Algorithmic States of Exception

McQuillan, D (2015, forthcoming) 'Algorithmic States of Exception', European Journal of Cultural Studies, Vol 18, No 4-5, ISSN 1367-5494

Abstract

In this paper I argue that pervasive tracking and data-mining are leading to shifts in governmentality that can be characterised as algorithmic states of exception. I also argue that the apparatus that performs this change owes as much to everyday business models as it does to mass surveillance. I look at technical changes at the level of data structures, such as the move to NoSQL databases, and how this combines with data-mining and machine learning to accelerate the use of prediction as a form of governance. The consequent confusion between correlation and causation leads, I assert, to the creation of states of exception. I set out what I mean by states of exception using the ideas of Giorgio Agamben, focusing on the aspects most relevant to algorithmic regulation: force-of and topology. I argue that the effects of these states of exception escape legal constraints such as concepts of privacy. Having characterised this as a potentially totalising change and an erosion of civil liberties, I ask in what ways the states of exception might be opposed. I follow Agamben by drawing on Walter Benjamin's concept of pure means as a tactic that is itself outside the frame of law-producing or law-preserving activity. However, the urgent need to respond requires more than a philosophical stance, and I examine two examples of historical resistance that satisfy Benjamin's criteria. For each in turn I draw connections to contemporary cases of digital dissent that exhibit some of the same characteristics. I conclude that it is possible both theoretically and practically to resist the coming states of exception and I end by warning what is at stake if we do not.

Threat models and data models

Edward Snowden's revelations (Electronic Frontier Foundation, 2014) are shocking to many because they suggest that the internet has been set to spy on us. Rather than being platforms for the free exchange of knowledge, the leaked documents show the internet and the web to be covered in surveillance machines that do not discriminate between suspects and the general population. Yet as disturbing as this picture might be, it is at the same time a diversion. By pointing the finger at the NSA and GCHQ, the revelations divert attention from the mechanisms of online business. Tracking is at the heart of Silicon Valley's operations (Mozilla, 2014) and online business-as-usual depends on ferreting out as much information as possible about users; our actions are recorded, collated and sold as part of the large-scale circulation of segmented advertising profiles. It is advertising revenues that oil the wheels of Silicon Valley and the implicit social contract is that service users will accept or ignore the gathering of their information in return for well-engineered free services such as Gmail and Facebook. It is important to realise that this is as expansive as the activities of PRISM, Boundless Informant and other intelligence agency programmes. If we are taken aback by reports that GCHQ developed code to extract user information from the popular gaming app Angry Birds (ProPublica et al., 2014), we should remember that the games companies themselves are already collecting and sharing this information for marketing purposes. In this paper, I will consider the implications of this activity in terms of a threat and the way this threat is connected to big data. When security professionals discuss risk with NGO activists or journalists who have a reasonable suspicion that they are under surveillance, they will often talk in terms of defining a threat model. In other words, rather than considering security as a blanket term, it is important to consider what specific information should be secret, who might want that information, what they might be able to do to get it and what might happen if they do (Bradshaw, 2014). The emerging potential for algorithmic states of exception outlined in this paper suggests that the business model and the threat model are becoming synonymous, by giving rise to interactions that interfere with our assumptions about privacy and liberty. In addition, the flow of everyday data that is being gathered by these companies has surged into a permanent tsunami, whoes landward incursions have become known as big data. The diverse minutiae of our digital interactions on the web and in the world (through smartphones, travel passes and so on) are aggregated in to this new object of study and exploitation. Industry tries to capture big data through definitions like 'volume, velocity and variety' (Gartner, 2011) so it can be positioned as both El Dorado (McKinsey, 2011) and panacea (Hermanin and Atanasova, 2013), perhaps unconsciously recapitulating alchemical notions of the Philosophers' Gold. Critics counter with questions about the ability of big data's numbers to speak for themselves, their innate objectivity, their equivalence, and whether bigness introduces new problems of its own (boyd and Crawford, 2011). I will suggest that the problems and the threats are not driven by big data as such, any more than the drifting iceberg is the cause of the global warming that unloosed it. Instead we need to look at the nature of the material-political apparatus that connects data to decision-making and governance.

The way society disciplines citizens through discourses of health, criminality, madness and security (Foucault, 1977) are given categorical foundations in the structures of data. Consider, for example, the category of 'troubled families' created by the Department for Communities and Local Government (Department for Communities and Local Government, 2014) to identify families as requiring specific forms of intervention from the agencies in contact with them. The 40,000 or so families whose 'lives have been turned around', by being assigned a single keyworker tasked with getting them in to work and their children back to school on a payment by results model, would have been identified through some operations on the data fields that make their existence legible to the government. In turn, various agencies and processes would have operated on those individuals as both effect and affect, as a created intensity of experiential state, in ways that would construct the subjectivity of membership of a so-called troubled family. These actions would, in turn, become new content for data fields and would form the substrate for future interventions. Thus, the proliferation of data does not simply hedge the privacy of enlightenment individuals but produces new subjectivities and forms of action. The data that enables this activity is produced by what Foucault called a dispositif: 'a heterogeneous ensemble consisting of discourses, institutions, architectural forms, regulatory decisions, laws, administrative measures, scientific statements, philosophical, moral and philanthropic propositions. Such are the elements of the apparatus. The apparatus itself is the system of relations that can be established between these elements.' (Foucault, 1980 quoted in Ruppert, 2012). This paper argues that the apparatus is undergoing a significant shift in the system of relations at several levels; in architectural forms (forms of database structures), administrative measures (as algorithms), regulation (as algorithmic regulation) and laws (as states of exception). The moral and philosophical propositions will considered at the end of the paper where I discuss potential means of resisting these shifts.

At the bottom layer of this stack of changes is the architecture of database systems. For the last few decades the Relational Database Management System (RDBMS) has been a core part of any corporate or state apparatus. The relational database transcribes between informational content and action in the world. It stores data in flat tables of rows, each row containing the same set of fields. Each table represents an entity in the world (for example, a person) and the fields are the attributes of that entity (which for a person could be name, age, sexual orientation and so on). Each row in the table is an instance of that entity in the world (so one table consists of many people) and the relationships between tables model relationships in the world (for example, between the table of people and the table of families). Operations on the data are expressed in Structured Query Language (SQL) which enables specific questions to be asked in a computationally effective manner (Driscoll, 2012). It is a powerful and efficient way to manage information at scale and up till now has been well suited to the needs of organisations. However it can be a real challenge to restructure a relational database, because new kinds of data have come along or because there is too much data to store on a single server. Under the pressure of social media and big data new forms of database are emerging which drop the relational model and the use of SQL. Commonly called NoSQL databases, their relative fluidity feeds in to the social consequences I am interested in understanding.

The structure of a relational database is an architecture of assumptions, built on a fixed ontology of data and anticipating the queries that can made through its arrangement of entities and relationships. It encapsulates a more-or-less fixed perspective on the world, and resists the re-inscription of the data necessary to answer a completely new and unanticipated set of questions. NoSQL dumps the neatly defined tables of relational databases in favour of keeping everything in 'schema-less' data storage (Couchbase, 2014). In NoSQL, all the varied data you have about an entity at that moment is wrapped up as a single document object - it does not matter if it duplicates information stored elsewhere, and the kinds of data stored can be changed as you go along. Not only does it allow data to be spread across many servers, it allows a more flexible approach to interrogating it. The data is not stored in neatly boundaried boxes but can easily be examined at different granularities; so for example, rather than retrieving the profile photos of a certain set of users, you can use an algorithm to search eye colour. These dynamic systems can handle unstructured, messy and unpredictable data and respond in real-time to new ways of acting on patterns in the data. Like a shoal of startled fish, the application of this heterogeneous data can sharply change direction at any moment. Throwing away the need to plan a database structure beforehand or to think through the use and articulation of the data leaves a free field for the projection of the imagination. In the next section, I describe how this accelerates the established trend of data-mining and prediction and feeds new ideas about possibilities for governance.

Algorithmic preemption

Data is transformed in to propensities through algorithms, in particular through forms of algorithmic processing known as datamining and machine learning. Data-mining looks for patterns in the data, such as associations between variables and clusters, while machine learning enables computers to get better at recognising these patterns in future data (Hastie 2003}. Hence there exists the possibility of making predictions based on inferences from the data. In the pioneering days of data-mining the interest was in the future purchasing decisions of supermarket customers. But the potential for empirical predictions is also attractive to social structures concerned with risk management, whether those risks are related to car insurance or the likelihood of a terrorist attack. For some, the massive rise in the means of finding correlations is something to be celebrated, enabling decisions about probable disease outbreaks or risks of building fires to be based on patterns in the data (Mayer-Schonberger and Cukier, 2013). However, a probabilistic algorithm will certainly result in some false positives, where it essentially makes wrong guesses. Moreover, the 'reasoning' behind the identification of risk by an algorithm is an enfolded set of statistical patterns and may be obscure to humans, even when all the data is accessible. As a result “data mining might point to individuals and events, indicating elevated risk, without telling us why they were selected” (Zarsky, 2002). Ironically, the predictive turn introduces new risks because of the glossed-over difference between correlation and causation. I show how this is amplified as decisions based on correlations move in to the social domain below.

The increasing use of prediction is colliding with our assumptions about political and judicial fairness, through preemptive predictions - forms of prediction which are 'intentionally used to diminish a person’s range of future options' (Earle, 2013). A good illustration of preemptive prediction is the no-fly list of people who are not allowed to board an aircraft in the USA. The list is compiled and maintained by the United States government's Terrorist Screening Centre. People are usually unaware that they are on the list until they try to board a plane, and face legal obfuscation when they try to question the process by which they were placed on the list (Identity Project, 2013).

The only way to tell if you have been taken off the list is to try to get on a flight again and see what happens. The principle of fair and equal treatment for all under the law relies on both privacy and due process, but the alleged predictive powers of big data mining are on course to clash with the presumption of innocence. In Chicago, an algorithmic analysis predicted a 'heat list' of 420 individuals likely to be involved in a shooting, using risk factors like previous arrests, drug offences, known associates and their arrest records. They received personal warning visits from a police commander, leading at least one person to worry that the attention would mis-identify him to his neighbours as a snitch (Gorner, 2013). Defending themselves against the charge that they were discriminating against the black community, the Chicago police officials referred back to the mathematical nature of the analysis. Thus preemptive measures are applied without judicial standards of evidence and that police are sometimes prepared to act on the basis of an algorithm while asserting that they do not understand the reasoning process it has carried out. While these cases may seem like outliers, the widespread adoption of algorithmic regulation may embed the same process at the core of regulatory action.

The concept of algorithmic regulation is being promoted as a mechanism of social governance. One of the leading proponents is Tim O'Reilly, previously credited as a spokesman for Web 2.0 and its strategy of basing online services on user-generated data. O'Reilly and others use the term algorithmic regulation to describe this computational approach to government. They argue that the dynamic and statistical feedback loops used by corporations like Google and Facebook to police their systems against malware and spam can be used by government agencies to identify and modify social problems. These processes are already at play in the private sector; if you agree to a black box recorder in your car that tracks your driving behaviour, you will be offered a hefty discount on your car insurance (Confused.com, 2014). For policy makers, this promises a seamless upscaling of Thaler and Sunstein's theory of the 'Nudge', where small changes to the so-called choice architecture of everyday life alters people's behaviour in a predictable and desirable way (Thaler and Sunstein, 2008). The resources available to governments have been thinned by crisis-driven cuts and outsourcing, but big data brings a wealth of information. The skills of commercial datamining and machine learning are ready to probe us for proclivities of which we may or may not be aware. Algorithmic regulation seems to offer an apparatus with traction on obesity, public health and energy use through real-time interventions. But, as we have seen, this is made possible by a stack of social technologies with the tendency to escape due process through preemption and justify actions based on correlation rather than causation. How do we understand the implications of pervasive yet opaque mechanisms where correlation becomes a basis for correction or coercion? I argue that a useful lens is Giorgio Agamben's ideas about the State of Exception.

States of exception

In his work on states of exception, Agamben examines the legal basis of events such as a declaration of martial law or the introduction of emergency powers, states of affairs where law, rights and political meaning to life are suspended (Agamben, 2005), of which an emblematic contemporary example is the detention camp in Guantanamo Bay. Roman law allowed for the suspension of the law in times of crisis through the idea that necessity has no law ('necessitas legem non habet'). In modern times the state of exception emerged from the emergency measures of World War One and reached its paramount manifestation in the Third Reich. Agamben interrogates the juridical significance of a sphere of action that is itself extrajudicial to understand the way it has been justified in a legal context and the broader implications of that justification. Historically, the state of exception has been brought within a juridical context by linking it with constituent power rather than constituted power; in other words, linking it not with the existing legal framework but with those forces that are the founding power of the constitution. This ultimately leads Agamben to the conclusion that our norms and rights are themselves rooted in the state of exception. We are living in a kind of fiction, a really-existing state of emergency, from which we cannot return directly to the state of law 'for at issue now are the very concepts of state and law'. However, the application to the question of algorithms comes to the fore through an intermediate part of Agamben's thesis, in the way that he identifies the topological structure of the state of exception as 'being-outside and yet belonging' and through his distinction between the law and the force of the law.

I suggest that 'being-outside and yet belonging' is the form of the spaces being created by the algorithmic apparatus. While tied to clearly-constituted organisational and technical systems, the new operations have the potential to create social consequences that are unaddressed in law. These experiences have been prototyped in social media. When Facebook's algorithms decide that an unlucky user has violated their Terms of Service, that person discovers they have no recourse; there is no real explanation of why they were excluded, and no-one to whom he or she can appeal. No matter that they were excluded simply for crossing some statistical confidence limit, or that their long virtual labour in liking, friending and updating helped generate real share value for the company, or that Facebook may have become an important lever in their social life or in a political campaign (York, 2010). Their prior agency and existence in this pseudo-public space has been algorithmically suspended. Payday lending companies like Wonga now use the full spectrum of heterogeneous data, including Facebook, to assemble thousands of dynamic data points to make loan decisions (Deville, 2013). Everyday life is becoming permeated by points of contact with algorithmic systems that can influence the friction or direction of our experience. In the 1950s, redlining was used to describe the way people were charged more for insurance and healthcare or denied services or jobs based on living in a deprived (often racially identified) part of town. The potential with big data and data-mining is a new and agile form of 'personal redlining' (Davidow, 2014) that is dynamic and updated in real-time. Ambitious forms of algorithmic regulation will combine with new forms of discrimination to apply limits and exclusions. The effect will be to apply continuous partial states of exception through algorithmically derived actions.

According to Agamben, the signature of a state of exception is 'force-of'; actions that have the force of law even when not of the law. Software is being used to predict which people on parole or probation are most likely to commit murder or other crimes. The algorithms developed by university researchers uses a dataset of 60,000 crimes and some dozens of variables about the individuals to help determine how much supervision the parolees should have (Bland, 2010). While having discriminatory potential, this algorithm is being invoked within a legal context. But the steep rise in the rate of drone attacks during the Obama administration has been ascribed to the algorithmic identification of 'risky subjects' via the disposition matrix (Cobain, 2013). According to interviews with US national security officials the disposition matrix contains the names of terrorism suspects arrayed against other factors derived from data in 'a single, continually evolving database in which biographies, locations, known associates and affiliated organizations are all catalogued' (Miller, 2012). Seen through the lens of states of exception, we cannot assume that the impact of algorithmic force-of will be constrained because we do not live in a dictatorship. Agamben's point is that there exists a confusion between dictatorship and the state of exception. The fascist states of the 1930s were not dictatorships but dual states with second structures that could exist alongside the constitution via the creation of states of exception. What we need to be alert for, according to Agamben, is not a confusion of legislative and executive powers but separation of law and force of law. The contention of this paper is that predictive algorithms increasingly manifest as a force-of which cannot be restrained by invoking privacy or data protection.

Protections against the abuse of modern bureaucratic and corporate data gathering have been established under the broad principle of a right to privacy and specific regulations regarding data protection. Responses to the risks posed by big data or algorithmic discrimination such as the 'Civil Rights Principles for the Era of Big Data' (The Leadership Conference, 2014) or the 'Seven Principles for Big Data and Resilience Projects' (Crawford and Meier, 2013) deploy these conventional ideas about rights. While this might be useful as tactic I am arguing that it is futile as a strategy. Firstly because predictive algorithms obfuscate the act of inference. This makes it a priori impossible to fulfil the basics of due process, that judgements about likelihood and balance of proofs are made openly. But secondly, and more fundamentally, the character of the state of exception erases the possibility of legal regulation. While a state of exception is not a dictatorship, it is a space devoid of law where legal determinations are deactivated, especially that between public and private. If there is no longer a public and private as far as the apparatus is concerned, resistance is going to require much more than data protection. Below, I take a lead from Agamben in looking for means of resistance to states of exception in the work of Walter Benjamin. I follow this by describing manifestations of those ideas in historical social movements and in contemporary forms of digital resistance.

Means of resistance

When considering what is to be done about the state of exception, Agamben draws on the ideas of Walter Benjamin, specifically the possibility of pure violence or pure means. Benjamin's line of thought is laid out in his essay 'On the Critique of Violence' (Benjamin, 1995), which sets out to escape the forms of violence (e.g. state vs revolutionary) that are offered as alternatives but in fact co-define each other. He asserts that ’all violence as a means is either law-making or law-preserving’. By this he means that violence either plays a part in constituting a new situation or is carried out by institutions trying to preserve the status quo. Taken together these forms of violence are mythic in the sense that they form an inescapable cycle. Moreover, they can never be easily separated because the practice of law-preserving always involves extension into constituting new sanctions. Benjamin's escape is a 'pure means' that breaks the cycle of mythic violence. So in Benjamin's mostly abstract reasoning we have a model for contesting states of exception, according to Agamben, because it doesn't ultimately rest on the authority of a legal framework which has 'at its centre the state of exception - [which] is essentially an empty space' (Agamben p97). Against a space that is devoid of law we have a resistance that escapes the cycle of law-making and law-preserving. In the remainder of this paper, I take this approach to suggesting lines of resistance to algorithmic states of exception. I do this through two historical examples that, I suggest, crystallise Benjamin's and Agamben's ideas as concrete social possibilities. I link each historical example to signs of similar modalities in contemporary struggles, and ask if they constitute viable starting points for resistance.

The first historical example is antinomianism, which manifested itself in the thirteenth and fourteenth centuries through the movement known as the Brethren of the Free Spirit. For the Brethren of the Free Spirit, God was immanent in everything and could therefore be directly experienced (Cohn, 1970). Those who were able to share this experience of oneness considered that they had moved beyond religious morality and earthly authority. As one said defiantly to his inquisitor 'Those who are in this degree of perfection and in the freedom of spirit are no longer obliged to obey men, or any precept, or the rules of the Church: they are truly free.' (Vaneigem, 1998). The message was one of a radical freedom through a direct immersion in the very ground of being. Although heavily repressed, antinomianism frustrated the Inquisition by frequently resurfacing and led directly to later currents of social change such as the Levellers and Ranters of the English Civil War (Hill, 1991). We can still experience some of their intoxicating irreverence through surviving texts such as Abiezer Coppe’s ‘A Fiery Flying Roll’ (Coppe, 1973), whose fiery rhetoric is designed to punch through rational understanding. Antinomianism as a philosophy and social practice fits Benjamin's description of action from the outside, that neither creates nor preserves law. I suggest that we can hear an echo of antinominianism in the contemporary social movement known as Anonymous.

Anonymous is a social movement with roots in the taboo-breaking irreverence of the online image board 4Chan. It was constituted through Operation Chanology, a set of actions against the Church of Scientology. While Anonymous is difficult to pin down using any of the traditional categories of ethics, sociology or history (Coleman, 2011), it draws its strength from a deep immersion in the technical ground of the internet and finds affinity through the subcultural memes that move freely across the web. It rejects external morality or constraints and features calls for absolute freedoms, especially freedom of speech. The splinter group Lulzsec was a breakaway from Anonymous that specialised in hacking in to private security firms and state surveillance agencies. It combined its online dumping of hacked data with ranting statements filled with a sense of revelation about the state of the world and the new apparatus. It was Anonymous at its most antinomian, marked by a mocking contempt for worldly powers in the form of corporations and governments. Lulzsec's final communiqué ‘50 Days of Lulz’ is a hacker version of Coppe's ranter rhetoric (Lulzsec, 2011). While experiencing its own version of the Inquisition in the form of FBI sting operations, Anonymous has multiplied and spread offline, with the signature Guy Fawkes masks visible at protests across the globe. Most importantly for the purposes of this paper, the antinomian activism of Anonymous and Lulzsec has been disruptive of the data-fueled apparatus of prediction and control. Lulzec targeted agencies and companies who are avowedly spying on us by hacking in to their databases and, in a kind of ritual inversion of the operations of those companies, releasing their data to the public. Anonymous sought more broadly to disrupt the apparatus of control, for example through Distributed Denial of Service attacks that overloaded the websites of organisations they saw as complicit. I suggest, therefore, that the countercultures of the internet are already generating forms of resistance that disrupt algorithmic enclosure without themselves engaging in the cycle of law-making and law-preserving.

Agamben makes it clear that only people's own determination can be relied on to challenge the state of exception. The task is not to confine the state of exception by appealing to rights and norms that are ultimately founded on it. 'To show law in its nonrelation to life and life in its nonrelation to law means to open a space between them for human action,' he writes (Agamben p88). The second historical example shows such human action in a form we could call pure norms, that is, values that enact themselves with an internal consistency that does not appeal to an already captured system. The events in question are the 18th Century food riots, as analysed by E.P. Thompson in his book Customs in Common (Thompson, 1993). Dispelling the food riots as an instinctive response to hunger, he discovers that the central action is not looting but 'setting the price'. People collectively appropriated the grain from farms and granaries to be sold at an affordable price. As the Sheriff of Gloucestershire wrote in 1766 'They returned in general the produce (i.e. the money) to the proprietors or in their absence left the money for them; and behaved with great regularity and decency where they were not opposed, with outrage and violence where they was: but pilfered very little'. Here we have a picture of ordinary people intervening to correct what they see as excess, without relying on a legal framework. Thompson referred to it as 'a moral economy'. I suggest that a similar re-assertion of normative relations without an appeal to law is present in the practice of Cryptoparties.

The idea of Cryptoparty was conceived in August 2012, following a Twitter conversation between Australian privacy advocate Asher Wolf and computer security experts in the wake of the Australian Cybercrime Legislation Amendment Bill (Blum-Dumontet, 2012), and the DIY movement quickly spread with cryptoparties popping up in cities across Australia, US, UK and Germany. They are peer-learning events where people share their knowledge and skills to ensure that private online chats stay private and that email and web browsing are as secure and anonymous as possible. Rather than trying to explain the complex mathematical concepts behind cryptography, cryptographies encourage people to look at the landscape of tracking and surveillance and to develop a sense of how they can raise the barrier to big data collection from their online activities. The shared ethos is a deep unease with the current direction of travel revealed by pervasive corporate tracking and blanket state surveillance. As Smari McCarthy has argued, the aim of easier-to-use encryption is to raise the cost for the NSA and the other intelligence agencies, by forcing them to use scarce human resources to apply specific targeted techniques, or to use a lot of costly processing power to break the encryption. 'They can scoop up the data of 2.5 billion internet users, making the cost per person per day a mere 13 cents. My five-year plan is to increase that cost to $10,000 per person per day.' (McCarthy, 2014). Thus, cryptoparties can also be seen as an example of autonomous price-setting, motivated by community norms acting in the space between law and life.

Learning against the machine

In this paper I have examined the practices of pervasive tracking and data-mining in order to understand where they might be leading us. Rather than staying with specific issues like NSA surveillance or big data, I have instead looked at some interlocking shifts in the machinery of governance. This includes changes to data structures and the tendency to attribute increased powers to algorithms. My suggestion is that the new algorithmic apparatus can be characterised by the production of states of exception. The result is an increase in actions that have the force of the law but lie outside the zone of legal determination. This renders forms of protection such as privacy regulation to be more or less ineffective. If regulation is ineffective, what is to be done? In trying to answer this question, I have drawn on the idea of pure means taken from the work of Walter Benjamin, and applied by Agamben to states of exception; that is, actions in and for themselves that do not rely on a formal external framework for justification. I have tried to make this mode of resistance more concrete through historical examples. By finding correlations between those examples and current digital social movements, I propose that it is possible to inhibit the advance of states of exception. This comes through adopting modes of social action that lie outside the mythic violence of the law. I believe this should be a matter of consideration based only on what we already know about the material-political relations being established. An apparatus is emerging that side-steps democratic mechanisms of debate, oversight and restraint. As much as we can look to history for examples of resistance, we can also look to it as a warning. As Agamben says, when the state of exception becomes the rule then the juridico-political system transforms itself into a killing machine. We know that the tabulations of IBM Hollerith machines played their part in the crimes of the Nazis (Black, 2012); this is not a lesson we need to re-learn when it comes to machine learning and preemptive algorithms. In his theses 'On the Concept of History,' Walter Benjamin refers to pure means as the real state of exception which will 'improve our position in the struggle against fascism' (Benjamin, 2009). In this sense, experimenting with actions to inhibit, slow down or reverse the emergence of algorithmic states of exception become an important way to learn against the machine.

References

Agamben G (2005) *State of Exception*. 1 edition. Chicago: University Of Chicago Press.

Benjamin W (1995) *Reflections: Essays, Aphorisms, Autobiographical Writings*. 1st Schocken edition edition. New York: Random House USA Inc.

Benjamin W (2009) *On The Concept of History*. New York: CreateSpace Independent Publishing Platform.

Black E (2012) *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation-Expanded Edition*. Expanded edition. Washington, D.C.: Dialog Press.

Bland E (2010) Software predicts criminal behavior. *msnbc.com*, Available from: http://www.nbcnews.com/id/38723688/ns/technology_and_science-science/t/software-predicts-criminal-behavior/ (accessed 2 May 2014).

Blum-Dumontet E (2012) There is No Party Like a CryptoParty. *The Huffington Post UK*, Available from: http://www.huffingtonpost.co.uk/eva-blumdumontet/cryptoparty-london-encryption-_b_1953705.html (accessed 16 May 2014).

Boyd D and Crawford K (2011) *Six Provocations for Big Data*. SSRN Scholarly Paper, Rochester, NY: Social Science Research Network, Available from:

http://papers.ssrn.com/abstract=1926431 (accessed 1 May 2014).

Bradshaw P (2014) Four examples of different threat models. *Online Journalism Blog*, Available from: http://onlinejournalismblog.com/2014/07/17/three-examples-of-different-threat-models/ (accessed 20 October 2014).

Cobain I (2013) Obama’s secret kill list – the disposition matrix. *the Guardian*, Available from: http://www.theguardian.com/world/2013/jul/14/obama-secret-kill-list-disposition-matrix (accessed 4 May 2014).

Cohn N (1970) *The Pursuit of the Millennium: Revolutionary Millenarians and Mystical Anarchists of the Middle Ages, Revised and Expanded Edition*. Rev Exp. Oxford University Press.

Coleman (2011) Anonymous: From the Lulz to Collective Action | The New Everyday. Available from: http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action (accessed 4 May 2014).

Confused.com (2014) Telematics insurance - Compare quotes. Available from: http://www.confused.com/car-insurance/telematics (accessed 6 November 2014).

Coppe A (1973) *A fiery flying roll*. Exeter : The Rota, Available from: http://archive.org/details/fieryflyingroll00coppuoft (accessed 3 November 2014).

Couchbase (2014) What is NoSQL Database & Why NoSQL | Couchbase. Available from: http://www.couchbase.com/why-nosql/nosql-database (accessed 2 May 2014).

Crawford K and Meier P (2013) Seven Principles for Big Data and Resilience Projects. *iRevolution*, Available from: http://irevolution.net/2013/09/23/principles-for-big-data-and-resilience/ (accessed 4 May 2014).

Davidow B (2014) Redlining for the 21st Century. *The Atlantic*, Available from: http://www.theatlantic.com/business/archive/2014/03/redlining-for-the-21st-century/284235/ (accessed 2 May 2014).

Department for Communities and Local Government (2014) Helping troubled families turn their lives around - Policy - GOV.UK. Available from: https://www.gov.uk/government/policies/helping-troubled-families-turn-their-lives-around (accessed 14 May 2014).

Deville J (2013) Leaky data: How Wonga makes lending decisions | Charisma Consumer Market Studies. Available from: http://www.charisma-network.net/finance/leaky-data-how-wonga-makes-lending-decisions (accessed 27 October 2014).

Driscoll K (2012) From Punched Cards to ‘Big Data’: A Social History of Database Populism. *communication 1*, 1(1), Available from: http://scholarworks.umass.edu/cpo/vol1/iss1/4.

Earle IK& J (2013) Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy. *Stanford Law Review Online*, 66, 65, Available from: http://www.stanfordlawreview.org/online/privacy-and-big-data/prediction-preemption-presumption (accessed 2 May 2014).

Electronic Frontier Foundation (2014) NSA Primary Sources. *Electronic Frontier Foundation*, Available from: https://www.eff.org/nsa-spying/nsadocs (accessed 1 May 2014).

Foucault M (1977) *Discipline and Punish: The Birth of the Prison*. Penguin Books.

Foucault M (1980) The Confession of the Flesh (1977) Interview. In: *Power/Knowledge: Selected Interviews and Other Writings - C. Gordon (ed.)*, New York: Pantheon.

Gartner (2011) Gartner Says Solving ‘Big Data’ Challenge Involves More Than Just Managing Volumes of Data. Available from: http://www.gartner.com/newsroom/id/1731916 (accessed 1 May 2014).

Gorner J (2013) Chicago police use heat list as strategy to prevent violence. *Chicago Tribune*, Available from: http://articles.chicagotribune.com/2013-08-21/news/ct-met-heat-list-20130821_1_chicago-police-commander-andrew-papachristos-heat-list (accessed 2 May 2014).

Hermanin C and Atanasova A (2013) Making ‘Big Data’ Work for Equality. *When it comes to fighting inequality in Europe, this tool is essential. Why aren’t we using it?*, Available from: http://www.opensocietyfoundations.org/voices/making-big-data-work-equality-0 (accessed 1 May 2014).

Hill C (1991) *The World Turned Upside Down: Radical Ideas During the English Revolution*. New Ed edition. London; New York: Penguin.

Identity Project (2013) "No-fly” trial, day 3: Why and how was Dr. Ibrahim barred from the U.S.? Available from: http://papersplease.org/wp/2013/12/04/no-fly-trial-day-3-why-and-how-was-dr-ibrahim-barred-from-the-us/ (accessed 23 October 2014).

Lulzsec (2011) 50 Days of Lulz - Pastebin.com. *Pastebin*, Available from: http://pastebin.com/1znEGmHa (accessed 4 November 2014).

Mayer-Schonberger V and Cukier K (2013) *Big Data: A Revolution That Will Transform How We Live, Work and Think*. London: John Murray.

McCarthy S (2014) Don’t Shoot the Messenger - Smári McCarthy. Available from: http://smarimccarthy.is/blog/2014/04/02/dont-shoot-the-messenger/ (accessed 6 May 2014).

McKinsey (2011) Big data: The next frontier for innovation, competition, and productivity | McKinsey & Company. *Big data: The next frontier for innovation, competition, and productivity*, Available from: http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation (accessed 1 May 2014).

Miller G (2012) Plan for hunting terrorists signals U.S. intends to keep adding names to kill lists. *The Washington Post*, 9th November, Available from: http://www.washingtonpost.com/world/national-security/plan-for-hunting-terrorists-signals-us-intends-to-keep-adding-names-to-kill-lists/2012/10/23/4789b2ae-18b3-11e2-a55c-39408fbe6a4b_story.html (accessed 4 May 2014).

Mozilla (2014) Lightbeam for Firefox. *Shine a Light on Who’s Watching You*, Available from: http://www.mozilla.org/en-US/lightbeam/ (accessed 1 May 2014).

ProPublica, Larson J, Glanz J, et al. (2014) Spy Agencies Probe Angry Birds and Other Apps for Personal Data. *ProPublica*, Available from: http://www.propublica.org/article/spy-agencies-probe-angry-birds-and-other-apps-for-personal-data (accessed 1 May 2014).

Ruppert E (2012) The Governmental Topologies of Database Devices. *Theory, Culture & Society*, 29(4-5), 116–136, Available from: http://tcs.sagepub.com/content/29/4-5/116 (accessed 1 May 2014).

Thaler RH and Sunstein CR (2008) *Nudge: Improving Decisions About Health, Wealth, and Happiness*. 1 edition. New Haven: Yale University Press.

The Leadership Conference (2014) Civil Rights Principles for the Era of Big Data. *The Leadership Conference on Civil and Human Rights*, Available from: http://www.civilrights.org/press/2014/civil-rights-principles-big-data.html (accessed 4 May 2014).

Thompson EP (1993) *Customs in Common*. New edition edition. London; New York: Penguin Books Ltd.

Vaneigem R (1998) *The Movement of the Free Spirit*. New York; Cambridge, Mass.: Zone Books.

York J (2010) Facebook Removes Moroccan Secularist Group and its Founder. *Global Voices Advocacy*, Available from: http://advocacy.globalvoicesonline.org/2010/03/14/facebook-removes-moroccan-atheist-group-and-its-founder/ (accessed 16 May 2014).

Zarsky TZ (2002) Mine Your Own Business: Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion. *Yale Journal of Law and Technology*, 5, 1, Available from: http://heinonline.org/HOL/Page?handle=hein.journals/yjolt5&id=3&div=&collection=.