legislation and policy are one part of this and countries are limiting data processing and data flows in ways that are more or less democratic. Indonesia, Nigeria, Russia, Vietnam and the United Kingdom have passed legislation and Brazil has its 'Internet Bill of Rights'. The European Court of Justice has upheld the 'right to be forgotten'. But companies are innovative. They can evade legislation by, for instance, running their analytics engines on separate databases without breaking the law. States are calling for open data flows to facilitate their security agendas and companies are lobbying for self-governance, claiming their formal representations of data access rights, copyright, and privacy norms in algorithms are, by definition, consistent with good behaviour and a better life.

Conventional privacy protection and human rights legislation has some traction, but rights-based approaches to privacy and surveillance that rely on informed consent are becoming unenforceable. If the quantification of everything means that life itself is likely to become humanly ungovernable, then care of the self and others could also start to become meaningless. The default assumption is that humans are empowered by an immersive mediated environment and they benefit as a result. Focusing on regulatory toolkits that might govern social machines and their developers is important, but better insight is needed into how to combat the notion that quantification is synonymous with the good life.

The digital world is not benign, but it is not predetermined either. Alternative societal outcomes are possible, but only if we can say and think about them; only if we can imagine them. Research is needed on who orchestrates actions based on the technologies of surveillance. We need a clearer view of who funds algorithmic computational research, who commercialises it, and who is using it to act on and shape our world. Coalitions of actors – scholars, activists, politicians and captains of industry will need to collaborate if the pathway we are following to a calculated – and unequal – future is to change. The current pathway is incompatible with human agency, and most likely with greater equality, for the great majority of the world's citizens. It is for this reason that the overwhelming fascination with the quantification of society needs to be questioned and resisted when it is inconsistent with human rights and values. The growing data driven intensity of our lives is only pre-determined if we persist in believing that it is and if we fail to change direction.

Bibliography

Amoore, L. A. (2011): Data derivatives: On the emergence of a security risk calculus for our times. *Theory, Culture & Society, 28*(6): 24-43.

Ananny, M. (2016): Toward an ethics of algorithms: Convening, observation, probability, and timeliness. *Science, Technology & Human Values, 41*(1): 93-117.

Arthur, W. B. (2009): *The nature of technology: What it is and how it evolves.* New York: Allen Lane.

Bucher, T. (2016): The algorithmic imaginary: Exploring the ordinary affects of facebook algorithms. *Information, communication & society,* Online 25 Feb.

Dennett, D. C. (1978): Toward a cognitive theory of consciousness. In C. W. Savage (Ed.). *Perception and cognition: Issues in the foundations of psychology, volume ix minnesota studies in the philosophy of science,* (pp. 201-228). Minneapolis, MI: University of Minnnesota.

Introna, L. (2016): Algorithms, governance, and governmentality: On governing academic writing. *Science, Technology & Human Values, 41*(1): 17-49.

Lazzarato, M. (2009): Neoliberalism in action: Inequality, insecurity and the reconstitution of the social. *Theory, Culture & Society, 26*(6): 109-133.

Mann, S., Nolan, J., and Wellman, B. (2003): Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society, 1*(3): 331-355.

Mansell, R. (2012): *Imagining the internet: Communication, innovation and governance.* Oxford: Oxford University Press.

Manyika, J., Lund, S., Bughin, J., Woetzel, J., Stamenov, K., and Dhingra, D. (2016): *Digital globalization: The new era of global flows.* McKinsey Global Institute, McKinsey & Company, Washington, DC.

Pitt, J., Busquets, D., and Riveret, R. (2013): The pursuit of computational justice in open systems. *AI & Society, Dec.*: 1-19.

Rheingold, H. (2002): *Smart mobs: The next social revolution.* New York: Perseus Press.

Rosenberg, N. (1982): *Inside the black box: Technology and economics.* Cambridge: Cambridge University Press.

Smart, P. R. and Shadbolt, N. R. (2014): Social machines. In M. Khosrow-Pour (Ed.). *Encyclopedia of information science and technology, third edition,* (pp. 6855-6862). Hershey, PA: IGI Global.