PHILOSOPHICAL TRANSACTIONS A

rsta.royalsocietypublishing.org

Research

Article submitted to journal

Subject Areas:
Ethics for Analytics

Keywords:
ethics, analytics, data science, modelling

Author for correspondence:
grindrod@maths.ox.ac.uk

Beyond Privacy and Exposure: Ethical Issues within Citizen-Facing Analytics

Peter Grindrod CBE

Mathematical Institute University of Oxford

We discuss the governing forces for analytics, especially concerning citizens' behaviours and their transactions, that depend on which of three *spheres* of operation an institution is in (corporate, public sector/government, and academic). We argue that aspirations and missions also differ by sphere even as digital spaces have drawn these spheres ever closer together.

We propose that citizens' expectations and implicit permissions for any exploitation of their data require the perception of a fair balance of benefits, which should be transparent (accessible to citizens) and justifiable. We point out that within the *corporate sphere* most analytics does not concern identity, targeted marketing, nor any direct interference with individual citizens; but instead it supports strategic decision making, where the data is effectively anonymous.

With the three spheres we discuss the nature of models deployed in analytics, including "black-box" modelling uncheckable by a human mind, and the need to track the provenance and workings or models. We also examine the recent evolution of personal data, where some behaviours, or tokens, identifying individuals (unique and yet non-random) are partially and jointly owned by other individuals that are themselves connected.

We consider the ability of heavily and lightly regulated sectors to increase access or to stifle innovation. We also call for clear and inclusive definitions of "data science and analytics", avoiding the narrow claims of those in technical sub-sectors or sub-themes.

Finally we examine some examples of unethical and abusive practices. We argue for an ethical responsibility to be placed upon professional data scientists to avoid abuses in the future.

THE ROYAL SOCIETY PUBLISHING

© The Author(s) Published by the Royal Society. All rights reserved.

1. Introduction

The pace at which citizen, customer, consumer and prosumer data is generated within evolving digital platforms raises a number of profound questions. In the UK the high household penetration of the internet and the “everything everywhere" expectation mean that participants of all ages are involved and exposed. The convergence of digital communications and mobile devices not only creates new digital spaces for the masses of individuals to act (e-commerce, 24/7 services, entertainment and media, social media, and opportunities to flaunt multiple digital personas), but it also provides essential and successful technology-driven *leap frogs*.

Digital platform operators (corporates, public sector, charities) may trap data that is itemising the behaviour of their users and they may curate and manage these digital resources (often at some considerable expense). That transaction data is analysed in order to provide some immediate response to the individual users, or else in the longer term it is repurposed and analysed for the strategic benefit of the platform and of its users (the latter strategic insights being often ignored or misunderstood by commentators, see section 5). This analysis is commonly referred to as “analytics" [1], and its function is to provide actionable insight. When operators are shifting from the old world into this new, data rich, world, this almost always drives a simultaneous change of culture. They switch from being service and supply-centric (focussing on how excellently, effectively and efficiently they can provide products and services to users) to becoming user-centric (understanding why and how their users interact with their offering, and seeking to grow certain types of user-behaviour) [4]. Of course some operators have no history prior to their digital incarnation, and in most cases they have operational and business models that rely explicitly on monitizing their users (beyond the actual user-platform transactions).

In the public sector we can see that digital platforms offer the chance to join processes up and to remove tiresome effort for citizens whilst creating efficiencies. The United Kingdom government portal https://www.gov.uk is a good example. Online car tax becoming linked both mandatory safety and performance testing and insurance information has made thing easier for many.

Recent discussions [2,3] have been held in the United Kingdom resulting in recommendations that a broad framework for the ethics of data science be adopted. In this paper we wish to focus on the *analytics* component of data science, and in particular we aim to reach beyond the issues of privacy and security, which often dominate yet are subject to existing legal instruments. We wish to highlight some of the ethical challenges within analytics practices in anticipation of any future agenda that may be set by the nascent United Kingdom Council for Data Ethics [3].

We shall consider a number of ethical issues that have implications for those working wiyhin data science in general and within analytics in particular. This is not meant to be an exhaustive review. The perspective adopted here is biased towards that of commercial (corporate) exploiters (looking outwards from commerce) rather than that of a public institutional or academic research standpoint. This is especially pertinent to ethics foresight for analytics as, over the past twenty years, data science has developed very rapidly so as to exploit proprietary corporate data, often and most radically by teams within data rich companies with access to data from their own digital platforms. Indeed, large scale data sets are rarely available, if at all, to academic researchers.

The dichotomy of the proprietary (rather closed) and the public/research (more open) data sciences, with their distinct histories and drivers, is highlighted in [1]:
“*Yet even before academic mathematicians became aware of this the genie was already out of the bottle. Many companies and institutions simply could not wait for the mathematical research community to catch up with the applications. The solutions to disruptive challenges and the novel opportunities so created were simply too valuable. ... Even the vocabulary was that of business competitiveness, and, for many analytics practitioners, like the author, it was essential that analytics was seen as the provider of a competitive edge, and an activity championed in business schools and adopted in boardrooms long before it crossed over into academic research with the mathematical sciences.*”

In the final section we shall summarize the key points from each of the particular challenges we have discussed.

2. Governing forces

We suggest that there should be a clear distinction made between the research programmes and projects carried out by individual academics and academic groups (and their communication with the public); the research and operations carried out by or on behalf of corporates, that have shareholders and lenders themselves and reputational value to protect; and the data science activities carried out by the public sector, including various arms of government. There is not a common code that is fit for all.

The "Responsible Research and Innovation" (RRI) framework for academic research is an approach that anticipates and assesses potential implications and societal expectations, with the aim to foster the design of inclusive and sustainable research and innovation. It is a key action of the "Science with and for Society" objective within EU Horizon 2020 [5], to be achieved both through thematic elements of RRI (public engagement, open access, gender, ethics, science education); and integrated actions that, for example, promoting institutional change to foster the uptake of the RRI approach by stakeholders and institutions. It thus appears to be self-perpetuating.

It is certainly necessary to govern the interventions and activities of academic researchers within digital spaces as these may not be fully accountable to any funders or those with reputations at stake; though universities, for example, have their own ethics committees. Such a framework is already redundant though within many commercial businesses where the stakes are so much higher. In general companies have a wide range of strategic and technical support to deal with reputational risks [6–8], and they are arguably far more savvy and risk aware than publicly funded researchers. Such support urgently needs to be extended into ethical domains, within fast paced, digital spaces.

The potential losses to shareholder value due to the perception of wrong doing or incompetence with customer/user data are enormous. Indeed the recent examples of VW's emissions software fraud [9], the cyber attacks on Talk-Talk [10], the recent "denial of service" attacks on British banks [11], and the newsworthy debate about profits and corporation taxes paid by Google and Vodafone [12] show how real are these reputation and value issues in providing a governor upon data science activities.

Moreover the public's attitudes can change and may leave businesses operating on the wrong side of the "creepy line", where their opaque activities are deemed to be unacceptable at worst or merely out of balance with the uses' benefits at best (see section 9). For example, an obvious project for analytics experts working with a loyalty card (for a supermarket chain, say) might be to collect the Twitter IDs of as many of its loyalty card members as possible. It might do so by running competitions or online raffles and inviting people to log in by their Twitter IDs. Once obtained the analysts could know about their customers' opinions, favourite TV, football allegiances, hobbies, and so on as well as which products they buy. This would in theory be great for both the customer and the retailer because they could better qualify savings and offers for people (personalised in terms of value and content), and generate more income from manufacturers (vendors). In the longer term this might build more loyalty and intimacy into the customer relationship management. The real problem here is that there is a very well understood balance of benefits derived from their loyalty card and the prospect of stalking their customers online might upset this (see also section 3). We know of no supermarket chain presently taking such a step without transparency and openness. The risk here, in terms of loss of reputation and shareholder value, is simply far too great.

The furore surrounding Facebook's emotions experiment [13] is worth considering in this "dual framing" because by stepping into an academic collaboration, and subsequently an open publication, the governing forces switched to include not only the usual corporate sphere constraints (user terms and conditions, data use policy, corporate reputation and transparency), which may or may not still have have legal consequences (with remedies such as changing the data use policy to say clearly that user data would be used for research purposes), but also the academic "responsible research" sphere, with both scientific and experimental constraints (those

of informed consent, the role of the internal review board, the potential harm that could be done, and fitness for publication by PNAS).

Increasingly ethical issues appear on the risk registers of companies and are up at a board level. Ethics foresight is in its infancy [14–16] yet it will become more essential and more obvious. It is especially relevant to sectors and activities that are underpinned by date science and analytics because their pace of change outstrips the ability of regulations to respond, and the data itself is often derived from individuals' behaviour on digital platforms. Companies cannot sleep walk into disasters. In other fields such as public policy making, law enforcement, counter terrorism, climate change, and energy supply there are horizon scanning and foresight activities (though of variable quality and exhaustiveness - hence the existence of "black swan" events). Many companies and public players who have an exposure to data and analytics should look forwards much more so as to consider (combinations of) possible events and issues such as those discussed here. It is the unknown unknowns that will be disruptive for good and ill. Ethics foresight for data science should become thus a key tool in de-risking investments within digital services, product and skilled jobs within the economy. It should be a "must have".

In [17] Richards and King raise three paradoxes (concerning transparency, identity and power, that are each reflected in sections of this paper). They conclude that
"*the answer must lie in the development of a concept of* Big Data Ethics – *a social understanding of the times and contexts when big data analytics are appropriate, and of the times and contexts when they are not.*"

Government departments and other public sector institutions have yet another set of governing forces. The public (and the media) holds such activities to a high standard concerning their aims, objectives performance (mission), and competencies. They have to do what is best for citizens and must be seen to be doing so. The strategic drivers for data science and analytics are from both policy and procedure. For example the public expects that government data is secure, perhaps much more so than of corporate data. In general in the UK there is a move to openness of public data (usually aggregated, non personal, data or national data resources such as maps, satellite images and so on). This is all to encourage innovation and better policy making [18]. The governing forces mandate the release or statistics (though often very far from real time and in aggregated ways that should not impinge on privacy) yet all too often data is published in inaccessible ways (the wide use of un-scrapable pdfs is galling).

An important way in which public sector data science differs from both corporate data science and academic research data science is that the government perpetually seeks to join disparate date sets together, usually around individuals. This could lead to efficiencies [19,20] as well as new ways of working. Thus, in the UK, HMRC data and crime data and health data and data on various interactions with social services, schools, immigration, passports office, and so on might all become joined. This challenge to "join the dots" is rather particular to the public sector domain data: supermarkets and mobile phone operators (usually referred to as MNOs) simply do their analytics over their own customer data (the "data is the data") and they only occasional seek to join data to other external datasets (for strategic reasons or following mergers and acquisitions) – those occasions are mostly one-offs. The national urge for "joining-up of data" also leads to concerns over its access, privacy, and the nature of personal information that is jointly owned or shared with others, as discussed in section 7 below.

The information broker is an obvious exception. Instead of dealing with its own proprietary and confidential data, it collects information, usually about a mass of individual people. The data is then sold on for targetted marketing purposes, for identity verification and detecting fraud, or for researching particular individuals. Clearly the joining up of data, in hard (logically matched) and soft (inferred) ways, is a key element. These brokers access public data (such as the electoral roll and other data set published by the government's open data initiatives) much more easily than they can any commercial data (for example, from an ISP, a e-commerce platform, or a loyalty programme).

Public sector data analytics must also engage with a wide range of potential users in a balanced way [21]. This is a crucial pillar of the United Kingdom's Open Government Partnership National Action Plans. Again this is highly distinct from corporate or research data science and analytics.

To summarise we argue that the governing forces, both constraining and driving data science and analytics, are rather distinct for three major "spheres": corporate, academic, and public sector. This has always been the case and those forces have mostly grown-up separately over many, many years. The challenge today is that all three sectors now inhabit the same digital spaces. They have converged onto digital platforms and they operate with common digital societies. We suggest that whenever any entity steps from one sphere into another sphere without anticipating the corresponding change in the governing forces this leads to large internal confusions (about what is right) and external confusion and possible harm. It is unhelpful therefore to address ethics and ethics foresight across these spheres; but rather their abilities, actions and aspirations should be contrasted. Equally it is simply a category error to export the present corollaries, practices and codes of working, that are subordinate to the governing forces, from one sphere to another sphere. For now *what is right* depends on the sphere that your are in.

3. Fairness and a Balance of Benefits

It is hard to be better than *free*. The power of free is compelling and it is well understood within behavioural economics [22]. We are used to free: Google, Facebook, Youtube, Twitter, Instagram, Linked In, are all free (at least in their simplest forms) while Ebay, Paypal, and Amazon are optional (pay if and when you transact). They provide fantastic feature-functionality and have become ubiquitous and depended upon within our lives. The users accept that there is a balance to be made. They get the free usage of these platforms/services and in return the company has a business model that somehow monitises their activity (their data) so as to make profit, then they build more cool applications and deliver them to the users free. Google Street View is a good example. There was (and is) clearly some invasion of public privacy and Street View may well provide some revenue-generating opportunities for Google, yet it is free to public users and most people use it habitually as a convenience. As such functionality becomes a routine part of our lives few people would ever wish to lose it. Similarly users accept that Facebook needs to have a business plan and to generate revenues in order to survive; yet many users could not conduct their social lives without relying on it. There is thus a balance where the members of the public know they are being exploited in some way, yet accept that in lieu of the clear benefits they recieve at no (or low) direct cost.

Loyalty cards do not drive loyalty, but they do allow holders to collect loyalty points over time that are redeemable in store, or with the airline, or the hotel, and so on. Users get offers and they get vouchers: sometimes as much as a few percent of their spending comes back to them. The loyalty card holders opt in - they may opt out if they wish. They get the customer benefits and in return the company collects longitudinal data on their transactions. This is used for a wide range of purposes (see section 5). Tesco plc, like many other retailers, believes their "Club Card" and their ability to understand their customers has been a key element in their growth over the past twenty five years or so. If Tesco invests abroad then it applies that element. It is a win-win: they anticipate and serve the customers better, and the customer get the immediate benefits as well as more things in the longer that people like them want to have (and may not even know it).

The perception of fairness is the key to trust here. It is a simple and transparent transaction, and it has the advantage of some immediate and quantifiable gain to the customers. Yet the absolute scale of the benefits is hard to assess.

Suppose that an energy supplier company finds some way to monitize its domestic customers' electricity smart meter data. For example it might sell it abroad to some foreign interest that is very curious about how people live in the United Kingdom (thinking that their own society and markets might develop in that way soon) yet have no intention of ever doing anything itself within the United Kingdom. The data would be providing some additional revenue back to the

energy supplier (does it matter how much?) yet there no incremental benefit at all to the domestic customers. Would customers not expect to share some of the bounty via reduced energy pricing?

What if an online store exchanges all of its basket data (rigorously annonimizing it first) with an online travel agent (so that the online travel agent could understand the sorts of things that people buy before they *disappear off the radar* for two weeks in August), in return for a free holiday for each and every member of its staff. The staff would each benefit and the online store would benefit from its more loyal and eager staff, excited and incentivised by their dividend holiday. The travel agent would benefit, by creating novel, insightful, new deals, products and services for pre-holiday makers. But the online store's own customers are not part of that. How much benefit would be acceptable, if it became widely known, before the customers wanted part of the action? Is it any different if the shareholders pocket the benefit as opposed to the staff?

The fair balance between the value to the platform (the data collector and operator) and the citizens/users must visible (even if not fully quantified). Since analytics offers companies the chance to create possibly many new value streams, monetising insights from the anonimized data assets (not by simply marketing more and more things back into its users) within their business model, this issue affects such activity disproportionately.

We suggest that there can be no user-perception of fairness, of the balance of benefits, if the users are in the dark as to the business models and the revenue streams of platforms. So where these may be opaque we feel that a qualitative explanation should be furnished to users. It is not necessarily the absolute value of corporate and customer benefits (the general user will have little wish to value the risks and the strategies within balance sheets) but it is a clear perception of mutual balance and respect that is most essential. On the other hand some companies may assert that the small print terms and conditions allow them to exploit their proprietary data (whilst holding to the permissions granted and their privacy commitments) in return for the large costs of its collection and curation. But while this may comply with the letter of the law it would be against a spirit of openness and transparency, and would erode trust.

4. Inclusion versus exclusion

Social inclusion (especially of poor, un-empowered, or minority segments) is concerned here with the use of big data and analytics by companies and institutions in ways that provide benefits to the whole of society (to all individuals and groups within society). In the recent US Federal Trade Commission report [24] it was emphasised that companies should have an understanding of the various laws, covering fair credit reporting, equal opportunities, civil rights, disability protection, employment law, fair housing, genetic information and nondiscrimination. These laws prohibit discrimination based on protected characteristics such as race, colour, sex or gender, religion, age, disability status, national origin, marital status, and genetic information. A focus on regulatory and legal tools is only ever part of the story since this generally shows how existing or possible legislation can prevent "bad things" from happening. The flip side of the coin is to avoid over regulation, that suppresses innovation or adds excessive cost and delays to business process, possibly preventing good things from happening, see section 8.

Often companies have a certain need for confidentiality and focus. They have to protect their existing customers from the competition, they protect their proprietary analytics methods and know-how, and they may protect their commercial strategies and interests. This is reasonable given that they have shareholders, lenders, and investors. The *secret sauce* within their analytics may be highly differentiating, allowing them to innovate new products and services. Yet the closed nature of proprietary data and proprietary analytics is very often read by commentators as if there is something to hide (and in some cases there may be). But this does not mean that companies should publish or make open their customer data or their methodologies. The data has not been sourced or collected at public expense and it is an asset of value to the company. Indeed, where the company's business model depends of using that data to drive their revenue channels then any publication would be reckless and would undermine their business. Of course keeping things in-house also creates some headaches for companies: their analytics is rarely benchmarked

(except by putting it into practice against competitors), and it is hard to manage the technical teams that may bamboozle their superiors (see section 2).

The power of data science to provide novel solutions to old problems is greatest when there is a growing and emerging market within society. Competitive advantages within focused market niches may be more fundable and investable than blockbuster products and digital personalisation is often a key differentiator. Any thoughts of deliberate exclusion though would be very counter productive and indeed the leap-frog nature of the innovation may deliver inclusion on a mass scale. Such inclusion is then at the very heart of the mission.

For example, with so many people the world over owning a mobile phone yet having little access to (any) financial services it is natural for a mobile network operator (MNO) to support simple m-wallets (cash-in and cash-out transactions). The next step is to allow such users to receive offers of small loans. Away from western economies there is no credit referencing available to the masses (since these rely on available financial track records of applicants); especially if users are on no databases at all and they cannot easily prove who they are and what they own (note that the rise of micro lending is stymied by its own face-to-face and paper driven processes). This is where a US company called Cignifi Inc (www. cignifi. com, initially started-up in the UK) stepped in. A customer of the MNO is on the MNOs own database with all their calls, texts and data transactions logged for billing purposes, for pre-pay and post-pay customers. Based on a few weeks worth of all such transactions (call taxonomy, day parts, week parts, duration, frequency, consistency, volatility, and so on) it is possible to segment user-behaviour at a very high resolution (without exploiting specific location information or text from messages or data, which are precluded by regulation). Then *guilt by association* applies and the experience of lending (the default rates, etc) is known within each segment. If a user's lifestyle and thus their behaviour changes then so may their behaviour-based credit reference. This is discussed further in [25] which details a 2010/11 collaboration with Oi Telecom (www.oi.br.com) and the Inter-American Development Bank (www.iadb.org) through its program"m-banking for the unbanked".

This exploits a double leap-frog since it provides loans and insurance solutions directly via the MNO without going through the conventional banks or credit agencies; and the MNO has already provided P2P communication, usually on an anonymous, pay-as-you-go, basis, without going through conventional land-lines and thus any user-registered telephone businesses. Operations such as Cignifi's would not be possible without data science and analytics, and a corporate perspective to drive its adoption: lending money widely while reducing the risk and thus keeping interest rates down.

Regulations to protect the customers' data privacy and prevent leakage also mean that Cignifi must typical work with the MNO's environment, and predictive analytics some details (message content and specifics of cell location) that are commonly held within the call data records. This incurs massive further cost and creates some hard challenges. But it is in every one of players' interests to get this right (see section 2).

5. What is analytics really used for?

Within commercial applications of data science (which are necessarily less open and less subject to independent challenge, for proprietary and competitiveness reasons) the data is often repurposed. That is, we gain access to possibly huge data samples that have not been collected with the analytst's true purpose, or any particular theory, in mind (and thus perhaps it cannot be theory laden [23]). This is clearly the case with analytics over loyalty card data and customer shopping basket data. The retailer's disaggregated data (the full list of products purchased within each basket or by each customer) is collected for a very straightforward purpose: that of billing at the till and the consequent award of loyalty points. It is collected and maintained at some expense within a database.

Many privacy and more general ethical commentators in the academic sphere (rather than those working within analytics in the commercial sphere) think that the primary use of retailer's data lies within the direct marketing (and targeting) of offers for yet more products and services:

if you buy dog food you may receive some dog product vouchers [26,27], or even Big Brother-like customer surveillance [28]. Yet any targeting activity actually takes place very soon after the basket data is collected (within weeks or months), and is the only such activity where the real identity of the customer is actually needed. The targeting itself is almost always logic (rule) driven: there is no smart inference or analytics present. There is no model there really: no *analytics*. Yet this raises issues of privacy and security (of personal information) along with issues of the appropriateness and frequency of direct communications and marketing.

In fact the most valuable usage of the customers' data occurs in a very different way and is not reliant upon the customers' personal details – merely using their unique ID (customer number) to string successive purchasing together, and some executive descriptions of their usual behaviour (their "segment", and their home store/region). This topic is described in [1], and includes many strategic activities (for the retailer) that are resolved by analyzing repurposed disaggregated basket/loyalty data, and in the process doing some modelling. These include customer behavioural segmentation and what type of behaviour is growing, customer behaviour and response to different formats of the offering, customer acquisition via different vectors, customer missions (how and why do customers shop?), investment into "stores within stores" and implants, pricing and promotion strategy, category ranging decisions, relative store performance, vendor intelligence sharing and support activities, the value of secondary displays, activity around specific events and festivals, and so on.

The simple point is that the real analytics within such a retailer, and the consequent need for ethics, is almost always aimed at these strategic questions and the consequent decisions made. These are very high value and high risk for the company and its shareholders, and also improve the offering for the customers as a whole. Yet too often ethical commentaries tend to be limited and obsessively wrapped up with the protection of the identity of, and the nature of access or communication with, the customers themselves. Neither of these is part of the *real* commercial sphere uses of analytics within these consumer-facing companies. These belong in the wider theatre of *ethics for business strategies and operations*, and not that of *ethics for analytics* addressed here.

6. The transparency of inferences, black boxes, and the end of theory or not.

The availability of very large data samples (so called "big data" resources) encourages those who would exalt the identification of structure and behaviour (within data) over theory:

> "This is the end of theory..." [29]
> "Every time I fire a linguist, the performance of the speech recognizer goes up." [30]
> "All models are wrong, and increasingly you can succeed without them." [31]

It is essential to delineate between at least two sorts of activities within data analytics: they can be thought of as data-driven analysis and theory-driven analysis. Confusingly they are sometimes referred to as "model-free" and "model-driven" respectively (by non-mathematical scientists), but this is to misunderstand the true nature of the term "model" (and "modelling", the art of discovering good models).

What is a model? We consider a sample space (a feasible set of possible observations equipped with a norm or a metric, and thus a topology) within which our many or few observations must live, and from which samples are drawn via some method or other. A "model" is a description of the structure observed within that sample space. Put more precisely, a model is a distribution defined over the sample space that describes the relative preponderance of the various different possible observations, or subsets of observations, exhibiting different types of internal structure in their attributes and relationships.

We may readily distinguish between two distinct classes of model (following [32,33] and the references therein), and the associated tasks of identifying the details of them. These issues are expanded further in [34].

Empirical models (data-driven). These are summaries of the observed distributions that are "discovered". They describe the sample and its properties. In the most extreme case the analyst will have (or rather will assert) no *a priori* view as to what the structure might be. The models may contain degrees of freedom (whether represented by a finite number of parameters, or possibly by an infinite number, whence sometimes called "non-parametric" – the distinction is a red herring for our purposes) which need to be calibrated to represent the distribution and structures inherent within the sampled observations. Such a model may be applied to new (incoming) observations to classify or complete them, thus inferring any element of the observation that is unknown (for example, in estimating some future behaviour if the object is dynamic, whence inference is called "forecasting"). Empirical models are just useful summary of the properties obvious or hidden within the sample.

Substantive models (theory-driven). These are distributions that describe the sampled data yet are constrained to reflect some underlying theoretical concept or hypothesis. Again, there will be some model parameters to be determined, reflecting the actual behaviour observed, and once tied down such a model, deemed to be significant and useful (accurate to some acceptable degree), may be applied to incoming observations and to make inferences. In this case those inferences and forecasts are made on the back of both the underlying theoretical ideas and the sampled observations. When substantive models are calibrated they may make a very poor description of the whole (because of their theoretical constraints), or there may even be some observations that contradict them. In the latter case either the observation is wrong or else the theory is falsified and a new paradigm must be sought. So we learn a huge amount from the falsification, or from even merely the poor performance, of substantive models. Hand argues [32] that if we ignore substantive models then we fail to extract the full value out of available data. With empirical modes we learn nothing general, only that the specific data can be well represented (or not) by the structures we have summarised.

Both types of model may invoke some parameters fitting and both may or may not incorporate a Bayesian prior expectations for such unknowns if the modellers have some expectation drawn from previous relevant expertise.

Empirical models often generate substantive models, almost immediately or in the course of time: this is very often the way of science. This is also true of commercial applications, where the interpretation of aberrations in data lead to insights that become substantive models to be tested.

In many applications, where there is a high degree of regulation or a right of challenge, the empirical models must be simple enough to allow some explanation (which covariate is driving a particular inference or decision – to lend money, or to deny an operation?). In such cases the choice of the possible structure must be severely curtailed - reduced to logistic regressions and score cards.

Where transparency is not needed, only unchallengeable performance, there is also an allowable "black box" mode of usage for empirical models (exploiting exotic classifiers and machine learning, in many forms) that do not require interpretation (explanation), and hence there is a successful pathway to exploitation. In cases such as online facial image recognition (for uploaded photographs on Facebook) [35], the empirical model (often in the form of a calibrated neural net or some other type of classifier) is simply deployed to remove grunt work for the user. When it fails, as it does occasionally, it is not catastrophic for users and is simply overridden by hand. The lack of transparency is traded for an ease-of-use within the non-critical nature of the activity. Such a lack of explanation would hardly be acceptable if its "victims" had some right of appeal, or the area of application (and the sector) was heavily regulated.

The ethical uses of models that we cannot watch or explain, or that act at scales which mean their working is unverifiable or uncheckable by a human mind, will become more problematic in the future. In cases where the models simply reduce work for humans this is acceptable and

aberrations are easily corrected. In applications where decisions are to made, beyond anomaly detection or prioritisation (for further action), then mistakes will occur. Of course all of this is predicated on some assumptions (no matter how hard the analyst tries to hide them) that the sample is not biased, that the data from the recent past is a good guide to any observations made in the future, and so on. For that reason alone there needs to be a more professional code of working amongst data scientists.

Finally, the discovery and calibration of (empirical and substantive) models is a very exciting and creative science, especially when the data is very large, will likely never be accessed again in the same way, and the sample structure very hard to classify and find. Once obtained though the models are usually employed blindly by others downstream. The know-how and possibly the assumptions actually made by the discoverers may not be available to those applying and operating. Thus there needs to be some traceability for models and modelling assumptions and constraints (just as we wish to trace foods from the farm to the fork). The professional data scientist should really be able to provide a traceable path from the original data science lab-based discovery of a model, and its calibration, into its myriad of possible applications (by machines very often). Log books for models? Or a free for all with no traceability and no provenance. These issues are relevant to all three spheres: transparency and traceability being essential in highly regulated sectors, or where there is a string need for public trust.

7. The nature of personal information

As more and more types of information become available for analysis it will become necessary to consider how such personal information is mapped to and from individuals. The simplest case is to have a unique ID for individuals: a name and address, or better still an NI (national insurance) number. There is a difference when the ID is unique and random (such as a loyalty card number) or unique and non-random (such as an name and address, part of which may be shared and thus connected to others). How about a fingerprint? For many years in the United Kingdom those accused of crimes have had their fingerprints taken and put on a UK data base. Often these are used in evidence since they may match scene of crime observations, and (modulo some highly expert interpretation) have a very low probability of false matches. They are (subject to expertise and subject to the quality of the observations) unique and random for the individual concerned

At the other extreme there is data which describes which of a large population segment an individual belongs to: hair colour, eye colour, race, age range, socio-economic grouping. Some of these are behavioural, some tribal (like football team allegiance), and some genetic.

But now we may collect data from individuals which is in nether class. This occurs when the observations are unique to the individual but are also related between pairs of individuals who are themselves closely connected somehow (and thus non-random). This particular problematic in the public sphere where there uses of data and analytics are held to the most stringent levels of accountability.

The most obvious example is the human genome. Consider the UK Police National DNA Database. This holds DNA profiles and relevant DNA samples from a select number of UK individuals. It is the largest database of its kind in the world and it is continuing to grow each year. Every profile in the database is derived from a sample collected from a crime scene or a police suspects. There are many people who are against the idea of extending the DNA database because of the potential threat it has to citizens' privacy [36] and the risk of data abuse is potentially high. But that is not our principal concern here. In fact in 2012, the UK Protection of Freedoms Bill aimed to redress the balance between the state's duty to protect the public and an individual's right to privacy. As a consequence 1,766,000 DNA profiles taken from innocent adults and children were deleted from the database.

The problem we raise here is that if you have a close relative in the database, then you may be identifiable from that profile. Though DNA is unique (except for identical twins) a close familial relationships between pairs of individuals can be inferred. In [37] there is a discussion of many of the ethical issues surrounding familial searching on the UK Police National DNA Database. This

in turn calls for much further thought about any other type of individuals' data that may infer relational (conditional) identities of other people should is stored and exploited. This is leading to a new area of research: group privacy [38].

Of course this is the flip side of many of the well-worn medical ethical questions arising when genetically based medical conditions are diagnosed within individuals with surviving relatives (and where mistakes may be rare or accidental [50], and thus notable).

In [37], referring to DNA databases, Haimes says the ethical considerations spread beyond identity (and privacy) issues and the part-connectivity of personal data has serious implications within people's lives and relationships:

"*What is remarkable to note here is the number of ways in which analyses of initially narrow aspects of genetics information tend to lead to [many more general] sorts of questions. Such questions might appear to be a long way away from my starting point of familial searching, but just as genetic information shows the interconnectedness of individuals, the analysis of questions surrounding familial searching also shows the far-reaching interconnectedness of social and ethical debates in law, medicine and families. The first point to make is that familial searching of forensic databases has potentially a far wider familial, community and societal impact than was first realized.*"

Kaye [39] argues more positively that familial matching should not be removed (as a permissible method of law enforcement information gathering) on constitutional grounds. Properly implemented, he states that it offers accurate leads in the investigations, and is compatible with constitutionally protected interests of both convicted offenders and their close relatives.

More recently in [40] the lack of almost any recognition that DNA is unique yet partly shared is discussed, pointing out that primary concerns over identity, security, and privacy have masked some deeper concerns over connectedness. Ram [40] says,

"*Courts, agencies, and legislatures have accepted that individuals have significant and cognizable interests in their identifiable genetic information. Many individuals appear similarly interested in protecting their identifiable genetic information from prying eyes. But the rules that these institutions embrace are largely under inclusive because they fail to take seriously the inconvenient fact that identifiable genetic information is involuntarily and immutably shared with close genetic relatives.*"

In the future there will likely be a number of similar challenges as novel digital assets and digital personas of *connected* people may exhibit connected properties, either in their digital behaviour, activities, opinions, or in their attributes, beyond any hard data. Suppose that some institution collects information on the behaviour of some digital asset (an account or an avatar, online, say), from a largish population sample, together with the corresponding hard identity and some hard attribute information of the individual (culture, race, beliefs, region, age, gender, socio-economic group...). The institution's analytics team may discover relationships (logical or merely correlations) between the digital behavioural attributes and the hard identity-based attributes. Nobody's behaviour (within digital space) is truly random: it would be very-hard work to be a totally random person. So the behavioural attributes constitute a non-random identity token, unique to the individual (given enough detail) yet with some relationship/similarity with those of others that are known to have a hard connection, say, some specific similar (or shared) hard attributes. As with DNA this could allow the searching of connected people not actually on the institutions database, yet connected in some way to a person who was on the database.

We suggest that in the future many broader concerns will be driven by the *connectedness of individuals*, which will become reflected in their digital activities, and facets of their digital behaviour. This includes digital identities and personas, that may be monitored and stored for a wide variety of highly legitimate purposes (trading, transactional, verification of identity, for example). And analytics will be the enabler of behavioural attributions of identify (connected or not). Whatever happens, the digital society will likely evolve much, much faster with respect to these problems than did the old non-cyber world of citizens rights, criminal databases and DNA. There is clearly a lot to learn from the last decade or argument and experience over connected, yet unique, personal identifiers. Some further clarification and insight will be required

here especially if data spaces are to be monitored routinely or otherwise "policed". There may be some implications for the Draft Communications Data Bill (2016).

8. Heavily and lightly regulated sectors

In some sectors the use of analytics has become very highly regulated; for competition, safety, security and inclusivity reasons, and operators are subject to a process that is overseen by government, generally to protect the citizens.

One such appears to be the development of new drugs by pharmaceutical companies [41], with the Association of the British Pharmaceutical Industry estimating that it costs on average £1.2bn to bring a new drug to market, and takes twelve years. This involves pre-discovery, actual discovery, pre-clinical trials, phases 1, 2 and 3 of clinical trials, and licensing stages. Almost all of these involve some data analysis. In many ways this whole pipeline is broken by bearing such costs, or through the pricing of drugs that NICE will not afford. So in fact the present process, imposed prior to licensing to protect citizens, is suffocating the industry and thereby putting citizens at risk. A creative way out of this is to have some pooling of information, sharing of targets at early stages and this supported by public money along side of multiple small and large corporations' investment, with only later stages becoming protected and competitive, see the "Bioescalator" concept in [42] for example.

About ten years ago the UK financial sector became acutely aware that the high degree of regulation had created barriers to new entrants to the retail banking sector. In essence this suppressed innovation and reduced choice for customers (at a time when the banking crisis pointed to many manifest failures of the incumbents). Yet the most powerful tool regulators have at their disposal is the ability to stimulate competition. New entrant, digital, banks challenge the status quo and a number have been licensed within the last few years. They are aligned perfectly with the growth of the enabling digital technologies and analytics. Some examples [43]: Atom Bank (digital only and plans an online-only current account); Fidor Bank (a social media and Web 2.0-based bank); Starling (a digital bank for tech-savvy consumers want and deserve more from their banks Ð they want easy, intelligent banking, not just mobile versions of paper statements); Charter Savings Bank (able to adopt modern technology, "unlike traditional banks which are held back by legacy IT infrastructures"); Hampden (cloud-based banking platform from Oracle); and Lintel Bank ("state-of-the-art IT", promises to open an account for a British citizen in just two minutes). Data science and analytics play a big part within these offerings, and the new business models continue to transform today's retail banking sector.

Elsewhere in the world, progress towards the mobile finance goal of "banking the unbanked" has been cautious within certain countries. While MPESA showed how m-wallets could work in Kenya more than a decade ago, others have held back, perhaps expecting the incumbent banks to respond themselves. Meanwhile the (global) MNOs have seen mobile banking as a strategic way to increase customer revenues and loyalty. In india things have now changed quite recently, and Kumar and Raman [44] state

"India's central bank, the Reserve Bank of India (RBI), has lagged behind other countries, moving gradually through a series of small steps to open up regulation for innovative models. However, on August 19, 2015, RBI finally took a massive catch-up step in digital finance, and, arguably, re-branded itself as innovation-friendly. It approved 11 applicants, including five of IndiaÕs MNOs, to organize and launch payments banks by early 2017."

In the UK energy sector the regulator, OFGEM, has run a number of research projects from 2010, funded by the £0.5B Low Carbon Network Fund [45], essentially trialing smart meters in a variety of ways, working through the regional distribution network operators (DNOs). However the programme did not require the projects to release any of the anonymised household smart meter data. The result was to inhibit innovation and to restrict access to those research groups actually tied into the projects. Arguably a much earlier release of the domestic smart meter data could have harnessed much effort from academic groups and micro companies. The sorry situation was not remedied until much later in 2015 when just one of the DNOs, UK Power

Networks, published the data in a form useful to other (qualifying) researchers [46]. The data was collected at the expense of existing energy customers.

On the other hand within sectors without any high degree of regulation (beyond privacy law and data protection) there is a much more creative and competitive zoo of data science activity. For example consider the retailers described above using their data and their analytics to better compete and serve their own customers. Or the digital marketing industry, which now outstrips every other advertising channel in the UK (exploiting analytics of search media and social media). In such cases, the discovery of what what works and some knowledge of why such methods can work has allowed companies to cease the indiscriminate broadcasting and move towards more personal marketing propositions. This in itself raises many interesting questions including which products and brands should be be targeted into social networks, for example, and will generate buzz; and which products are inappropriate for this and need to relay on broadcasting (on the backs of buses for example) [1,49]. Here the data exploited is usually proprietary data and its security is paramount (for reputational and shareholder value reasons for the corporate, and for privacy reason for the citizen – interests are highly aligned).

Between these two extremes lie activities where the location of the big data and its exploitation may be controlled (due to security concerns), or where the analytics may be able to access only part of the data (for very good privacy reasons, as in telephone call data records, for example). Or else some other partial constraints are applied. This often make life difficult for analytics to be carried out within the cloud, or elsewhere, at very low cost. So any tightening or constraint comes with a cost which must be borne by the company or its customers.

It is however the also the case that regulation and legislation has been used to close down certain innovative yet undesirable business practices (spyware and deceptive data collection) [47]. So we must distinguish between the ethics of dubious monitoring and data collection and the ethics of the data analytics.

The willingness of governments and regulators to seek legal constraints on data storage, analytics and applications is very clear. But given the global nature of digital platforms, the connected nature of digital spaces and the confusion over who is who, and who is where, this is increasingly problematic.

So the pace and nature of the digital economy undermines the old world of rather clunky regulation. In some cases it takes years for regulators to catch up (if at all), as was the case with P2P file sharing sites, that though not illegal in themselves, enabled violations of copyright and piracy; and yet was thought to be acceptable in some circumstances by a majority of those who were aware at that time [48]. More realistically new business models emerge from new disruptive players that see the ethical and regulatory gap as an opportunity to position something that is more functional, something of higher quality (than the wild west solution), and something that is more ethically acceptable to the public and the regulators. Sometimes arms races are opportunities.

Analytics, the activity of extracting isight, from large data sets - such as behavioural or transactional data, is the underpinning activity behind many new business models. To be able to deliver intelligent semi-automated services to customers/citizens at low risk (or else escalate *difficult* cases), in real time, working 24/7, will create new business models within digital spaces. across a wide range of sectors. The scaling and reach of digital offerings and their centralised deployment (hence central control agility) means that companies can run with low costs and evolve to meet customers' needs. For entrepreneurs this is a perfect storm. The role of regulators as both the gate keepers and arbiters of good practice must extend to ethical challenges. Since the data and the analytics may often both be proprietary (and confidential), the regulator cannot always see the practice and instead focusses on qualification of the players (who is doing what, why are they seeking to do it?) and the outcomes (what is the impact on the customer access and inclusivity, and on the market's entrants, the competition, and the barriers to choice), and policy. "Doing the right thing", responding to ethical challenges, may seem voluntary yet companies are subject to other governing forces, as discussed in section 2, such as reputation and shareholder value.

In summary we suggest that regulation is sometimes a blunt tool and may suppress digital innovation, at best by merely adding costs of the compliance and qualification barriers. The pace of change of digital platform development and adoption, as well as the nature of novel analytics, means that a regulatory response is relatively slow, and may be focussed on imposing existing rights (inclusiveness, privacy, copyright) upon operations.

9. Public opinion and attitudes and their pace of change

We have discussed the "creepy line" in section 2. It is interesting how often the prime minister and government ministers are found behind the curve of what is and is not acceptable to the public. Announcements appear to scramble to get onto the right side of an argument. We see this a-plenty in present debates about Syria and refugees. The public's opinion also intrudes into the Westminster-centric democratic process, not least via the petitions website.

In fact Pandora's box is open and it cannot be closed again now. Members of the public have a thirst for this and assert themselves through blogs, online chats, Twitter and petitions. And the wisdom of the crowd is often a lap ahead of policy and operations.

Two helping hands are available. First analytics: as analytics becomes real time, 24/7 and at a very large scale it may be possible in the future for companies, public institutions and governments to receive much earlier warnings and intelligence about changes in the public's mood and attitudes (see discussion in [51]). Second there needs to be more research on the issues of social norms within digital spaces which should yield a more subtle and useful taxonomy of attitudes. This is computational sociology resting on analytics; and is the heart of modern advances in social network analysis, community detection and much more, see [52] for example.

In the longer term there is the whole question as to what is and isn't acceptable as digital citizenship and participation. Just because a particular individual can do something, or aspires to do something, it does not mean that the government should react and engage. The principal of fair and wide access (inclusion) must apply. Yet the intelligence gathering (analytics) from observing digital society, including the wisdom exhibited by online crowds, should indeed be a principle tool of government, providing a secure environment for us to work, rest, and play online, looking after the digital aspirations of the nation, and creating wealth with high value jobs products and services. It is easy to scaremonger about data: with security and privacy (and by extension "ownership" of data) being in the foreground on such occasions. This can inhibit whole sectors so extreme care must be taken (for example the aborted smart meter roll-out in Holland). Not only must there be a balance between the outcomes and benefits (to the individual and wider society, as well as to the operating corporations/institutions), there also need to be a balance of effort made in informing the public's awareness and knowledge and in responding to public's concerns. For, as we noted in section 5, there may be a gap between what commentators and interest groups think that analytics is be used for and the actual aims, emphasis, activities of its practitioners, and the value created.

10. Programmes, Definitions and Practices

From an ethical standpoint any UK **national programme** in data science, such as that of the Alan Turing Institute, needs to set out strong governance structures around the investment of public and charitable monies, so as to (i) avoid conflicts of interests by having their present end-exploiters dominate their own senior and external advisory boards (this is avery common mistake in science programmes - the advisors have no interest in having the programme changing direction); (ii) counter special pleading of academic groups (with the those researching in particular fields too influential in strategic programme design) which reduces agility; (iii) avoid too much bottom-up programme design - a programme must have a clear mission (what will it delivery,when?), and be very assertive and precise about what success actually looks like.

There is much reinvention, of new from old, within data science and analytics. Nature abhors a vacuum, so without clear **definitions** many activities and subfields may enter into

the novel realm data science. Data science certainly contains elements to do with the capture, management, storage, curation, access and pre-processing of unstructured and structured data, and the distribution and performance of computes. Yet even if we focus solely on the analytics part, the art of distilling insights from data, we may find some activities that are understandable though questionable.

The re-badging of traditional statistics as analytics sometimes leads to rather expensive offerings to students that perhaps should be best avoided [53]. This is because they only represent a small part of the whole cannon.

It is simply an error to say that statisticians and others have for many years been doing *all* facets of analytics in the modern sense. For example, Donoho [54] says,

"This new field [Greater Data Science] is a better academic enlargement of statistics and machine learning than today's Data Science Initiatives, while being able to accommodate the same short-term goals".

Here Donoho is largely defining "analytics" as emerging from the existing machine learning and statistics perspectives – though he should perhaps give more prominence to other underpinning mathematical ideas. Modern applications of graph theory, numerical linear algebra, spectral theory for matrices and tensors, dynamical systems theory, computational topology, and stochastics and probability theory, all set within the context of very large and/or very constant steams of data, give rise to firm underpinnings of analytics too, along side of and applied statistics. and machine learning. It is clear that Donoho's vision of Greater Data Science is an enlarged and modernised activity, though perhaps not yet large enough. The vocabulary should be more inclusive. National programmes need to avoid subjective and restrictive definitions that preclude wide R&D: we do not know where the next game-changing concept will come from. We suggest that leadership needs to be both inclusive and visionary, and also mistrusting of apparent consensus.

The academic sphere's perspective of data science is very often biased towards analytics for machine, engineering, or scientifically generated data: monitoring, satellite, genome, imaging, voice, text, video, for a very wide range of applications. This is often because such data is readily available for open and publishable research. The citizen, customer, peer-to-peer, prosumer sources of data add up to much more than these though, and also underpin novel companies, products, services and economic growth. So there needs to be a constant rebalancing of effort in order to maximise impact. In sectors such as banking and security the emergence of new technologies such as distributed ledgers has the possibility of being disruptive - of changing the game. So, again, national programmes need to avoid restrictive definitions of applications that define safe, low risk, unadventurous research programs. This can be problematical where there is a requirement peer review or consensus building, which tend to avoid controversial or visionary elements.

Next we consider some examples of distinct types of **practice** within analytics and its exploitation which have the potential to mislead or to cause harm.

Visualisation, and especially the visualisation of big data, is quite often listed as an admissible component of analytics, though visualisation in itself is not always actionable. In many cases visualising data for the first time produces a powerful "wow" effect, as existing hunches and ideas are confirmed and new ones discovered. But the second time the image is viewed it is less exhilarating and the hundredth time it is unremarkable. This is a very common mistake in analytics. It is the actionability of the insight that counts. Visualisations need to be as dynamic as the data, and certainly as dynamic as the changes that can be effected on the data generators. Then users will come back again and again to confirm the consequences of their invested effort. Data visualisation also offers the opportunity to mislead viewers: in sometimes compelling ways [55]. So care must be taken not to overbias, oversimplify or bamboozle.

Sometimes the very size of data leads to issues when we search for inferences. Hand says [57]

"*The Improbability Principle tells us that events which we regard as highly improbable occur because we got things wrong. If we can find out where we went wrong, then the improbable will become probable.*"

The point is that the larger the data is the more we need to mistrust miraculous events: if the data is large enough than many low probability events will happen. Analytics professionals should

guard against such occurrences and must avoid being beguiled by unexpected relationships and structures. It should be part of a professional code for data scientists to guard against this, yet too often the rare or extreme event is presented without a true calculation of whether events such as these occur in data like this.

Quite common and un-professional is the allowance of an assumption of causality within observed relationships where there is no known causal link. Recently in [58] the authors stated "Screen time [at 14 years] was associated with lower academic performance [at 16 years], suggesting that strategies to limit screen behaviours among adolescents may benefit academic performance." This cautious "may" was somehow lost in the subsequent media reporting which went straight down the causal route, with no proven causal link [59]. In fact it is easy to construct the opposite casual link to explain the correlation: the subjects who were always relatively poor academically were destined to get poor results at 16 years. At the age of 14 they displayed an early warning to their parents by spending little time doing homework they felt would be beyond them and settling down to some relaxing screen time instead. The point here is that those in analytics should seek to avoid such causal interpretations being placed on their results without the necessary caveats. In [59] there appear no such caveats.

This leads us to suggest that there should be a general ethical responsibility places on data scientists to step forward and correct known abuses of their outputs that could lead to the profession falling into disrepute. The situation is entirely analogous to the intervention made by the Royal Statistical Society into the case of Sally Clarke, a victim of a miscarriage of justice, over the abuse of probability [60].

Instances of data scientific fraud appear to be rare to date. Intentional fraud often appears in sciences where data has been fabricated or results created in order to gain reputation, esteem and preferment for the authors. Such fraud is almost never seen within the mathematical and theoretical sciences, it is more prevalent in the experimental sciences. It will however no doubt occur more and more within data science and analytics too - both within public institutions and commercial ones, see [61] for a recent example of apparently fabricated data. In general the publication of data (allowing some reproducibility) and of methods is a safeguard. But in commercial sectors, or security sectors, such a lack of confidentiality may be highly undesirable. In such cases considerations akin to those encouraging "whistle blowing" might be required to protect institutions from malpractice within their own analytics teams, and data processors, and all that that implies. Events surrounding the access and capture of data itself and subsequent strategic practices and permissions come to mind, such as "Snowden", rather than the deliberate abuse or fabrication of false analytics and insights.

11. Conclusions

We have discussed how the governing forces for analytics, and especially analytics concerning citizens' behaviours and transactions, depend on which of three *spheres* of operation an institution is in: these are corporate, public sector/government, and academic. Confusion arises when institutions switch spheres or when ethical codes, standards and practices developed for one sphere are applied to another. The digital spaces have drawn these spheres ever closer together, and future ethics foresight and considerations (from the nascent Council for Data Ethics) should not treat these in a common way. The public does not appear to be naive about these distinctions.

The insights to be gained from data analytics are valuable to both the operators and the public, often the data generators on platforms: the public's implicit permission (beyond "terms and conditions") requires there to be a perceived fair balance of benefits. These benefits are not necessarily quantified (how does the user value the free functionality of Facebook or Youtube against the corporate profits made?) but they should be mutually respectful, visible, and justifiable. Where companies monetise data in otherwise hidden ways some qualitative description of those revenue channels should be accessible to users. At a minimum some statement about all present and known future uses of the data should be made in laymen's language and the extent to which that may have any impact on users, whether visible or not.

Analytics naturally segments citizens, by behaviour, risk, and their potential value to platforms. However there are clear commercial or operational benefits to be gained from being inclusive. On the other hand analytics should not be employed to infer customer attributes that may be used to discriminate unfairly against citizens where theses not directly relevant to the business propositions (which may be illegal). For example, behavioural insights might infer (by stealth) ethnicity, ability, culture, religion, IQ or the potential to behave in certain modes.

We have explained that most of the analytics carried out in the *corporate sphere*, over proprietary data, is not concerned with identity. Marketing and targeting applications are relatively straight forward and are carried out relatively soon after data is collected. Thereafter the true value of the customer/user data is in supporting strategic decisions: usually customers data is analysed to explain what it going on and what is likely to happen in the face of investments made under risk and managing and evolving the offering. These are very big calls and the companies' "behavioural insights teams" do nothing that involves the actual identities of the customers. They discover, monitor, and forecast the volumes and tendencies for customers to exhibit desirable and undesirable behavioural traits.

We have discussed the nature of data modelling within analytics: empirical (data driven) model descriptions of samples and substantive (theory driven) models. An extreme version of the former is black-box modelling based on methods that may be uncheckable by a human mind or that are inexplicable structural summaries, identified through machine learning, extrapolated and re-applied as *classifiers*. We suggest that the latter are simply inappropriate within some fields, mostly due to a lack of transparency. We also point to the "careers" that models themselves may have and the need for logs (traceable audits) to be available. This is most essential in the case where there have been many hands and no individual or team may be able to give a full account of the provenance and workings of a particular model (substantive or empirical).

The nature of personal data is changing at a pace, and in the future individuals may become identified with the behaviour of their digital assets (personas, accounts, entities in digital spaces). Where such tokens identifying individuals are unique (if fully disclosed) and yet non-random, some facets (attributes) may be jointly owned by individuals that are connected (or similar) in some way to the full owner. The individual should not be treated as if they are the sole and complete owner of the token and the token should not be treated as if it only identified the individual (and could not partly identify other connected individuals). Some further clarification will be required here especially if data spaces are to be monitored routinely or "policed". There may be implications for behavioural data collected under a future "snoopers charter" for example (the Draft Communications Data Bill at the time of writing in February 2016).

We have considered some heavily and lightly regulated sectors from the point of view of their ability to increase access and competition or to stifle innovation. These issues are particularly relevant given the pace of change in data science and analytics. Regulation may be slow to respond to innovations and inevitably be rather retrospective. Ethics foresight (the ability to foresee ethical challenges ahead) should become more routine.

We have discussed how public opinion and social norms may change, and thus introduce challenges to operational platforms. The "wisdom of the crowd" often evolves at pace and maroons previously accepted positions and opinions. Analytics (being 24/7 and responsive) could help here along with further research into computational sociology - both driven by data. Members of the public as prosumers have a desire to assert themselves through blogs, online chats, Twitter and petitions. This should be a welcome extension of participation and enrich our democracy.

We have highlighted some issues surround the setting up of a national programme (such as that of the Alan Turing Institute in the UK), involving data science and analytics. We have suggested that there should be clear and inclusive definitions of data science and analytics avoiding narrow claims from those in technical sub-sectors or sub-themes – there must be support for a very broad canvas. Moreover, as the profession become more mature, it will be morally wrong to allow any single "sphere" of operation (academic, corporate, or public sector) to define

the whole canvas in its own selective terms and thus exclude others. Leadership needs to be very visionary, not bottom up, and be mistrusting of any apparent consensus.

Finally we examined some examples of poor (unethical) practices where the misuse of analytics and the misrepresentation and misinterpretation of the derived insights might cause harm. We suggested that there should be an ethical responsibility placed upon data scientists to avoid abuses of analytics and the outputs that would bring the emerging profession into disrepute, or otherwise cause harm, and to intervene appropriately. This license to act is certainly up to and including whistle blowing and the public highlighting of malpractice.

Acknowledgements

The views expressed in this paper are those of the author and they do not represent the views for the Alan Turing Institute or its board. The paper has benefitted from conversations with those in corporations and academia, and most recently from those attending Whitehall-Alan Turing Institute round tables at the British Academy convened by GoScience (Spring 2016, at the British Academy). Especially the author would like to acknowledge many helpful discussions held with Jumbly Grindrod, Clive Bowman and Luciano Floridi.

References

1. Grindrod, P., Mathematical Underpinnings of Analytics, OUP, 2015.
2. The Opportunities and Ethics of Big Data – Workshop Report, Royal Statistical Society, 2016, http://www.rss.org.uk/Images/PDF/influencing-change/2016/rss-report-opps-and-ethics-of-big-data-feb-2016.pdf.
3. House of Commons Science and Technology Committee, The big data dilemma, Fourth Report of Session 2015Ð16, http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/468/468.pdf, HC 468, Published on 12 February 2016 by authority of the House of Commons London: The Stationery Office Limited.
4. Davenport, T.H., Harris, J.G., Competing on Analytics: The New Science of Winning, Harvard Business School Press, 2007.
5. Geoghegan-Quinn, M., (2012), Responsible Research and Innovation EuropeÕs ability to respond to societal challenges, from Science in Dialogue - Towards a European Model for Responsible Research and Innovation, Odense, Denmark, 23-25 April 2012, Science in Society http://ec.europa.eu/research/science-society.
6. Marsh LLC, 2016, Reputational Risk and Crisis Management https://www.marsh.com/us/services/marsh-risk-consulting/reputational-risk-crisis-management.html.
7. IBM, 2012, IBM Global Reputational Risk and IT Study, http://www-935.ibm.com/services/uk/gbs/bus/html/risk_study.html.
8. Deloitte, 2016, Perspectives: Reputation risk http://www2.deloitte.com/nz/en/pages/governance-risk-and-compliance/articles/reputation-risk.html.
9. Car Magazine, Volkswagen's emissions 'cheat' software scandal: an explainer, 25 November 2015.
10. Williams, C., TalkTalk cyber attack will cost company up to č35m. Technology, Daily Telegraph, Media and Telecoms, 11 Nov 2015. http://tinyurl.com/gp6m5lm
11. Osborne, H., HSBC suffers online banking cyber-attack, The Guardian, Friday 29 January 2016, http://tinyurl.com/z7vah4u
12. Murphy, R., GoogleÕs tax deal is another HMRC big business disaster, Tax Research UK, January 2016
13. Kramera, A.D., Guillory, J.E., Hancock, J.T., Experimental evidence of massive-scale emotional contagion through social networks, PNAS, vol. 111 no. 24, 8788Ð8790, doi: 10.1073/pnas.1320040111, 2014.
14. Floridi, L., 2013. The Ethics of Information. Oxford: Oxford University Press.
15. Floridi, L., 2014. The Fourth Revolution - How the infosphere is reshaping human reality. Oxford: Oxford University Press.
16. Sama, L.M., Casselman, R.M., Proceedings of the International Association for Business and Society, Vol. 25, 2014, Proceedings of the Twenty-Fifth Annual Meeting DOI:

10.5840/iabsproc20142510, Ethical Foresight in Business: Interpreting Societal Cues for Better Ethical Management, 2014.
17. Richards, N.M., King, J.H., Three Paradoxes of Big Data, Stan. L. Rev. Online 41, September 3, 2013.
18. Open Data Institute, Open data roadmap for the UK - 2015 http://theodi.org/roadmap-uk-2015.
19. Policy Exchange, January 2015, Small Pieces Loosely Joined: How smarter use of technology and data can deliver real reform of local government http://tinyurl.com/nrwxkow.
20. Peters, S., Joining the dots – Analysis and factual trends, new techniques, Blog, 15 October 2014, Civil Service Quarterly, GOV.UK, (2014) https://quarterly.blog.gov.uk/2014/10/15/joining-the-dots/.
21. Maltby, P., Re-engaging with our external data users, Blog, 10 December 2015, Data in government, GOV.UK, https://data.blog.gov.uk/2015/12/10/re-engaging-with-our-external-data-users/
22. Ariely, D., Predictably Irrational: The Hidden Forces That Shape Our Decisions, Harper Collins, 2008.
23. Pietsch, W., Draft. Aspects of theory-ladenness in data-intensive science. http://philsci-archive.pitt.edu/10777/1/pietsch_data-intensive-science_psa.pdf
24. Federal Trade Commission Big Data: A Tool for Inclusion or Exclusion? January 6, 2016. http://tinyurl.com/j99454j
25. Cignifi Inc., Building the Bridge to New Customers in Brazil, White Paper, available from www.cignifi.com, September 2011.
26. Murphy, P.E., Ethics of Marketing, Volume 2. Business Ethics, Published Online: 21 JAN 2015 DOI: 10.1002/9781118785317.weom020002
27. Frank, A., Teens in the Crosshairs: Is Targeted Marketing Ethical? American University, American Today, Campus News, September 14, 2011.
28. Smith, A., Sparks, L., (2003), Making Tracks: Loyalty Cards As Consumer Surveillance, in E-European Advances in Consumer Research Volume 6, eds. Turley and Brown, Provo, UT : Association for Consumer Research, Pages: 368-373.
29. Anderson, C., Wired Magazine, 06.23.08, The End Of Theory: The Data Deluge Makes The Scientific Method Obsolete. http://www.wired.com/2008/06/pb-theory/
30. Jelinek, F., IBM, an iconic quite usually attributed to the IEEE Automatic Speech Recognition and Understanding workshop held in 1985.
31. Norvig, P., Google research director, at the O'Reilly Emerging Technology Conference, March 2008.
32. Hand, D.J., Modern statistics: the myth and the magic (The address of the President, delivered to The Royal Statistical Society on Wednesday, December 10th, 2008) J. R. Statist. Soc. A (2009) 172, Part 2, pp. 287Ð306.
33. Hand, D.J., Brentnall A., and Crowder, M.J., (2008) Beyond empirical scorecards. Journal of Financial Transformation, 23, 121-128.
34. Grindrod, J. J. , Grindrod, P. , Data Science and Scientific Methodology, draft, 2016.
35. Anthony, S., FacebookÕs facial recognition software is now as accurate as the human brain, but what now? ExtremeTech.com, March 19, 2014, http://tinyurl.com/npaqtbw.
36. GeneWatch, Human Genetics, Privacy and Discrimination, The UK Police National DNA Database, http://www.genewatch.org/sub-539478.
37. Haimes, E., Social and Ethical Issues in the Use of Familial Searching in Forensic Investigations: Insights from Family and Kinship Studies, The Journal of Law, Medicine & Ethics, Volume 34, Issue 2, 263Ð276, 2006.
38. Floridi, L., 2016, Group Privacy: a Defence and an Interpretation, in Group Privacy - New Challenges of Data Technologies, Springer, Edited by Linnet Taylor, Bart van der Sloot, Luciano Floridi, forthcoming.
39. Kaye, D.H., The Genealogy Detectives: A Constitutional Analysis of 'Familial Searching', American Criminal Law Review, Vol. 51, No. 1, 2013, pp. 109-163.
40. Ram, N., DNA by the entirety, Columbia Law Review, Vol. 115, No. 4 (May 2015), pp. 873-939.
41. BBC Magazine, Monitor, Small Data: The huge cost of developing drugs, 12 May 2014.
42. City Deal: Oxford and Oxfordshire, Deputy Prime Minister's Office, The Rt Hon Greg Clark MP, The Rt Hon Nick Clegg MP and Cabinet Office, 30 January 2014

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/276205/Oxford-Oxfordshire-City-Deal.pdf
43. Flinders, K., 21 Jan 2015, Six challenger banks using IT to shake up UK retail banking, Computer Weekly, http://www.computerweekly.com/news/2240238535/Six-challenger-banks-using-IT-to-shake-up-UK-retail-banking.
44. Kumar, K., Raman, A., Did IndiaÕs Central Bank get Payments Bank Approvals Right? (2015) CGAP, http://www.cgap.org/blog/did-indiaÕs-central-bank-get-payments-bank-approvals-right.
45. Ofgem, Low Carbon Networks Fund https://www.ofgem.gov.uk/electricity/distribution-networks/network-innovation/low-carbon-networks-fund.
46. UKPN, http://innovation.ukpowernetworks.co.uk/innovation/en/Projects/tier-2-projects/Low-Carbon-London-(LCL)/
47. Stern, R.H., FTC cracks down on spyware and PC hijacking, but not true lies, Micro Law, IEEE MICRO (Jan.-Feb. 2005).
48. Cosgrove-Mather, B., Poll: Young Say File Sharing OK CBS News, 2003. http://www.cbsnews.com/news/poll-young-say-file-sharing-ok/
49. Grindrod, P., Higham, D.J., Laflin, P., Otley, A., Ward, J.A. ,(2016) Inverse network sampling to explore on-line brand allegiance, European Journal of Applied Mathematics, pp 1 - 13, DOI: 10.1017/S0956792516000085, Published online: 23 February 2016.
50. Allen-Mills, T., The Sunday Times, News, Frost's son was not told of fatal heart condition, 31 January 2016. http://www.thesundaytimes.co.uk/sto/news/uk_news/article1662811.ece?CMP=OTH-gnws-standard-2016_01_30.
51. Morabito, V., Big Data and Analytics: Strategic and Organizational Impacts, Springer; 2015 edition (Jan. 2015)
52. Newman, M.E.J., Networks: An Introduction, OUP, Oxford, 2010.
53. Krivanek, M., Data Science Courses to Avoid, Data Scince Central, June 4, 2015http://www.datasciencecentral.com/forum/topics/data-science-courses-to-avoid
54. Donoho, D., 50 years of Data Science, Sept. 18, 2015 Version 1.00, http://courses.csail.mit.edu/18.337/2015/docs/50YearsDataScience.pdf.
55. Kwapien, A., Remove Your Rose Tinted Glasses: Data Visualizations Designed to Mislead, The datapine Blog, News, Insights and Advice for Getting your Data in Shape, Dec 2nd 2015 http://www.datapine.com/blog/misleading-data-visualization-examples/.
56. Buzzfeed, The 10 Most Bizarre Correlations, posted on Apr. 11, 2013, http://www.buzzfeed.com/kjh2110/the-10-most-bizarre-correlations#.ofE5b5ZjL.
57. Hand, D.J., The Improbability Principle: Why Coincidences, Miracles, and Rare Events Happen Every Day, Bantam Press, 2014.
58. Corder, K., Atkin, A.J., Bamber, D.J., Brage, S., Dunn, V.J., Ekelund, U., Owens, M., van Sluijs, E.M.G., Goodyer, I.A., Revising on the run or studying on the sofa: prospective associations between physical activity, sedentary behaviour, and exam results in British adolescents, International Journal of Behavioral Nutrition and Physical Activity 201512:106 DOI: 10.1186/s12966-015-0269-2, 2015.
59. Burns, J., Extra screen time hits GCSE grades, BBC News, 4 September 2015, http://www.bbc.co.uk/news/education-34139196.
60. Sally Clark, Royal Statistical Society, News Release, Tuesday 23 October 2001, see http://www.sallyclark.org.uk/RSS.html.
61. Singel, J., The Case of the Amazing Gay-Marriage Data: How a Graduate Student Reluctantly Uncovered a Huge Scientific Fraud, nymag.com, the Science of Us, 2015 http://nymag.com/scienceofus/2015/05/how-a-grad-student-uncovered-a-huge-fraud.html