‘Hypernudge’: Big Data as a Mode of Regulation by Design’

by

Karen Yeung[*]

Abstract (250 words max)

This paper draws on regulatory governance scholarship to argue that the analytic phenomenon currently known as ‘Big Data’ can be understood as a mode of ‘design-based’ regulation. Although Big Data decision-making technologies can take the form of automated decision-making systems, this paper focuses on algorithmic decision-guidance techniques. By highlighting correlations between data items that would not otherwise be observable, these techniques are being used to shape the informational choice context in which individual decision-making occurs, with the aim of channelling attention and decision-making in directions preferred by the ‘choice architect’. By relying upon the use of ‘nudge’- a particular form of choice architecture that alters people’s behaviour in a predictable way without forbidding any options or significantly changing their economic incentives, these techniques constitute a ‘soft’ form of design-based control. But, unlike the static Nudges popularised by Thaler and Sunstein (2008) such as placing the salad in front of the lasagne to encourage healthy eating, Big Data analytics nudges are extremely powerful and potent due to their networked, continuously updated, dynamic and pervasive nature (hence ‘hypernudge’). I adopt a liberal, rights-based critique of these techniques, contrasting liberal theoretical accounts with selective insights from science and technology studies (STS) and surveillance studies on the other. I argue that concerns about the legitimacy of these techniques are not satisfactorily resolved through reliance on individual notice and consent, touching upon the troubling implications for democracy and human flourishing if Big Data analytic techniques driven by commercial self-interest continue their onward march unchecked by effective and legitimate constraints.

[*] Professor of Law, Director, Centre for Technology, Ethics, Law & Society (TELOS), The Dickson Poon School of Law, King’s College London. An earlier version of this paper was presented at *Algorithms and Accountability,* an international conference hosted by the NYU Law Institute and the Department of Media, Culture and Communications at New York University, New York, 28 February 2015. I am grateful to Joris van Hoboken and Helen Nissenbaum for hosting my visit and providing me with an opportunity to discuss my ideas at such an immensely stimulating forum. I am also indebted to Barbara Prainsack, Roger Brownsword, Lyria Bennett Moses, John Coggan, Alessandro Spina and Chris Townley for comments on earlier drafts. All errors remain my own.

1. Introduction

It is claimed that society stands at the beginning of a New Industrial Revolution, powered by the engine of Big Data. This paper focuses on how industry is harnessing Big Data to transform personal digital data into economic value, described by one leading cyberlawyer as the 'latest form of bioprospecting' (Cohen 2012). Although the term 'Big Data' is widely used, no universal definition has yet emerged. Big Data is essentially shorthand for the combination of a technology and a process (Cohen 2012: 1919). The technology is a configuration of information-processing hardware capable of sifting, sorting and interrogating vast quantities of data very quickly. The process involves mining data for patterns, distilling the patterns into predictive analytics, and applying the analytics to new data. Together, the technology and the process comprise a methodological technique that utilises analytical software to identify patterns and correlations through the use of machine learning algorithms applied to (often unstructured) data items contained in multiple data sets, converting these data flows into a particular, highly data-intensive form of knowledge (Cohen 2012: 1919). A key contribution of Big Data is the ability to find useful correlations within datasets *not capable of analysis by ordinary human assessment* (Shaw 2014). As boyd and Crawford observe, 'Big Data's value comes from patterns that can be derived from making connections about pieces of data, about an individual, about individuals in relation to others, about groups of people, or simply about the structure of information itself. Big Data is important because it refers to an analytic phenomenon playing out in academia and industry' (boyd and Crawford 2012: 662), and it is this understanding of Big Data as a methodological approach and an analytic phenomenon that this paper adopts.

I argue that Big Data's extensive harvesting of personal digital data is troubling, not only due to its implications for privacy, but due to the *particular way* in which that data is being utilised to shape individual decision-making to serve the interests of commercial Big Data barons. My central claim is that, despite the complexity and sophistication of their underlying algorithmic processes, these applications ultimately rely on a deceptively simple design-based mechanism of influence -'nudge'. By configuring and thereby personalising the user's informational choice context, typically through algorithmic analysis of data streams from multiple sources claiming to offer predictive insights concerning the habits, preferences and interests of targeted individuals (such as those used by on-line consumer product recommendation engines), these nudges channel user choices in directions preferred by the choice architect through processes that are subtle, unobtrusive yet extraordinarily powerful. By characterizing Big Data analytic techniques as a form of nudge, this provides an analytical lens for evaluating their persuasive, manipulative qualities and their legal and political dimensions. I draw on insights from regulatory governance scholarship, behavioural economics, liberal political theory, information law scholarship, Science & Technology Studies (STS) and surveillance studies to suggest that, if allowed to continue unchecked, the extensive and accelerating use of commercially driven Big Data analytic techniques may seriously erode our capacity for democratic participation and individual flourishing.

2. Big Data as a form of design-based regulation

My analysis begins by explaining how Big Data algorithmic techniques seek systematically to influence the behaviour of others, drawing on a body of multidisciplinary scholarship concerned with interrogating 'regulatory governance' regimes and various facets of the regulatory governance process.

2.1 Design-based regulatory techniques

Regulation or regulatory governance is, in essence, a form of systematic control intentionally aimed at addressing a collective problem. As Julia Black puts it, '[r]egulation, or regulatory governance, is the organised attempt to manage risks or behaviour in order to achieve a publicly stated objective or set of objectives' (Black 2014: 2).[1] Many scholars analyse regulation as a cybernetic process involving three core components that form the basis of any control system – i.e. ways of gathering information ('information gathering and monitoring'); ways of setting standards, goals or targets ('standard-setting'); and ways of changing behaviour to meet the standards or targets ('behaviour modification') (Hood et al 2001). Within this literature, the techniques employed by regulators to attain their desired social outcome are well established as an object of study (Morgan and Yeung 2007). While legal scholars tend to focus on traditional 'command and control' techniques in which the law prohibits specified conduct, backed by coercive sanctions for violation, cyberlawyers and criminologists have explored how 'design' (or 'code') operates as a regulatory instrument (Lessig 1999; Zittrain 2007; von Hirsh et al 2000; Clarke and Newman 2005). Although design and technology can be employed at the information-gathering phase (eg. the use of CCTV cameras to monitor behaviour) and behaviour modification phase of the regulatory cycle (eg. car alarms which trigger if unauthorised interference is detected), design-based regulation embeds standards *into* design at the *standard-setting* stage in order to foster social outcomes deemed desirable (such as ignition locking systems which prevent vehicle engines from starting unless the occupants' seatbelts are fastened), thus distinguishing design-based regulation from the use of technology to facilitate regulatory purposes more generally (Yeung 2008; Yeung 2016).

2.2 Choice architecture and 'nudge' as instruments for influencing behaviour

[1] This definition amalgamates various refinements to the definition of regulation which Julia Black has offered over time: see Black (2001), Black (2008: 139) and Black (2014:2).

Since 2008, considerable academic attention has focused on one kind of design-based approach to shaping behaviour – nudge - thanks to Thaler and Sunstein, who claim that a nudge is 'any aspect of choice architecture that alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives.' (Thaler and Sunstein 2008:6). The intellectual heritage of *Nudge* rests in experiments in cognitive psychology which seek to understand human decision-making, finding considerable divergence between the rational actor model of decision-making assumed in microeconomic analysis and how individuals actually make decisions due to their pervasive use of cognitive shortcuts and heuristics (Kahneman and Tversky 1974; 1981). Critically, much individual decision-making occurs subconsciously, passively and unreflectively rather than through active, conscious deliberation (Kahneman 2013). Drawing on these findings, Thaler and Sunstein highlight how the surrounding decisional choice context can be *intentionally designed* in ways that systematically influence human decision-making in particular directions. For example, to encourage customers to choose healthier food items, they suggest that cafeteria managers place the healthy options more prominently– such as placing the fruit in front of the chocolate cake (Thaler and Sunstein 2008: 1). Due to the 'availability' heuristic and the influence of 'priming', customers will systematically tend to opt for the more 'available' healthier items.

2.3 Big Data analytics as informational choice architecture

To understand how Big Data analytics techniques utilise nudge, we can distinguish two broad configurations of Big Data driven digital decision-making analytic processes:

(a) *automated decision-making processes:* Many common transactions rely upon automated decision-making processes, ranging from ticket dispensing machines to highly sophisticated techniques used by some financial institutions offering consumer credit, such as pay-day loan company Wonga (https://www.wonga.com/loans-online). Although varying widely in complexity and sophistication, not all of which rely on Big Data driven analytics, these decision-processes automatically issue some kind of 'decision' without any need for human intervention beyond user input of relevant data (or data tokens) and thus constitute a form of action-forcing (or coercive) design (Brownsword 2006; Yeung & Dixon-Woods 2010); and

(b) *digital decision guidance processes*: In contrast, digital decision 'guidance' processes are designed so that it is not the machine, but the targeted individual, who makes the relevant decision. These technologies seek to *direct or guide* the individual's decision-making processes in ways identified by the underlying software algorithm as 'optimal', by offering 'suggestions' intended to prompt the user to make decisions preferred by the choice architect (Sellinger and Seager 2012).

While automated algorithmic decision-making raises serious concerns (eg; Citron 2008; Citron and Pasquale 2014; Pasquale 2015), this paper focuses on Big Data driven decision guidance techniques. These techniques harness nudges for the purpose of 'selection optimisation'. Consider how internet search engines operate: in response to a query, Big Data analytic techniques mine millions of webpages with lightning speed, algorithmically evaluating their 'relevance' and displaying the results in rank order. In the Google search engine, for example, the most prominently displayed sites are 'paid for' sponsored listings (thus enabling firms to pay for search engine salience), followed by weblinks ranked in order of Google's algorithmically determined relevance. Although theoretically free to review *all* the potentially relevant pages (from the hundreds of thousands ranked), in practice each individual searcher is likely to visit only those on the first page or two (Pasquale 2006). Hence the user's click through behavior is subject to the 'priming' effect, brought about by the algorithmic configuration of her informational choice architecture seeking to 'nudge' her click through behavior in directions favoured by the choice architect. For Google, this entails driving web traffic in directions that promote greater use of Google applications (thereby increasing the value of Google's sponsored advertising space). Other algorithmic selection optimization techniques operate in a similar fashion, helping the user identify which data items to target from a very large population. For example, so-called 'predictive policing' techniques use Big Data analytics to identify the 'highest risk' individuals or other targets to assist enforcement officials determine their inspection priorities, thereby increasing the efficiency and efficacy of their inspection and enforcement processes (eg. Cuckier and Mayer-Schonberger: 186-189).

Although the concept of nudge is simple, Big Data decision-guidance analytics utilize nudge in a highly sophisticated manner. Compare a simple static nudge in the form of the speed hump, and a highly sophisticated, dynamic Big-Data driven nudge in the form of Google Maps navigation function. In neither case is the driver compelled to act in the manner identified as optimal by the nudge's architect. Hence a motorist approaching a speed hump willing to endure the discomfort and potential vehicle damage that may result from proceeding over the hump at speed need not slow down. Nor is the driver using Google Maps compelled to follow the 'suggestions' it offers. But if the driver fails to follow a suggested direction, Google Maps simply reconfigures its guidance relative to the vehicle's new location via algorithmic analysis of live data streams that track both the vehicle's location and traffic congestion 'hot spots' that are algorithmically predicted to affect how quickly the vehicle will reach its desired destination.

While the self-executing quality of many static forms of design-based regulatory instruments obviates the need for human intervention, so that the enforcement response is automatically administered once the requisite standard has been reached, this makes them a rather blunt form of control (Latour 1994: 39-40). Although vehicles should proceed slowly in residential areas to ensure public safety, speed humps invariably slow down emergency vehicles responding to call-outs. In contrast, Big Data driven nudges avoid the over and under-inclusiveness of static forms of design-based regulation (Yeung 2008). Big Data driven nudges make it possible for automatic enforcement to take place *dynamically* (Degli-Esporti 2014), with both the standard and its execution being continuously updated and refined within a networked environment that enables real-time data feeds which, crucially, can be used to *personalise* algorithmic outputs (Rieder 2015). Networked, Big Data driven digital guidance technologies thus operate as self-contained cybernetic systems, with the entire tripartite regulatory cycle continuously implemented via a recursive feedback loop which allows dynamic adjustment of both the standard setting and behaviour modification phases of the regulatory cycle enabling an individual's choice architecture to be continuously reconfigured in real-time in three directions:

a) refinement of the *individual's choice environment* in response to changes in the target's behaviour and the broader environment, identified by the algorithm designer as relevant to the target's decision-making, based on analysis of the target's constantly expanding data profile;

b) *data feedback* to the choice architect, which can itself be collected, stored and repurposed for other Big Data applications; and

c) monitoring and refinement of the individual's choice environment in light of *population-wide* trends identified via population-wide Big Data surveillance and analysis.

Big Data driven nudging is therefore nimble, unobtrusive and highly potent, providing the data subject with a highly personalised choice environment - hence I refer to these techniques as 'hypernudge'. Hypernudging relies on highlighting algorithmically determined correlations between data items within data sets that would not otherwise be observable through human cognition alone (or even with standard computing support (Shaw 2014)) thereby conferring 'salience' on the highlighted data patterns, operating through the technique of 'priming', dynamically configuring the user's informational choice context in ways intentionally designed to influence her decisions.

3. Are Big-data driven 'hypernudge' techniques legitimate?

Although hypernudging entails the use of 'soft' power, it is extraordinarily strong (i.e. 'soft' power need not be 'weak': Nys 2004). And, where power lies, there also lies the potential for overreaching, exploitation and abuse. How then, should the legitimacy of hypernudge be assessed, understood primarily in terms of conformity with liberal democratic principles and values rooted in respect for individual autonomy? Before proceeding, two considerations should be borne in mind. First, the massive power asymmetry between global digital service providers, particularly Google and Facebook, and individual service users cannot be ignored (Zuboff 2015) especially given that the scale of corporate economic surveillance via Big Data tracking dwarfs the surveillance conducted by national intelligence agencies (Harcourt 2014) particularly as the Internet of Things devices continues to spread its tentacles into every area of daily life (Peppett 2014). Secondly, Big Data hypernudging operates on a one-to-many basis. Unlike the speed hump which directly affects only one or two vehicles at any moment in time when proceeding over it, a single algorithmic hypernudge initiated by Facebook can directly affect millions of users simultaneously. Hence Facebook's soft algorithmic power is many orders of magnitude greater than those wishing to install speed humps to reduce vehicle speeds and is therefore considerably more troubling.

3.1 The Liberal Manipulation Critique of Nudge

Despite enthusiastic embrace by policy-makers in the USA and UK, Thaler & Sunstein's nudge proposals have been extensively criticised. Leaving aside criticisms of the idea of 'libertarian paternalism' which Thaler and Sunstein claim provides the philosophical underpinnings of nudge, two lines of critique have emerged: those doubting their effectiveness, and those which highlight their covert, manipulative quality. My analysis focuses on the second cluster of criticisms (the 'liberal manipulation' critique.)

(a) The illegitimate motive critique (the 'active' manipulation critique): First, several critics fear that nudges may be used for illegitimate purposes. Consider the so-called 'Facebook experiments' undertaken by social media giant Facebook by manipulating nearly 700,000 users' News Feeds (that is, the flow of comments, videos, pictures and web links posted by other people in their social network) to test whether exposure to emotions led people to change their own Facebook posting-behaviours through a process of 'emotional contagion' (Kramer et al 2014) provoking a storm of protest. Critics called it a mass experiment in emotional manipulation, accusing Facebook of violating ethical and legal guidelines by failing to notify affected users that they were being manipulated in the experiment (cf Meyer 2015). Facebook defended its actions as legitimately attempting 'to improve our services and to make the content people see on Facebook as relevant and engaging as possible' (Booth 2014). But five months after the experiments became public, Facebook Chief Technology Officer Mike Schroepfer acknowledged that it had mishandled the study, announcing that a new internal 'enhanced review process' for handling internal experiments and research that may later be published would be instituted (Luckerson 2014).

(b) The nudge as deception critique (the 'passive' manipulation critique): Secondly, even if utilised to pursue legitimate purposes, others argue that nudges that deliberately seek to exploit cognitive weaknesses to provoke desired behaviours entail a form of deception (Bovens 2008; Yeung 2012). The paradigmatic autonomous decision is that of a mentally competent, fully informed individual, arrived at through a process of rational self-deliberation, so that the individual's chosen outcome can be justified and explained by reference to reasons which the agent has identified and endorsed (Berlin 1969: 131). Yet the causal mechanism through which many nudges are intended to work deliberately seek to by-pass the individual's rational decision-making process, exploiting their cognitive irrationalities and thus entailing illegitimate manipulation, expressing contempt and disrespect for individuals as autonomous, rational beings capable of reasoned-decision making concerning their own affairs (Yeung 2012: 137). These concerns resonate with legal critiques which highlight how powerful internet intermediaries (such as Google), act as critical gatekeepers, with Pasquale and Bracha observing that search engines filter and rank websites based on criteria that will inevitably be structurally biased (designed to satisfy users and maintain a competitive edge over rivals), thus generating systematically skewed results aimed at promoting the underlying interests of the gatekeeper, thus distorting the capacity of individuals to make informed, meaningful choices and undermining individual autonomy (Pasquale & Bracha 2015).

(c) The lack of transparency critique: Pasquale and Bracha's concerns reflect growing calls for institutional mechanisms that can effectively secure 'algorithmic accountability,' given that sophisticated algorithms are increasingly utilised to render decisions, or intentionally to influence the decisions of others, yet operate as 'black boxes', tightly shielded from external scrutiny despite their immense influence over flows of information and power (Diakopoloulos 2013; Pasquale 2015; Rauhofer 2015). Critics of nudge also highlight their lack of transparency, drawing analogies with subliminal advertising which are widely regarded as unethical and illegitimate (cf Thaler and Sunstein 244). Although traditional nudge techniques vary in their level of transparency (Bovens 2008) the critical mechanisms of influence utilized by hypernudging are embedded into the design of complex, machine-learning algorithms, which are highly opaque (and typically protected by trade secrets: Rauhofer 2015; Pasquale 2006), thus exacerbating concerns of abuse.

3.2 Can these concerns be overcome via notice and consent?

Can these objections to the opacity and manipulative quality of hypernudging be overcome, either through individual consent to their use or because substantive considerations are sufficiently weighty to override them?[2] I will focus on the first of these possibilities, employing a rights-based approach viewed through the lens of liberal political theory (Raz 1986; Dworkin 1977) before interrogating this approach by drawing on insights from STS and surveillance studies. The right most clearly implicated by Big Data driven hypernudging is the right to informational privacy, given the continuous monitoring of

[2] In relation to big data surveillance techniques by government intelligence agencies, considerable discussion has focused on the extent to which interests of public and national security overrides fundamental rights, such as rights to liberty and privacy: in the USA, see for example The President's Review Group on Intelligence and Communications Technologies (2013).

individuals and the collection and algorithmic processing of personal digital data which hypernudging entails. Legal critiques of Big Data processing techniques (and their antecedents) have therefore largely centred on whether the systematic collection, storage, processing and re-purposing of personal digital data collected via the internet has been authorised by affected individuals thereby waiving their right to informational privacy.

Contemporary data protection laws rest on what Daniel Solove calls a model of 'privacy self-management' in which the law provides individuals with a set of rights aimed at enabling them to exercise control over the use of their personal data, with individuals deciding for themselves how to weigh the costs and benefits of personal data sharing, storage and processing (Solove 2013). This approach ultimately rests on the paradigm of 'notice and consent', which contemporary data protection scholars have strenuously criticised. Critics argue that individuals are highly unlikely to give meaningful, voluntary consent to the data sharing and processing activities entailed by Big Data analytic techniques, highlighting insuperable challenges faced by individuals navigating a rapidly evolving technological landscape in which they are invited to share their personal data in return for access to digital services (Acquisti et al 2015). First, there is overwhelming evidence that most people neither read nor understand on-line privacy policies which users must 'accept' before accessing digital services, with one oft-cited study estimating that if an individual actually read them, this would consume 244 hours per year (McDonald and Cranor 2008). Various studies, including those of Lorrie Crannor, have sought to devise creative, practical solutions that will enable on-line mechanisms to provide helpful and informative notice to networked users, yet all have been found inadequate: either because they were not widely used, easily circumvented or misunderstood (Crannor et al 2014-2015). Secondly, people struggle to make informed decisions about their informational privacy due to problems of bounded rationality and problems of aggregation: struggling to manage their privacy relations with the hundreds of digital service providers that they interact with on-line (Solove 2013: 1890) and finding it difficult, if not impossible, adequately to assess the risk of harm in a series of isolated transactions given that many privacy harms are cumulative in nature (Solove 2013: 1891). Thirdly, individuals' privacy preferences are highly malleable and context-dependent. An impressive array of empirical privacy studies demonstrate that people experience considerable uncertainty about the importance of privacy owing to difficulties in ascertaining the potential consequences of privacy behaviour, often exacerbated by the intangible nature of many privacy harms (eg how harmful is it if a stranger becomes aware of one's life history?) and given that privacy is rarely an unalloyed good but typically involves trade offs (Acquisti et al 2015). Empirical studies demonstrate that individuals' privacy behaviours are easily influenced through environmental cues, such as defaults, and the design of web environments owing to pervasive reliance on heuristics and social norms. Because people are often 'at sea' when it comes to the consequences of their feelings about privacy, they typically cast around for cues in their environment to guide their behavior, including the behaviour of others and their past experiences, so that one's privacy preferences are highly context dependent rather than stable and generalizable to a wide range of settings (Acquisti et al 2015). According to Acquisti and his colleagues, this extensive uncertainty and context dependence implies that people *cannot* be counted on to navigate the complex trade-offs involving privacy in a self-interested fashion (Acquisti et al 2015). Thus many information law scholars seriously doubt that individual acceptance of the 'terms and conditions' offered by digital service providers (including Google, Facebook, Twitter and Amazon), typically indicated by clicking on a web page link, constitutes meaningful waiver of one's underlying rights to informational privacy (Solove 2013: 1880-1903) which even the industry itself acknowledges is a serious problem[3].

The adequacy of a privacy self-management model is further undermined in the Big Data environment.[4] First, the 'transparency paradox', identified by Helen Nissenbaum, emphasizes that in the complex and highly dynamic information network ecology that now characterises the internet, individuals must be informed about the types of information being collected, with whom it is shared, and for what purpose, in order to give meaningful consent. But providing the level of detail needed to enable users to provide genuinely informed consent would overwhelm even savvy users because the practices themselves are volatile and indeterminate, as new providers, parties and practices emerge, all constantly augmenting existing data flows (Barocas and Nissenbaum 2014: 59). Yet to avoid information overload, reliance on simplified, plain language notices is also inadequate, failing to provide sufficiently detailed information to enable people make informed decisions (Nissenbaum 2011). Secondly, the right to informational privacy includes the 'purpose specification principle,' requiring data collectors to state clearly the explicit purpose of collecting and processing that data *at the time of collection*.[5] Yet, as Ryan Harkins, Microsoft's privacy lawyer observes, this principle is largely antiethical to the concept of Big Data,

[3] To quote Microsoft's privacy lawyer, Ryan Harkins, 'the informed consent edifice is cracking, because it places much of the burden on individuals who are expected to read privacy notices' … 'while the notice and consent edifice may have been cracking before, I think it's fair to say that big data threatens to obliterate it altogether because big data will mean that there will be even more data collected. It'll be overwhelming and it will make it extremely hard for individuals to provide effective consent or make informed decisions about all of the data that's being collected about them and about all of the prospective uses of the data….and this challenge will be compounded by the rise of the internet of things' per Harkins cited in Crannor et al 2014-15: 795-786.

[4] In the USA and Canada, this right is protected primarily through the Fair Information Principles through specific legislation in particular contexts while in the EU, it is primarily protected via the EU Data Protection Directive and the ECHR Article 8 right to privacy.

[5] In the EU Data Protection Directive, this is expressed in Art 6(1)(b) which provides that 'Member States shall provide that personal data must be… (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards' (EU Directive 95/46/EC). The OECD Fair Information Practice Principles includes the 'Purpose Specification Principle', which provides that '[t]he purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.' (http://oecdprivacy.org/)

which is all about collecting more and more data in the hope that you might subsequently be able to use it in unexpected ways (Crannor et al 2014-15). The public furore surrounding the Facebook experiments is instructive. Although Facebook claimed that all 700,000 individuals who were subjected to the experiment had provided informed consent by accepting Facebook's terms of service, critics claim that this fell well short of the 'informed consent' that underpins universally accepted ethical principles governing research on human subjects exemplified in the Helsinki Declaration (World Medical Association 2013). The affected Facebook users could not reasonably have expected that they would be subjected to systematic emotional experimentation when they accepted Facebook's terms and service, but nor is Facebook likely to have contemplated that possibility either, so it could not have specified this proposed purpose in its terms and conditions at that time (although Facebook could have notified affected users of its intention prior to conducting the experiment and offered them an opportunity to opt out).

Thirdly, the primary business model through which Big Data is being monetized preys directly upon the susceptibility of individuals' privacy behaviour to subconscious external influence, particularly the powerful heuristics associated with ostensibly 'free' services. The predominant business model for contemporary digital services is one of 'barter', with users agreeing to disclose their personal data to firms in return for services (Van Dijck 2014: 2000) under a 'free' rather than 'fee' for services revenue model, thereby eliminating an important barrier to adoption faced by firms seeking to attract new customers with initially high uncertainty about their valuation of the service offered (Lambrecht 2013). Yet, as behavioural economist Dan Ariely demonstrates, 'the power of free can get us to make many foolish decisions' (Ariely 2009). Accordingly, in a Big Data environment, existing notice and consent model *cannot* be relied upon to protect the right to informational privacy, given that individuals are typically asked to consent to the processing of their personal data at some future time, for purposes they could not reasonably have contemplated.

3.3 Authorising Deception?

Although digital privacy policies are often drafted in breathtakingly broad, open-ended terms that could be literally interpreted to include Big Data driven hypernudging techniques, these policies are inadequate to authorize their *deceptive* qualities. Deception is a prima facie moral wrong because it violates the autonomy of the person deceived, involving the control of another without that person's consent (Wendler 1996: 91). Thus in addition to the right to informational privacy, on-line digital users have a separate and distinct right not to be deceived, rooted in a moral agent's basic right to be treated with dignity and respect. Thus, even assuming that routine acceptance of on-line privacy notices constitutes valid consent by a user to the sharing and processing of her personal data on-line, this consent does not *thereby* constitute a concomitant waiver of her right to not to be deceived. For this, specific consent to the use of techniques of deception is needed. Consider, for example, a cafeteria manager who, wishing to encourage healthier food choices, places the following sign at the cafeteria entrance:

> Many patrons want to eat healthy food but often have difficulty choosing the healthier items when selecting from the food on display. In order to assist then, we have arranged the food items on display with the healthier items displayed more prominently, making it more likely that customers will choose those items.

Although such a notice may overcome the manipulative, opaque qualities of the nudge in question (particularly if customers may leave the cafeteria and dine elsewhere), it is likely to distort the effectiveness of the nudge in eliciting the desired behavioural response. As Bovens puts it, the psychological mechanisms that are exploited by nudge techniques 'work best in the dark' (Bovens 2008: 3).

It is also doubtful whether disclosure by digital service providers that they are *withholding* material information is sufficient to overcome these objections, particularly if fundamental rights are implicated. Consider the practice of 'digital gerrymandering,' a term coined by leading American cyberscholar Jonthan Zittrain following the Facebook experiments to describe how easily social media platforms could utilize Big Data analytics actively to manipulate the voting behavior of individuals during an election campaign. For Zittrain, digital gerrymandering 'clearly seem wrong,' yet he struggles to articulate the nature of the wrong, suggesting it might constitute an 'abuse of a powerful platform' (Zittrain 2014). Might such a practice be acceptable if Facebook's terms and conditions included the following?

> The content of your news feeds is determined by an algorithm that has been constructed in ways intended to foster Facebook's success as a commercial enterprise.

This notice seems inadequate to authorize digital gerrymandering, because it fails to provide users with sufficient notice of the *deceptive* nature of the technique involved. Consider then the following more detailed statement:

> The content of your newsfeeds is determined by an algorithm that has been constructed in ways intended to encourage you to favour the views of political candidates favoured by Facebook.

By notifying users that relevant information of a certain kind will be omitted from their news feeds, users who are unhappy with this policy can stop using the service, while those who are content to proceed might be regarded as providing 'second order consent', thereby waiving their right not to be deceived (Wedler 1996) and their underlying democratic and constitutional rights to freedom of information and political participation. But second order consent processes would not overcome the objection that in practice, people do not read digital privacy notices, let alone properly comprehend their consequences. Furthermore, as Zuboff observes, the tools Google offers 'respond to the needs of beleaguered second modernity individuals – like the apple in the garden – once tasted, they are impossible to live without' (Zuboff 2015: 83).

Digital gerrymandering is an extreme example, but it nevertheless highlights how Big Data hypernudging techniques could be employed in ways that undermine individual autonomy and the quality of democratic participation. But what of techniques that are not so obviously deceptive nor directly implicate democratic participation – the kinds of practices that might be regarded as more akin to conventionally accepted marketing techniques used by firms to peddle their wares? What of the algorithmic design of Facebook functions aimed at keeping users logged in to Facebook, since the longer they linger, the more advertising they exposed to, thereby enhancing the commercial value of Facebook? As Bernard Rieder argues, Big Data driven algorithmic models are being used by institutions as a form of 'accounting realism' to 'sniff out patterns or differentiations in data and, by optimising for a target variable, transform them into (economic) opportunity' in pursuit of self-serving purposes (Rieder 2015). Yet liberal political theory has little to say about such techniques – if their use is adequately disclosed and duly consented to, there is nothing further of concern: individual autonomy is respected, while the market mechanism fosters innovation in the digital services industry.

4. Post-liberal Critiques: Selective Insights from STS and Surveillance Studies

The inability of the liberal political tradition to grasp how commercial applications of Big Data driven hypernudging implicate deeper societal, democratic and ethical concerns is ultimately traceable to its understanding of the self and the self-society relation. As Julie Cohen observes, within the liberal tradition, the 'self' as legal subject, has three principal attributes: (1) the self is a definitionally autonomous being possessed of liberty rights that are presumed capable of exercise regardless of context; (2) the legal subject possesses the capacity for rational deliberation and this capacity too is detached from contexts, situated within the tradition of Enlightenment rationalism in which the existence of universal truths amenable to rational discourse and analysis is presumed; and (3) the selfhood that the legal subject possesses is transcendent and immaterial - it is distinct from the body in which the legal subject resides (Cohen 2012). This, she argues, results is an emphasis on individual consent and a conception of privacy harm that is both economic and individualized so that the 'distress' associated with interference attracts little monetary compensation (Cohen 2012; Rauhofer 2015). Cohen laments US law's response to concerns about the genuineness of consent in networked environments by seeking to correct information asymmetries faced by the liberal consumer when consenting to data collection for profiling purposes (Cohen 2015). For Cohen, by looking to economics rather than sociology, which is more congenial to law's conventional grounding in philosophical commitments associated with liberal political theory (rather than political theory more generally), and to analytic philosophy rather than the sociology of knowledge, the centrality of consent in the liberal paradigm is reinforced, conveying the impression that there is nothing more at stake individually or collectively (Cohen 2015).

The liberal account's emphasis on consent flows naturally from the special significance of individual choice. My self-regarding choices are imbued with moral and political significance simply because they are *mine*, and it is presumed in liberal societies that they are worthy of respect, however foolish or unwise, for that reason alone. The core liberal idea of personality articulated in terms of personal autonomy demands that individuals be allowed to choose and pursue their different plans or paths of life for themselves *without interference from others* (Kleinig 1985). But what, exactly, constitutes an 'interference' with an agent's choice (Yeung 2016)? While coercive choice architectures (evident in the design of prisons, for example, or the gunman who offers his victim 'your money or your life?') clearly constitute interferences, what of the rearrangement of the informational choice architecture intended to nudge the agent's choices in particular directions? Choices cannot be made abstracted from their context: they are always made from a limited choice set or options and, so long as we interact others, the actions of others will affect the range of options open to us at any time (Wertheimer 1987). Yet from the liberal viewpoint, except in relation to pervasive choices (Raz 1986) one cannot object simply on the basis that the actions of another have reduced the scope of one's choices. As White reminds us, when I take the last seat at the bar, you have to stand or go find somewhere else to drink and, from the liberal perspective, there is nothing problematic about this (White 2010).

But conventional liberal accounts of individual autonomy are criticised by those who highlight their problematic divergence from aspects of identity through which most of us define ourselves[6]. These critics point out that we are deeply enmeshed in identity-constituting relations, cultural and other connections, and that we have little or no choice over some aspects of the self (such as our embodiment) and which conventional liberal accounts fail to take seriously (Christman 2009). One strand of STS scholarship can be understood as taking these critiques even further, rejecting conventional liberal conceptions of the autonomous self by emphasizing the nature of human self-hood as both embodied and subjectively experienced (Kleinmann and Moore 2014) and thus offer a more realistic account of the actual, embodied experience of individuals and human decision-making. Rather than decontextualize and abstract the self from her environment, these inquiries focus on how individual self-understanding and self-development are pervasively shaped by the surrounding environment, including technological artefacts. Networked information communications technologies, like other artefacts, shape and mediate our relationship with the world around us and, over time, we come to perceive the world

[6] The concept of 'relational autonomy' offers a potentially fruitful approach: see Nedeksky 1990; Mackenzie and Stoljar (2000). I am indebted to Barbara Prainsack for drawing my attention to this literature.

through the lenses that our artefacts create (Verbeek 2006). As a result, networked information technologies directly configure citizens themselves, actively shaping the relationship between humans and their world, and the way in which they perceive and understand themselves (Cohen 2012).

So understood, Big Data hypernudging constitutes a 'soft' a mechanism of surveillant control. But, unlike the disciplinary control emphasised by Foucault and epitomised by Bentham's Panopticon (Lyon 2014: 6), Big Data's algorithmic control operates in a more subtle yet 'seductive' manner (Boyne 2000) via continuous feedback loops based on an on-line user's interactions, configuring individuals on-line by 'tailoring their conditions of possibility' (Cheney-Lippold 2011:169). The resulting form of control is both more potent and powerful than the kind of disciplinary control typically associated with pre-digital forms of surveillance which rely upon the coercive experience of living with the uncertainty of being seen (Lyon 2007: 59). Yet this process is essential to an emerging form of information capitalism which Shoshana Zuboff dubs 'surveillance capitalism', dominated by powerful transnational corporations ('surveillance capitalists') (Zuboff 2015). Unlike industrial capitalism, in which power was identified with the ownership of the means of production and which prevailed from the early to late twentieth century, the surveillance capitalism emerging at the dawn of the 21st century produces a new form of power, constituting a new kind of invisible hand in which power is now identified with ownership of the means of behavioural modification (Zuboff 2015: 82). It rests on a default business model that depends upon 'eyeballs' rather than revenue as a predictor of remunerative surveillance assets (Zuboff 2015: 81).

While Zuboff regards Google's products and practices as the leading exemplar of surveillance capitalism at work, Facebook's News Feed algorithm vivid illustrates the role of algorithms in this emerging 'logic of accumulation'(Zuboff 2015). Victor Luckerson has recently described how News Feed's controversial emergence in 2006 has evolved into 'the most valuable billboard on Earth', tracing its evolution from a fairly crude algorithm based on essentially arbitrary judgments by software engineers assigning point scores to different features of Facebook posts to determine their ranking, into a complex machine learning system that provides a much more individualized user experience, in which the algorithm adapts to users' behavior – for example, people who click on more photos see more pictures, and those who don't see fewer (Luckerson 2015). Because the average Facebook user has access to about 1500 posts per day but only looks at 300, most see only a sliver of the potential posts in their network each day: hence algorithmic ranking critically determines how these posts are filtered and highlighted in users' News Feed (Luckerson 2015). Facebook therefore invests substantially in developing its News Feed algorithm, claiming to use thousands of factors to determine what shows up in any individual's news feed, and typically making two to three changes to the algorithm weekly. This is Zuboff's surveillance capitalism in operation, undertaken by Facebook for purposes that are portrayed as offering customers a highly personalised, 'meaningful' informational environment that is dynamically and efficiently updated in ways ultimately designed to foster and entrench Facebook as the leading global provider of social networking services, thus securing and expanding its revenue base.

5. Conclusion

I have demonstrated how Big Data driven decision guidance techniques can be understood as a design-based instrument of control, operating as a potent form of 'nudge'. The algorithmic analysis of data patterns dynamically configure the targeted individual's choice environment in highly personalised ways, affecting individual users' behavior and perceptions by subtly molding the networked user's understanding of the surrounding world. Their distinctly manipulative, if not straightforwardly deceptive, qualities arise from deliberately exploiting systematic cognitive weaknesses which pervade human decision-making to channel behaviour in directions preferred by the choice architect. Yet for liberals, except in clear cases of deception, and provided that the targeted individual consents to the deliberate configuration of her informational choice environment, having been duly notified of the choice architect's purpose, there is nothing especially troubling about them (Ford 2000). It is this largely liberal perspective that informs the work of many privacy law scholars, who highlight the inadequacy of notice and consent procedures in digital, networked environments, emphasising the systematic failure of users to either read or properly understand the significance of digital privacy policies so that the action of clicking on a website to indicate user acceptance typically falls well short of the informed consent required to authorise interfere with fundamental rights.

Yet the liberal focus on notice and consent fails grapple with the particular *way* in which Big Data algorithmic techniques exert behavioural influence through the hyperpersonalisation of individuals' informational choice environments. Optimists, such as Eric Goldman, argue that the algorithmic manipulation of general search engine results need not concern us because the efficient functioning of markets will ensure that alternative search engines will emerge to provide algorithmic evaluations that better meet individual needs (Goldman 2006). But this fails to recognise that the selective omission of relevant information can be deceptive, yet is virtually impossible for affected users to detect. Moreover, such naïve faith in the market as a vehicle for securing algorithmic accountability seems completely misplaced given the opacity of the underlying algorithms and the lack of awareness or understanding by many digital service users of their significance and operation (Karahalios 2014) and the dominance of a handful of extraordinarily powerful transnational companies in a global networked market for digital services.

Big Data digital guidance technologies are proving difficult for individuals to resist, operating through subtle persuasion rather than blunt coercion (Ford 2000). Supported by the prevailing neoliberal ideology that has fuelled the rapid growth of the Big Data industry, these applications 'beckon with seductive allure' (Cohen 2012) offering myriad modern conveniences that offer bespoke, highly personalised services that are algorithmically designed to respond rapidly, dynamically and as unobtrusively and seamlessly as possible. By willingly and actively allowing ourselves to be continuously, pervasively and increasingly subjected to Big Data hypernudging strategies, our relationship with the emerging commercial Big Data Barons takes the form of what Natasha Dow Schull refers to as 'asymmetric collusion'. Dow Schull's observations refer to the relationship between gambling addicts and the US gambling industry, in which the latter maximises its returns by successfully harnessing the power of algorithmic analytics to adapt the design of both casino layouts and the gambling machines which they house, in order to 'give players what they want'(Dow Schull 2012). The relationship between commercial Big Data-driven service providers and individual is similarly structured: through our increasing willingness to submit ourselves to continuous algorithmic surveillance in return for the highly tailored convenience and efficiency which their selection optimisation tools appear to offer, we also engage in a process of asymmetric collusion that threatens ultimately to impoverish us. Like so many addictions, our short term cravings are likely to be detrimental to our long term well-being. By allowing ourselves to be surveilled and subtly regulated on a continuous, highly granular and pervasive basis, we may be slowly but surely eroding our capacity for authentic processes of self-creation and development (Cohen 2012). While lawyers might be tempted to dismiss these concerns on the basis that 'we have given our informed consent', evidenced by our willingness to incorporate these services into our daily lives, this consent is arguably is more akin to that of the compulsive gambling addict (Dow Schull 2012) than that the liberal ideal of the autonomous self. The neoliberal self is primarily a consumer of digital services, rather than a politically active citizen engaged in processes of public deliberation that characterise the deliberative democratic ideal (Gutman and Thompson 1996). As Zuboff chillingly observes, Google's tools are not the objects of value exchange, but 'hooks' that 'lure users into extractive operations that turn ordinary life into the daily renewal of a 21st century Faustian pact' (Zuboff 2015: 83-84). Yet, she points out that, unlike former industrial capitalists, who were dependent upon institutionalised reciprocity between employee and consumer populations in the form of durable employment systems, steady wage increases and affordable access to goods and services for more consumers, surveillance capitalists are structurally independent from their populations, thus allowing them and their practices to escape democratic scrutiny (Zuboff 2-15: 80).

To take seriously the implications of the Big Data revolution that we are currently embarking upon, we must lift our eyes beyond the familiar liberal fixation with notice and consent (Brownsword 2004). Before succumbing to the allures of the convenience and efficiency that Big Data claims to offer, we must be attentive to its regulatory power, operating as a particularly potent, pervasive yet 'soft' form of control, modulating our informational environment according to logics that are ultimately outside our control and which erode our capacity for democratic self government (Cohen 2012). As we increasingly retreat into our own algorithmically determined 'filter bubbles' (Pariser 2012) our exposure to shared, diverse and unexpected experiences that are essential to sustain our capacity for individual flourishing and democratic engagement is correspondingly diminished. If we are to avoid narrow and commercially filtered, algorithmically determined lives, we must establish more effective, practically enforceable constraints to tame the excesses of Big Data driven hypernudging which will secure meaningful accountability over the algorithms that exert ever more influence on our lives, in ways that allow genuine democratic participation and input into the design of the networked digital technologies which we increasingly find so irresistible.

8991 words (everything)

References

Acquisti, A., Brandimarte, L., & Lowenstein, G. (2015). Privacy and Human Behavior in the Age of Information. *Science,* 347, 509-14.

Ariely, D. (2009). *Predictably Irrational: The Hidden Forces That Shape Our Decisions*. London: Harper Collins.

Barocas, S., & Nissenbaum, H. (2014). Big Data's End Run around Anonymity and Consent. In J. Lane, V. Stodder, S. Bender & H. Nissenbaum (Eds.), *Privacy, Big Data and the Public Good* (pp. 44-75) New York: Cambridge University Press .

Berlin, I. (1969) Two Concepts of Liberty. In I. Berlin, *Four Essays on Liberty* (pp. 118-172) London: Oxford University Press.

Black, J. (2001), Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. *Current Legal Problems,* 54, 103-46.

Black, J. (2008) Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes. *Regulation & Governance,* 2, 137–64.

Black, J. (2014). Learning from Regulatory Disasters, Sir Frank Holmes Memorial Lecture, Retrieved from: http://www.ssrn.com/en/.

Bovens, L. (2008). The Ethics of *Nudge*. In T. Grune-Yanoff and S.O. Hansson (Eds.) *Preference Change: Approaches from Philosophy, Economics and Psychology*. Chapter 10. Dordrecht, Heidelberg: Springer.

Booth, R. (2014, June 30). Facebook Reveals News Feed Experiment to Control Emotions. *The Guardian*. Retrieved from: http://www.theguardian.com.

boyd, d., and Crawford, K. (2012). Critical Questions for Big Data. *Information, Communication and Society,* 15, 662-79.

Boyne, R. (2000) Post-Panopticonicism. *Economy & Society*, 29, 285-307.

Brownsword, R. (2004). The Cult of Consent: Fixation and Fallacy. *Kings College Law Journal,* 15, 223.

Brownsword, R. (2006). Code, Control, and Choice: Why East Is East and West Is West. *Legal Studies,* 25, 1-20.

Cheney-Lippold, J. (2011). A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control. *Theory, Culture & Society,* 28, 164-81.

Christman, J. (2009). Autonomy in Moral and Political Philosophy. *Stanford Encyclopedia of Philosophy*, http://plato.stanford.edu/entries/autonomy-moral/.

Citron, D., K. (2008). Technological Due Process. *Washington University Law Review,* 85, 1249.

Citron, D. K., & Pasquale, F . (2014). The Scored Society: Due Process for Automated Predictions. *Washington Law Review,* 89, 1-33.

Clarke, R.V. & Newman, G.R. (Eds) (2005). *Designing out Crime from Products and Systems*. Monsey, New York: Criminal Justice Press.

Cohen, J.E. (2012). *Configuring the Networked Self*. New Haven: Yale University Press.

Cohen, J. E. (2015). Studying Law Studying Surveillance. *Surveillance & Society,* 13, 191-01.

Cranor, L., Frischmann, B.M., Harkins, R. & Nissenbaum, H. (2013-14). Panel I: Disclosure and Notice Practices in Private Data Collection. *Cardozo Arts & Entertainment Law Journal,* 32, 781-812.

Cukier, K., & Mayer-Schonberger. V., (2013). *Big Data*. London: John Murray.

Degli Espoti, S. (2014). When Big Data Meets Dataveillance: The Hidden Side of Analytics. *Surveillance & Society*. 12, 209-25.

Diakopoulos, N. (2013, October 3). Race Against the Algorithms. *The Atlantic.* Retrieved from: http://www.theatlantic.com/world/.

Dow Schull, N. *Addiction by Design* (2012). New Jersey: Princeton University Press.

Dworkin, G., (1988). *The Theory and Practice of Autonomy*. Cambridge: Cambridge University Press.

Dworkin, R., (1977). *Taking Rights Seriously*. London: Duckworth.

Feinberg, J. (1989). *The Moral Limits of the Criminal Law Volume 3: Harm to Self*. Oxford: Oxford University Press.

Ford, R.T. (2000). Save the Robots: Cyber Profiling and Your So-Called Life. *Stanford Law Review,* 52, 1573-84.

Goldman, E. (2006). Search Engine Bias and the Demise of Search Engine Utopianism. *Yale Journal of Law & Technology,* 8, 188-200.

Gutmann, A., & Thompson, D. (1996). *Democracy and Disagreement*. Cambridge MA: Harvard University Press.

Harcourt, B.E. (2014) *Governing, Exchanging, Securing: Big Data and the Production of Digital Knowledge*. (Columbia Public Law Research Paper No 14-390). Retrieved from: http://www.ssrn.com/en/.

Hood, C., Rothstein, H., & Baldwin, R. (2001) *The Government of Risk*. Oxford: Oxford University Press.

Kahneman, D. (2013). *Thinking, Fast and Slow*. New York: Farrer, Strauss and Giroux.

Karahalios, K. (2015) Uncovering Algorithms: Looking inside the Facebook News Feed. Retrieved from https://civic.mit.edu/blog/natematias/uncovering-algorithms-looking-inside-the-facebook-news-feed.

Kleinig, J. (1978). Human Rights, Legal Rights and Social Change. In E. Kamenka & A Erh-Soon Tah (Eds.), *Human Rights* (pp. 136-147), London: Edward Arnold.

Kleinman, D.L. & K. Moore (2014). The Web, Digital Prostheses and Augmented Subjectivity. In P.J. Rey & E. Boesel (Eds.), *Routledge Handbook of Science, Technology and Society*, Whitney: Routledge.

Kramer, A.D. I., Guillory, J. E. & Hancock. J.T. (2015). Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks. *Proceedings of the National Academy of Sciences of the United States of America.* 111, 8788–90.

Lambrecht, A. (2013) The Economics of Pricing Services Online. In S.N. Surlauf & L.E. Blume (Eds.), *The New Palgrave Dictionary of Economics.* Retrieved from: http://www.dictionaryofeconomics.com/dictionary

Latour, B. (1994). On Technical Mediation - Philosophy, Sociology, Genealogy. *Common Knowledge.* 3(2), 29-64.

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. Basic Books: New York.

Lukerson, V. (2014, October 2). Facebook Changing Research Methods after Controversial Mood Study. *Time Magazine*. Retrieved from http://time.com/.

Lukerson, V. (2015, July 9). Here's How Facebook's News Feed Actually Works. *Time Magazine*. Retrieved from: http://time.com/.

Lyon, D. (2007). *Surveillance Studies*. Cambridge: Polity Press.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data & Society,* 1-13.

Mackenzie, C., & Stoljar. (2000). *Relational Autonomy: Feminist Perspectives on Autonomy, Agency and the Social Self*. Oxford: Oxford University Press.

McDonald, A. M., & Cranor, L.F. (2008). The Cost of Reading Privacy Policies. *A Journal of Law and Policy for the Information Society.* 4, 541.

Morgan, B., and Yeung, K. (2007). *An Introduction to Law and Regulation*. Cambridge: Cambridge University Press.

Meyer, M. N. (2015). Two Cheers for Corporate Experimentation - the A/B Illusion and the Virtues of Data-Driven Innovation. *Colorado Technology Law Journal.* 13, 273.

Nedelsky, J. (1990). Law, Boundaries and the Bounded Self. *Representations,* 30, 162-89.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus.* 140 (4), 32-48.

Nye Jr, J. (2004) *Soft Power*. New York: Public Affairs.

Pariser, E., (2012) *The Filter Bubble.* London: Penguin Books.

Pasquale, F. (2006). Rankings, Reductionism, and Responsibility. *Cleveland State Law Review.* 54, 115-38.

Pasquale, F. (2015). *The Black Box Society*. Cambridge MA: Harvard University Press.

Pasquale, F., & Bracha, O. (2015). Federal Search Commission? Access, Fairness and Accountability in the Law of Search. *Cornell Law Review.* 93, 1149-91.

Peppet, S. R. (2014). Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security and Consent. *Texas Law Review.* 93, 85.

President's Review Group on Intelligence and Communications Technologies (2013) *Liberty and Security in a Changing World*. Washington DC: Office of the Whitehouse.

Rauhofer, J. (2015). Of Men and Mice: Should the EU Data Protection Authorities' Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle. *European Data Protection Law Review.* 1, 5-15.

Raz, J. (1986). *The Morality of Freedom*. Oxford: Clarendon Press.

Rieder, B. (2015, February) On the Diversity of the Accountability Problem - Machine Learning and Knowledge Capitalism. Paper presented at the meeting of NYU Information Law Institute, Algorithms and Accountability Conference, New York

Shaw, J. (2014). Why "Big Data" Is a Big Deal. *Harvard Magazine.* 116 (4), 30-35.

Solove, D.J. (2013). Privacy Self Management and the Consent Dilemma. *Harvard Law Review* 126, 1880-93.

Thaler, R., & Sunstein, C. (2008). *Nudge*. London: Penguin Books.

Tversky, A ., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science.* 185, 1124-30.

Tversky, A, & Kahneman, D. (1981). The Framing of Decisions and the Psychology of Choice. *Science.* 211, 453-58.

van Dijck, J. (2014). Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. *Surveillance &Society.* 12(2), 199-208.

Verbeek, P.-P. (2006). Materializing Morality: Design Ethics and Technological Mediation. *Science Technology &Human Values,* 31, 361.

von Hirsch, A., Garland, D. & Wakefield, A. (Eds).(2000). *Ethical and Social Perspectives on Situational Crime Prevention*. Portland, Oregon: Hart Publishing.

Wendler, D. (1996). Deception in Medical and Behavioral Research: Is It Ever Acceptable?. *The Milbank Quarterly.* 74 (1), 87-114.

White, S. J. (2010, May). What's Wrong with Coercion? Paper presented at the meeting of the Society for Ethical Theory and Political Philosophy, Northwestern University.

World Medical Association (2013). Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Subjects. *JAMA.* 310, 2191-94.

Yeung, K. (2008). Towards an Understanding of Regulation by Design. In R. Brownsword & K. Yeung (Eds.) *Regulating Technology* (pp. 79-94). Portland, Oregon: Hart Publishing.

Yeung, K., & Dixon-Woods, M. (2010). Design-Based Regulation and Patient Safety: A Regulatory Studies Perspective. *Social Science and Medicine.* 71, 502-09.

Yeung, K. (2012). Nudge as Fudge. *Modern Law Review.* 75(1), 122-48.

Yeung, K. (2016). The Forms and Limits of Choice Architecture. *Law and Policy*, forthcoming.

Zittrain, J. Tethered Appliances, Software as Service, and Perfect Enforcement. In R Brownsword & K Yeung (Eds.) *Regulating Technologies*, Portland, Oregon: Hart Publishing.

Zittrain, J. (2014). Engineering an Election. *Harvard Law Review Forum.* 127, 335.

Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Informal Civilization. *Journal of Information Technology.* 30, 75-89.

8985words (everything)

7.3.16

Yeung Big Data as Hypernudge Short for Revised with Author Details 2016.docx