Big Dataveillance: Emerging Challenges
David Lyon, Queen's University

Draft May 3 2016.

INTRODUCTION

Cynics may say that the only new thing about Big Data is the name. After all, corporations and governments have been gathering big data and searching for patterns for years. But the widespread use of the term, Big Data, itself has catalyzed both corporate celebration and controversial debate, that refuses to die down. Why?

Because Big Data practices throw down a gauntlet to many conventional ways of doing things – for example abandoning what were once seen as the rules for statistical analysis, and, when applied, challenging basic aspects of the rule of law. In Big Data Surveillance, it is machines that 'see' or 'watch,' not passively (as in the panopticon) but predictively. BDS 'learns' through correlations and reproduces what was input.

Here, we discuss Big Data *Surveillance*, which has become increasingly important to large organizations and to ordinary people, within today's digital modernity. The statistical and software practices now gathered together under the often-hyped heading of big data now contribute to a novel surveillance situation for which a good term is 'Big Dataveillance.' All major surveillance trends (Bennett *et al* 2014) are affected by big data.

Debating Big Dataveillance is vital because even if we can't *define* Big Data it's clear that rapid developments under that name challenge our conventional capacity to respond. Basic questions are raised beyond individual privacy and rights and indeed beyond specific harms. Big Data Surveillance sharply raises issues about the *agents* of surveillance and about not merely limiting harms but about seeking the *common, public good* (van der Sloot, Broeders and Schrijvers 2016).

Our lives are made transparent to organizations in ways that are often scarcely visible to us; much Big Data Surveillance is hidden from us. The flows of data are fast and circulate within a broader range of organizations than ever before. Relationships between space and time alter and with them, power relations (Bauman 2000: 9). This aspect of digital modernity is "liquid surveillance," which has some specific characteristics and is further facilitated by big data.

Big data is both highly dynamic and weakly structured, which lends 'liquidity' to surveillance (Bauman and Lyon 2013, Lyon 2016). This is a slippery kind of surveillance in both senses. We have less idea of what is happening (Lupton 2015:34) and how it affects our lives and less sense of what, if anything, can be done about it (cf Solove 2013).

In the Western world, many discovered big data in September 2013, when a "Snowden document" was released, showing that the NSA tracks the social connections of Americans and others, using a colossal cache of data from phone call and email logs. Their sophisticated graphs of some Americans' social connections can identify their associates, their locations at certain times, their traveling companions and other personal information (Poitras and Risen 2013).

The NSA also "enriches" these data with material from other sources -- public, commercial; things like bank codes, insurance information, Facebook profiles, passenger manifests, voter registration rolls, location-based services, property records and tax data. All can also be stored for later use. The official reason is to find out who might be directly or indirectly in a contact chain connected with someone of foreign intelligence interest. NSA analysts seek both "person-centric" analyses and "relationship types" that yield "community of interest" profiles.

The Snowden leaks show the extent of the use of everyday social media – as well as data sourced from economic transactions, sensors, government and ubiquitous cameras (Michael and Lupton 2015:5, Lyon 2014) -- as the *source* of actionable data – data that can be captured, assembled, classified and analyzed. These data enable the analytics from which profiles and predictions about us are made, always with a view to enlarging our opportunities or restricting our options.

They illustrate the common characteristics of big data – volume, velocity and variety – and also some 'Vs' that are less discussed, such as veracity and vulnerability (Saulnier 2016, cf Pasquale 2015).

Some starting assumptions: Algorithms and analysis are socially shaped and in turn shape social outcomes. The technologies and practices are bound up with government and corporation, now operating together more closely than ever. Surveillance capitalism is key (Zuboff 2015). So it's not a 'society vs technology' question – Big Data is techno-cultural or socio-technical. And it's complex; Big Data probably does hold positive promise in some areas.

Big Data is not raw or neutral or objective. It is constituted within already-formed-and-emergent commercial, policing, administrative and security assemblages and affect people's lives accordingly. The primary surveillance questions are ethical. To limit ourselves to legal, technical or administrative issues is inadequate. On the other hand, data subjects are not passive but actually develop various tactics to engage online.

1. BIG DATAVEILLANCE

The term 'big dataveillance' puts the accent on the *kind* of surveillance in question. It connects 'big data' practices with surveillance done using data trails, something that has been happening since the 1980s using computer data and using "small data" before that. It picks up clues from bits of information left behind

every time we log on, make a call, are monitored by sensors or cameras, make a transaction with a bank, another business or a government department.

Big dataveillance, like big data generally, is far from any kind of 'settled' state; it's volatile and contested (Michael and Lupton 2015, Kitchin and Lauriault 2015, Clarke 2014). Such chronic volatility, along with its adoption as a key mode of accumulation, may be part of what's 'new' about big dataveillance, beyond the name. Plus, innovations in technology, the widespread use of electronic devices, and massive dependence on technology for social purposes each make real-time information readily available. This occurs in so-called liberal-democratic societies (Bigo and Tsoukala 2008).

"Datafication" (Van Dijck 2014) normalizes the process that turns social action into quantified data and allows data to be the currency of exchange between those who want it for business or security purposes and those apparently willing to part with it. As Van Dijck shows, this involves beliefs in big data and trust in its agents. "Life-mining" makes available many aspects of social life not previously accessible by security agencies, corporations or the academy. "Friending" and "liking" become algorithmic relations and the results of tracking them are taken as symptoms or sensors, as ways of knowing what the public is thinking or feeling.

But the technological channels are not neutral and the aggregate data do not have a direct relation with individuals whose lives contributed to them. Analysis and projection or deduction and prediction do not have self-evident links (Amoore 2011). At the same time, personalization and customization are central to big data (Andrejevic 2012: 86). "Dataveillance [has] profound consequences for the social contract between corporate platforms and government agencies on the one hand and citizens-consumers on the other" (Van Dijck 2015).

Big dataveillance is facilitated by the increasing digitization of everyday life, which in turn relates to the political economy of surveillance, or what Shoshana Zuboff calls "surveillance capitalism" (Zuboff 2015), marked by its dependence on big data. Her study of Google chief economist Hal Varian's work shows why Google workers, paid or not, experience "studied indifference." This analysis can be extended to Big Dataveillance.

2. CHANGING PRACTICES

New modes of data capture and analytics

The sources for data capture have proliferated exponentially -- web data, sensors, internet of things, government data, social media, transactional data plus new analytic paths: streaming, text. Smart and autonomous cars present new issues here! So personally identifiable information is not what it was. What counts, now, is data fragments, an algorithmic assemblage. Excess data-generation has become the norm (and data minimization is viewed as deviant).

Reliance on algorithmic modes of data capture and analysis often reinforces discrimination, as several studies indicate (Miller 2015). Google advertising shows ads for high-income jobs are frequently shown more to men than women (Carnegie-Mellon); ads for arrest records show up on searches for distinctively black names (Harvard); advertisers can target people in low income areas with high-interest loans (FTC) (Cf Dwork and Mulligan 2013). The questions pertain to far more than just national security!

Especially in mobile contexts, using social media is a new source of intelligence information, not only for corporations seeking new markets but also in national security. This is seen for instance in the LEVITATION disclosures about Canada's CSE in their search of "radicalized youth" by checking downloads (Gallagher and Greenwald 2015). They did not obtain corporate compliance. The ATOMIC BANJO program taps directly into internet cables and sifts individual IP addresses (cf Forcese and Roach 2015).

This happens most obviously in online environments of connectivity. As Van Dijck observes, data culled from social media sites, including so-called "affective" traffic from "like" and "favorite" buttons, are the basic data for mining (Van Dijck 2013: 162). Predictive analytics are used by statisticians who examine relationships between past variables to gauge the likelihood of recurring actions. Facebook and Google, in particular, invest much in this to improve ad-effectiveness. Google and Twitter try to tie these to real-time occurrences – such as health challenges – in order to maximize the current relevance of their clients' advertising.

From social sorting to personal profiles?

"Dataveillance—the monitoring of citizens on the basis of their online data—differs from surveillance on at least one important account: whereas surveillance presumes monitoring for specific purposes, dataveillance entails the continuous tracking of (meta)data for *unstated preset purposes*." (Van Dijk 2015). This may be done in government or corporate contexts. For example, Facebook uses "ethnic affinity groups" to help companies using their data to know how they should advertise, distinguishing – possibly prejudicially -- between, black, hispanics and the like (Hern 2016).

Social media is scanned by systems used by police to determine your 'threat rating.' Data-mining technologies, now using 'big data' techniques, provide police with masses of information, often already targeted at specific persons or neighbourhoods, with likely inequitable effects. 'PredPol' e.g. predicts times and places for future crimes. They sort and score billions of commercial records in seconds to make the green yellow, red threat rating. They include checking social media for 'warning signs.' So much for 'blind justice' – this is pre-judgment by algorithm.

Antoinette Rouvroy calls this "algorithmic governmentality;" a "change in approach in the detection, classification and predictive assessment of events in

the world and of the behaviour and propensities of its inhabitants …a new way of making the world 'predictable,' if it cannot be made 'significant'" (in the sense of statistical validation) combined with new ways of exercising power (2015: 18). Unlike the governmentality described by Foucault, based on categories, algorithmic governmentality uses personalization and profiling – fragmented individuals without a collective context – that are calculable, comparable, indexable and interchangeable. Making common cause, or framing one's own narrative, does not enter the picture.

So is social sorting giving way to other modes of surveillance? No, social sorting is as pervasive as ever ( ). But a discernible trend is customizing to the individual level, where the profile is not one of group-association – as in geodemographic marketing's "you are where you live" – but is narrowed to the atomized subject-body. Rather than use post-codes to classify groups, around the turn of the C21st, marketers began to shift to records of web-searches and browsing histories to produce personalized. Traditional geodemographic marketers followed suit, especially once data – especially geo-locating data, started to flow from Facebook and Twitter and other social media.

The shift from postcode to individual profiling "commodifies the individual" (Dalton and Thatcher 2015:4). This connects, too, with the "quantified self" (Lupton 2016). Assuming that social identity can be algorithmically quantified and that personal data are predictive, advertisers engage with customers in ways that can resemble self-fulfilling prophecies. But how this happens remains hidden in the "black box" of the analytic algorithms, known only to their corporate owners, that classify the individual. Thus results are used without questioning how they came to be "successful" except in crude market terms of competitive advantage.

So-called "data singularity," means that sensors can be attached to anything and everything – doors, dams, streets and subways – that send data constantly to data centres. This is the 'internet of things,' where continuous improvement is the key. But inevitably it also has surveillance aspects; it *is surveillant.* 'Salesforce,' that spearheads such developments and knows about revenue, next to Amazon's knowledge of purchasing and Google's grasp of all people do on the internet. (Hardy 2016)

3. A NEW NEW SURVEILLANCE?

Gary Marx spoke in the 1980s of a "new surveillance" – from human to machine monitoring, using computer technologies. Is Big Dataveillance another "step change" in surveillance (cf Kitchin and Lauriault f/c)? Do big data practices – and the laws supporting them reflect a structural shift in the distribution of authoritative and allocative resources and a challenge to the knowledgeability of everyday actors – the subjects of surveillance? Do such surveillance practices signal some basic alterations in our social relationships – for instance in the modes of interaction between individuals and organizations? Can we frame the new in terms of the past from which it grew?

If there is a new structural type emerging than it is part of a larger issue of "digital modernity," requiring a "digital sociology" (Lupton 2015). It has to grapple with "liquid surveillance" and "surveillance capitalism" (Zuboff 2015). The tasks are to identify the features of the emerging stuctural alteration, indicate what are the main historical links that made it possible (Abrams 1972 cf Zuboff 2015) and to consider alternative futures in the light of the big data drive.

Some key issues relating particular to big data and "smart cities" are raised by Klauser and Albrechtslund (2014) that point to key social structural dimensions of big data: agency, temporality, spatiality and normativity. They also, rightly, connect the trends towards self-tracking (at an individual level) with infrastructural issues ("smart cities"). These categories helpfully point of other ways (though this is not exactly their intention) of determining how far big dataveillance amounts to a qualitative change.

All this leads *beyond* conventional ways of thinking about surveillance (Albrechtslund and Klauser). New practices are beyond single technologies, such that all kinds of different purposes may lie behind the surveillance; beyond organizations, raising questions of indvidual actors proactively engaging with and initiating surveillance; beyond the monitoring of humans to the surveillance of objects such as smart meters; beyond risk, as different surveillance purposes are brought together in fresh ways, including self-management / cultivation; and beyond rigidity.

Profile, Predict, Prevent

One of the most significant aspects of big dataveillance is its attempt to foresee the future in order to control the present. And as Cukier and Mayer-Schönberger (2013: 170) say, "data predictions about individuals may be used to, in effect, punish people for their propensities, not their actions. This denies free will and erodes human dignity." This is not *always* a problem of course, it depends on how dataflows are collected, managed, stored.

Predictive analytics are used to assess likely future behaviours or events and to direct appropriate action. It can produce "anticipatory governance" (Rouvroy 2015). Such "preventative prediction" makes the presumption of innocence the first casualty. This has been a feature of air travel for a number of years, with passengers profiled for risk and levels of security checks prior to starting their journey (Dodge and Kitchin 2004, Amoore 2006).

More recently prevention/preemption has been extended to general policing, with it being used by a number of US police forces to identify potential future criminals and to direct the patrolling of areas based on an analysis of historical crime data, records of arrests, and the known social networks of criminals (Siegel 2013; Stroud 2014). In such cases, a person's data shadow does more than follow them; it precedes them, seeking to police behaviours that may never occur

(Stalder 2002; Harcourt 2007). As a consequence, people are treated differently in anticipation of something they may or may not do (Kitchin and Lauriault 2015).

In the world of 'il/liberal' and 'liquid' surveillance, the casualities are any real interest in real causalities or inner reasons; individuals become black boxes. 'Subjects' are assessed by multiple metrics, dependent on data stocks derived from big data. The rule of probability means that power is constantly confronted with pure chance, but uses big data and algorithms to make chance real (cf Gandy). Future probabilities make all the difference, as they're projected onto ordinary lives of citizen-consumers. There's a parallel, duplicate reality; power and business are geared to the fiction, but not fantasy (big data makes is sounds plausible), of a probable reality. Diagnoses, consumer advice and judicial sentences depend on it.

CONCLUSION

We are in transition to an emerging era of digital modernity, fuelled by surveillance capitalism that generates liquid, large-scale dataveillence. It is different from what went before – it is more pervasive, privacy is increasingly undermined, people and places are profiled and socially sorted, and algorithmic governance is a reality (cf Kitchin 2015: 184, Rouvroy 2016). Big data's 3 Vs, velocity, variety and volume are important, of course, but another V, vulnerability, is tremendously significant and demands attention.

While small data, slow data and select data may offer some practical alternatives, it is equally important to have a sense of the ethical imperatives relating to dignified personhood, mutuality, trust, rights and social justice that underlie them. Crucial and consequential matters include the question of predictive analytics, that appear simultaneously in several domains from health and medicine to policing and security to consumer marketing. Discriminatory practices are facilitated, the black boxes of data analytics remain stubbornly closed and time-honoured reliance on due process, the rule of law and the presumption of innocence is undermined. Statistical rule threatens to sidestep or stifle proper political discourse which makes it harder to challenge the discrimination and degraded justice.

Ask, where things have gone badly wrong *and* what priorities – what vision for the future – should we seek? Memories must be reconnected with hopes even as we oppose those key consequences of big data surveillance that magnify the marginalization and disadvantage of the already vulnerable or that close off the chances for thoughtful political debate. Of course, big dataveillance is complex, messy and morally ambivalent – but this simply means that more resources and research is needed to ensure that worst cases are resisted and human-scale values and practices are retrieved.

Bibliography

Abrams, Philip, 1972 The sense of the past and the origins of sociology, *Past and Present*. 55: 18-32.

Al-Suwaidi, Maha. 2015. The Case for Qatar. *Harvard Political Review*. At http://harvardpolitics.com/world/case-qatar/?gclid=Cj0KEQjwxI24BRDqqN3f-97N6egBEiQAGv37hAEDDWmDpbAlw8ZZJScf4kKYtpGN66umD7RBD3-P_Z8aAksm8P8HAQ/

Amoore, Louise 2011 Data Derivatives : On the Emergence of a Security Risk Calculus for Our Times. *Theory Culture and Society* 28 (6): 24 -43.

Andrejevic, Mark. 2012 (cited in van Dijk)

Anderson, Chris. 2008. The end of theory: the data deluge makes the scientific method obsolete. At http://www.wired.com/2008/06/pb-theory/

Ball, Kirstie, Daniel, Dibb and Meadows. 2010. 'Democracy, surveillance and "knowing what's good for you' in Haggerty and Samatas eds. *Surveillance and Democracy*. London and New York: Routledge

Bauman, Zygmunt and David Lyon 2013 *Liquid Surveillance: A Conversation*, Cambridge: Polity Press.

Bauman, Zygmunt. 2000. *Liquid Modernity*. Cambridge: Polity Press

Bedoya, Alvaro. 2016 'The color of surveillance' *Slate*. http://www.slate.com/articles/technology/future_tense/2016/01/what_the_fbi_s_surveillance_of_martin_luther_king_says_about_modern_spying.html/

Bigo, Didier and Anastassia Tsoukala eds. 2008. *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes*. London and New York: Routledge.

boyd, danah & Crawford, Kate. 2012. Critical questions for Big Data: provocations for a cultural, technological, and scholarly phenomenon, *Information, Communication & Society,* 15 (5), 662-79.

Burrows, Roger and Nicholas Gane. 2006

CitizenLab. 2015. Hacking Team leak highlights CitizenLab research. At https://citizenlab.org/2015/08/hacking-team-leak-highlights-citizen-lab-research/

Clarke, Roger. 2015. 'Big data, big risks' at http://www.rogerclarke.com/EC/BDBR.html

Cukier and Mayer-Schönberger. 2013. *Big Data: A Revolution that will Transform the Way we Live, Work and Think*. New York: Houghton Mifflin Harcourt.

Dalton, Craig and Thatcher, Jim. 2015. Inflated granularity: spatial big data and geodemographics. *Big Data & Society*. July-December: 1-15.

Dwork, Cynthia and Deirdre Mulligan. 2013. It's not privacy and it's not fair. *Stanford Law Review Online*. 66(35). At http://www.stanfordlawreview.org/online/privacy-and-big-data/its-not-privacy-and-its-not-fair

Forcese, Craig and Kent Roach. 2015. False Security: The Radicalization of Canadian Anti-Terrorism. at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2655781/

Foucault, Michel. 1980. *History of Sexuality*. Intro.

Gallagher, Ryan and Glenn Greenwald. 2015. Canada casts global dragnet over file downloads. *The Intercept*. January 28. At https://theintercept.com/2015/01/28/canada-cse-levitation-mass-surveillance/

Harcourt, Bernard. 2015 *Exposed: Desire and Disobedience in the Digital Age*. Cambridge: Harvard.

Harcourt, Bernard. 2007 *Against Prediction*. Chicago: University of Chicago Press.

Hardy, Quentin. 2016. 'Looking beyond the internet of things' *New York Times*. January 16. http://www.nytimes.com/2016/01/02/technology/looking-beyond-the-internet-of-things.html?emc=edit_th_20160102&nl=todaysheadlines&nlid=55961761&_r=0/

Harcourt, Bernard. 2007. *Against Prediction*. Chicago: University of Chicago Press.

Hern, Alex. 2016. Facenook's 'ethnic affinity' advertising sparks concerns of 'racial profiling.' *The Guardian.* March 22. At http://www.theguardian.com/technology/2016/mar/22/facebooks-ethnic-affinity-advertising-concerns-racial-profiling?utm_source=esp&utm_medium=Email&utm_campaign=GU+Today+main+NEW+H&utm_term=163258&subid=13802525&CMP=EMCNEWEML6619I2/

Jones, Robert. 2014. UAE betting on big data as CIOs plan analytics investments. *ZDNet*. February 06. At http://www.zdnet.com/article/uae-betting-big-on-big-data-as-cios-plan-analytics-investments/

Kitchin, Rob and Tracey Lauriault. Forthcoming 2015. Towards critical data studies: Charting and unpacking data assemblages and their work. in Eckert, J., Shears, A. and Thatcher, J. (eds) Geoweb and Big Data. University of Nebraska Press. At http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2474112/

Kitchin, R. (2014) *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences.* London: Sage.

Klauser, Francisco and Anders Albrechtslund 2014 'From self-tracking to smart urban infrastructures: towards an interdisciplinary research agenda on big data' *Surveillance & Society* 12:3 273-286. http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/viewFile/infrastructures/infrastructure

Lupton, Deborah 2014 *Digital Sociology*, London and New York: Routledge.

Lyon, David. 2016. 'Surveillance, liquidity and the ethics of visibility' in Carlo Bordoni ed. Special issue on Zygmunt Bauman, *Revue de Philosophie*

Lyon, David. 2015 *Surveillance after Snowden*. Cambridge: Polity.

Lyon, David. 2014. Snowden, surveillance and big data: Capacities, consequences, critique. *Big Data & Society* 1(1):

Lyon, David 2003 *Surveillance after September 11*, Cambridge: Polity.

Marwick, Alice. 2012. The public domain: social surveillance in everyday life, *Surveillance and Society*. 9(4): 373-398.

McCulloch, Jude and Wilson, Dean. 2015. *Pre-crime, preemption, precaution and the future*. London: Routledge.

MEM 2014. Snowden to reveal secrets of Arab dictators. *Middle East Monitor*. April 28. At https://www.middleeastmonitor.com/news/europe/11140-snowden-to-reveal-secrets-of-arab-dictators/

Michael, Mike and Deborah Lupton 2015 'Towards a manifesto for the '"public understanding of big data"' *Public Understand of Science*, 1-13

Miller, Claire Cain. 2015. When algorithms discriminate. *NYT* July 09. At http://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html?emc=edit_th_20150710&nl=todaysheadlines&nlid=55961761&_r=3&abt=0002&abg=0

NU-Q. 2013. Big Data Conference Report.

Orton-Johnson K. and Prior, N. 2013. *Digital Sociology: Critical Perspectives*. Houndmills: Palgrave Macmillan.

Pasquale, Frank. 2015. *The Black Box Society*. Cambridge: MA: Harvard University Press.

Risen, James and Laura Poitras. 2013. NSA gathers data on social connections of US citizens. *Washington Post.* September 28. http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html/

Rouvroy, Antoinette, 2016. Of data and men: Fundamental rights and freedoms in a world of big data, Report to the Council of Europe, January. Report T-PB-BUR(2015)09REV.

Rouvroy, Antoinette and Thomas Berns. 2013. Gouvernementalité algorithmique et perspectives d'émancipation : le disparate comme condition d'individuation par la relation? *Reseau* 31(177): 163-196.

Saulnier, Alana. 2016. PhD Dissertation. Queen's University.

Van der Sloot, Bart, Dennis Broeders and Erik Schrijvers (eds.). 2016. *Exploring the Boundaries of Big Data*. The Hague: Netherlands Scientific Council for Government Policy (WRR). http://www.wrr.nl/fileadmin/en/publicaties/PDF-Verkenningen/Verkenning_32_Exploring_the_Boundaries_of_Big_Data.pdf

Van Dijk, Jose 2014 'Datafication, dataism, and digital dataveillance: Big data between scientific paradigm and ideology.' *Surveillance & Society*, 12:2, 197-208. At http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/datafication/datafic

Wolf, Burkhardt. 2015. Big data, small freedom? Informational surveillance and the political. *Radical Philosophy*. May/June. At https://www.radicalphilosophy.com/commentary/big-data-small-freedom#ref-10-a

Zuboff, Shoshana. 2015. 'Big Other: Surveillance capitalism and the prospects of an information civilization.' *Journal of Information Technology.* 30: 75-89.

Zuboff, Shoshana. 2016. *Master or Slave? The Fight for the Soul of Our Information Civilization.* New York: Public Affairs.

Additional sources:

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754 (Zuboff Big Other)
http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html (Zuboff secrets of survcapm)
http://www.lse.ac.uk/newsAndMedia/videoAndAudio/channels/publicLecturesAndEvents/player.aspx?id=3350 (Pasquale lecture)
http://digital-studies.org/wp/wp-content/uploads/2015/02/Repot-Digital-Studies-October-7-2014.pdf (Rouvroy algorithmic governmentality)