



Guernsey Financial  
Services Commission

## The Paradox in Big Data's relationship with Regulation and Freedom

### Introductory Remarks

Thank you for inviting me to speak here today about big data and the opportunities it offers. As William McChesney Martin, Chairman of the Federal Reserve remarked in 1955, the Federal Reserve, “is in the position of the chaperone who ordered the punch bowl removed just when the party was really warming up.” Whilst much has changed in the world of data in recent years – which of us has not marveled at populist works on the subject such as Mayer-Schönberger and Cukier’s “Big Data” – the role of the regulator has a certain constancy in terms of being there to tell unpopular truths at inconvenient times which others, because of their desire for fame or fortune, find it more difficult to tell. Like a monk, on becoming a regulator, you are meant to give up in your quest for fame and fortune. Being able to do so makes it easier to question popular established verities.

Let me start by way of anecdote. This summer we employed a number of summer interns to sort through more than five million pages or c. 1,750 boxes, scanning and shredding to make sure that by next Spring, if not a bit beforehand, the Commission is in a position where it is GDPR compliant. Whilst it was a bureaucratic chore, it will save us money on archive space in the longer term and I'd certainly commend doing something similar. That said, my purpose today is not to talk to you about how to be GDPR compliant but rather to talk about why, in my view, it is critical that we are careful about big data. Let me start off by reading you a few lines from the preamble to the GDPR itself,

“The processing of personal data should be designed to serve mankind. ... This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.”<sup>1</sup>

It is on the purposes and consequence of the use of big data that I will speak today. Data is, all too often, not used to serve the common good. To give you some regulatory examples, some things pretty close to what might reasonably be described as big data go into the construction of banks internal models under Basel II and Basel III and into insurance internal models under the terms of Solvency II in the European Union. As the financial crisis proved with regard to

---

<sup>1</sup> Section 4, Preamble to the General Data Protection Regulation - [http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf)

the Basel II internal models, the fact that a lot of data went into them didn't make them good of themselves. The data, in itself, may have been reasonable in some cases but the artifice which went into various banks' models was noteworthy. The assumptions embedded within the algorithms were proven by events to be in some cases naive, in other cases positively Machiavellian in that they were designed to paint a falsely comfortable picture about a whole series of exposures, which created, under even slightly stressed conditions, bankruptcy-inducing liabilities for the banks in question. Much good work has been done by my counterparts in the Bank of International Settlements in trying to improve the rules so that the models are better set up going forwards but, next time anyone talks to you about big data being able to aid understanding and solve problems, it is as well to remember the role models played in the financial crisis and how the black boxes designed to help large banks and regulators understand and manage vast quantities of data were actually quite capable of compounding misinformation and burying decent leading indicators of problems without a trace. There is nothing which is innately wonderful about big data – the uses to which it is put and the hands which manipulate it determine whether it, to quote the EU, it “serves mankind”.

### Charting the Course of Human Progress

I would argue that, over the past four centuries in the West, there has been a symbiotic relationship between human progress and some of the human rights cited in the preamble to the GDPR. From a British perspective, we can perhaps look at the writing of John Locke in the 1680s which justified the Whigs turning against the authoritarianism of James II and fermenting the Glorious Revolution whose principles were codified in the 1688 Bill of Rights. That bill, of itself, did not guarantee complete freedom of speech but it did guarantee freedom of speech within Parliament as well as ensuring full religious freedom for all Protestants, tantamount to freedom of speech, albeit couched in the rather clerical language of a more devout age. What this new toleration meant was that no one was allowed to use to coercive power of the state to enforce a particular view of the truth, a truly revolutionary innovation. From this grew through the 18th and 19th Centuries a culture in which - provided that one did not threaten another with violence - there was very considerable freedom of speech, thought and (wealth permitting) action. In this environment, mimicked to some degree by the United States through its Bill of Rights, science was free to question orthodox thinking whilst industrialists were free to experiment with new means of production which, whilst often enriching them, bought goods to the masses which were once the preserve of princes, thus spreading broad foundations upon which human progress could be built – both from the perspective of knowledge and material things.

What is noteworthy about this great age of human progress between 1689 and 1914 was how often established wisdom was wrong. What made the British Isles and the fledgling American Republic different from most other nations was the way in which freedom of thought and speech were allowed, enabling a few brave souls the liberty to challenge, to prove their case and to advance mankind without being unduly burdened by oppressive censorship and worse.

This tradition of free critical thinking was one in which I, as a cold war baby, was raised, the tradition in which both William Beveridge on the socialist side could write, “Full Employment in a Free Society” alongside Hayek's “The Road to Serfdom”. This, far more than the

distribution of wealth, is what divided East from West in the Cold War – we were free to speak the truth (or what we understood to be the truth) and they were not. I was brought up to consider this as possibly my most valuable birthright – that provided I did not threaten another human with violence I could say what I wanted and, at worst, people would merely dismiss me as an eccentric rather than seeking to sanction me for incorrect thinking. It was one of the things that made the UK special. Much has changed since I was a child. There have been huge further advances, often interestingly pioneered in the United States, a land whose constitution guarantees a considerably above average amount of freedom of speech and thought to those with enough energy or resources to take advantage of it.

The biggest advance, in so much that it has enabled a whole series of future advances, has perhaps been the internet.

### The Ability to Act

I remember reading George Orwell's 1984 for the first time and being horrified not so much by the rats as by the telescreen which listened to your every move, checking up that you were doing the things which Big Brother wished whilst refraining from thought crime. Now not only do we have televisions which constantly monitor us in our own homes but also toasters and kettles and nice little wrist sized trinkets that can and do monitor every inward movement of our bodies 24 hours a day, 365 days a year. The Internet of Things is I believe the marketing term for the vast array of surveillance equipment now semi-voluntarily installed in many modern homes. Not content with this, tech companies have lured an astonishingly large portion of the population into revealing their innermost concerns and fears on-line and sharing it not with one or two trusted soulmates but with everyone they have ever met as well as a few others besides.

This increase in monitoring by private and state sector actors, combined with the vast increases in computing power required to process the immense amounts of data collected have given rise to an ability to act – that is an ability to police deeds, speech and thought of which a true totalitarian such as Stalin could only have dreamed.

Many may say that all such technological advances are benign and whilst some technology company will sometimes overstep some privacy boundary and accidentally infringe Article 8 of the European Convention of Human Rights (ECHR)<sup>2</sup>, it is benign because providing you are not breaking a law, no one is stopping you doing anything. I would certainly like, building on the shoulders of others, to challenge such thinking.

In order to effect some change, you normally need to be both able to do something and to wish to do it. It logically follows that freedom is threatened when forces with the ability to act in a way which constrains freedom are combined with forces with a will to act in a way which constrains freedom.

I hope I have explained up to this point, in summary form, how structures with the ability to act against freedom exist now as never before in the history of human civilisation. As I will

---

<sup>2</sup> Article 8 is the right to respect for private and family life

now explore, the will to act to constrain freedom has increased markedly in the last few years in a number of ways.

### The Will to Act

I don't want to talk much about politics per se today. I will merely observe that that Francis Fukuyama's thesis in *The End of History and the Last Man* that Western liberal democracy's triumph may signal the end of sociocultural human evolution was wrong. Since he wrote that in 1992 various ideological movements have embedded themselves within Western society. These ideologies threaten the hugely beneficial Western consensus which has developed since the 1680s, that there should not be "truths" which are not open to challenge and intellectual debate. Whilst one may choose to agree or disagree with some of the ideological movements objectives it is difficult to deny that some wings of each of these ideological movements have sought to use totalitarian means to suppress those wishing to exercise their freedom to challenge the beliefs of some in the movement. Such ideologues have, in their belief that their version of the truth was so perfect sought to put their "truth" on a pedestal beyond legal challenge. They have, in other words, exhibited a will to act to suppress freedom of speech and thought.

Turning to the commercial sector, here the ability to act leads to an imperative to act. As Mayer-Schonberger and Cukier note in *Big Data of the Medici*, "In the 16th Century they became the most influential bankers in Europe, in no small part because they used a superior method of data recording, the double entry system." The case is scarcely different today with various tech companies having used their embedded data advantages to acquire positions which might, most politely, be described as oligopolistic. Still some of you may be thinking that this does not really matter as technology firms provide valued and ever improving services to you and your families. My contention is that this exploitation of your data really does matter rather a lot. Let me make the impact of the internet of things and social networks real by turning to insurance. As some of you may be aware, I chair the Audit and Risk Committee of the International Association of Insurance Supervisors (IAIS) and, whilst I do not claim in any way to speak for IAIS today, my work with it has developed my appreciation of the threat to freedom represented by the prospective use of big data by insurers and those seeking to act as service providers to insurance companies.

Let me start with telematics. I can remember, as a private sector strategy consultant more than fifteen years ago working on a pitch to a major international car manufacturer to help it develop its telematics strategy – the installation of monitoring tools on its cars to assist drivers and theoretically improve road safety, maintenance scheduling etc. Many of the things which the firm was then only just thinking about have now become near standard equipment on cars, not least of which are the so called black boxes which track exactly where you drive, at what times of day, how fast, constantly assessing whether you are starting to brake the recommended braking distance before a junction and condemning you to the degree that your behaviour does not fall within the norms of the model. I can remember passing my driving test as a youngish teenager and being able, that evening, to drive off in my father's car for the first time by myself. The sense of freedom and the possibilities which the endless roads presented were inspiring and empowering. How much less so in this fast approaching age where every movement is

monitored by a big brother insurance company capable of cancelling your cover at next to no notice or sending your parents nasty letters telling them how bad your driving has been. It also potentially allows covert discrimination using other measures as proxies for gender typical behaviours thus circumventing the European Court of Justice ruling that insurance must be gender neutral. Whilst many will argue with the inherent fairness of that particular ECJ decision given the very different behavioural traits generally exhibited by teenage boys behind a wheel when compared to girls of a similar age, the fact remains that this is a soft example of freedoms being indirectly damaged and, potentially, of illegal discrimination taking place through the backdoor of big data.

Then we have what some in the insurance industry like to term individually tailored insurance. Such a nice marketing term that. Who, after all, wouldn't like their friendly insurance agent or web adviser to tailor their insurance policy to meet their need ensuring that they didn't pay for cover they didn't require. I fear that reality could become somewhat more sinister as insurance becomes less of a commodity with pooled risk and more of a one way bet for the insurer against you. What it could mean, via the use of big data, is that insurance companies trawl through the reams of data held about you by technology companies and develop new algorithms based on combining their loss data with technology company data gathered through social networks and the internet of things to identify new key risk indicators for the provision of insurance. Thus, that "like" you gave to your friends ironic Greek holiday snap could potentially put £20 on your car insurance because the insurer's big data black box says that people who like Greek holiday photographs on a social network are statistically 5% more likely to have a serious car accident. Suddenly big data does not seem so much fun does it? The trouble is that you can't really blame the insurance companies because it is a case of eat or be eaten. If they don't do this, assuming the algorithms make some technical sense, their rivals will do it better and then undercut them on pricing for all the lower risk customers leaving the insurer which rejects big data with merely the loss making customers.

Lastly, let me turn to a really serious potential issue involving insurance. We now live in a world where you can take a sample and have it sent off for genetic profiling. Your doctors can also do this so they can work out what might be going wrong or what might go wrong with you in the future. That all sounds good until you realise that your insurers or their agents could also find a way to access that information as part of their haul of big data to evaluate what would be a suitably individually tailored health insurance policy for you. Or, even if you are careful about your privacy, you might find a close relative has done such a genetic profile and your insurer will work out the relationship and extrapolate from there. Suddenly, because of something over which you have absolutely no control, because of something you were born with or because you have a disabled relative, you find you can't afford your insurance premiums and your family has no medical cover. Suddenly the loss of the historic pooling of medical risk by insurers which served the common good even whilst it required those who were very healthy (and therefore, of course, statistically much more likely to be higher earners) to pay more seems rather a shame. In fact, depending on where you live and whether there is a viable state funded health sector, it might be quite literally terminal. Big data comes with big risks to society and particularly to vulnerable elements of society. I am not saying it is working like that here and now but I am saying that big data enables a quiet return to the sort of eugenics

rejected by Western society on the defeat of Germany in 1945 and that there are clear commercial pressures on insurance companies to go down such disturbing avenues in their use of big data.

### The impact on freedom

With the above theoretical examples about insurance, I hope I have shown some of the risks posed to Western society from the untrammled use of big data by one small part of the financial services sector and the chilling effect which that could have on freedom of movement, on affordability and on health outcomes. Let me turn away from insurance to potential uses of big data in what is sometimes called RegTech – the use of big data by regulators. Prof Cossin and Ong Boon Hwee, in their book *Inspiring Stewardship*<sup>3</sup>, set out how their teams used qualitative big data – annual reports and so forth - to deduce, on the basis of the use of certain set of words whether some companies were well run or badly run.

For example, companies which could reasonably be regarded as being well run tended to use emphatic words such as “absolute, always, completely, never, ever“ a lot. They also used the word, “yes“ more frequently than other companies. Conversely potentially badly run companies used extreme words to describe customer complaints and financial performance (extraordinary, super) whilst using the word “no“ more than other companies<sup>4</sup>. There were different traits depending on what area of a company was being discussed. For staff matters, the better rated companies used words such as “aligned, bonuses, career, colleagues, compensation, recognition“ a lot whereas potentially badly run companies used words such as “appraisal, assigned, dismissed, evaluated, job, hire“ and so on rather more<sup>5</sup>. The analysis was quite subtle but nonetheless potent.

Prof Cossin and Ong Boon Hwee show with a reasonable degree of scientific rigour, how certain words we use can be, in a big data world, used to deduce whether we are good or bad, competent or incompetent and so forth. If we substitute Prof Cossin’s focus on formal annual corporate filings as a means of judging goodness and badness and consider the alternative source of, “everything we have said within microphone distance of our smartphone in the last two years“ we may like to pause for reflection. How truly free can we be in a world of big data to express our real views on anything and to challenge established orthodoxies without automatic condemnation (with real adverse consequences for our lives) by programs analysing big data?<sup>6</sup>

This is not to say that there are not considerable advantages from some perspective from the innovations offered by big data. Certainly it is possible to see how its gathering and analysis of data from the homes of older people living alone could potentially allow them to remain safely in their homes for far longer than is currently the case, possibly allied to robotics able to

---

<sup>3</sup> P. 165-179 *Inspiring Stewardship* (Wiley) 2016

<sup>4</sup> P. 168 *Ibid*

<sup>5</sup> P. 169 *Ibid*

<sup>6</sup> See also p. 93 of *Big Data* which deals with the datafication of moods. Written by Viktor Mayer-Schonberger and Kenneth Cukier (2013) John Murray

deliver some caring services. What I am saying is that we need to be cautious because of how potentially threatening it is to critical rights and freedoms.

I'm sure all of you can't recite every part of the UN's 1948 Universal Declaration of Human Rights and the European Convention of Human Rights. I looked through them whilst preparing this talk and considered which of these are materially threatened by the unmediated use of big data. To take examples from the Universal Declaration:-

- Article 1 – All human beings are born free and equal in dignity. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.
- Article 12 – No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor attacks upon his honour and reputation.
- Article 13 – Everyone has the right to freedom of movement and residence within the borders of each state.
- Article 17 – No one shall be arbitrarily deprived of his property.
- Article 18 – Everyone has the right to freedom of thought, conscience and religion.
- Article 19 – Everyone has the right to freedom of expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. }

I could make a similar list from the ECHR as the EU has already done in its preamble to the GDPR. As Mayer Schonberger and Cukier observe, “In the era of big data the three core strategies long used to ensure privacy – individual notice and consent, opting out and anonymisation – have lost much of their effectiveness<sup>7</sup>“. They also observe that the problem with relying on big data predictions, such as those I set out above with regard to the insurance sector, is that doing so, “negates the very idea of the presumption of innocence, the principle upon which our legal system, as well as our sense of fairness, is based. And if we hold people responsible for predicted future acts, ones they may never commit, we also deny that humans have a capacity for moral choice.<sup>8</sup>“

To this it is also worth adding the issue of who is undertaking this deprivation of rights. Locke observed in his *Second Treatise on Government*, “The legislative neither must nor can transfer the power of making laws to anybody else, or place it anywhere but where the people have”.<sup>9</sup> The commercial entities undertaking the development and exploitation of big data have arrived at a situation where their actions could come pretty close to law making because of the pervasive power they have to enforce their big data derived judgements on large populations. Big tech are not, however, Locke's people or any other people recognisable as a description of those upholding the democratic will.

---

<sup>7</sup> *Ibid* p. 156

<sup>8</sup> *Ibid* p. 162

<sup>9</sup> Para. 142 *Second Treatise on Government* (1956 Edition) Blackwood

When exploitation of big data challenges so many human rights, dearly won by the West in the 1940s, rights built on the received wisdom of our ancestors as to what a highly civilised society could and should represent, we may have cause for caution.

What then of the paradox of my title? It is simply this: historically, advocates of freedom have defended a limited state on the basis that a pervasive state would threaten freedom. We may now have arrived at a situation where, in order to defend freedom and the human rights closely associated with that freedom, we may require rather more pervasive regulation of those exploiting big data to ensure that their actions do not breach Article 17 of the ECHR which prohibits any group or person from engaging in any activity or act aimed at the destruction of any of the rights. Thus the protection of human rights, the protection of those freedoms which have over the past three and a half centuries, helped the West advance civilisation and human wellbeing, require the increased regulation of the commercial sector to stop it privatising lawmaking and, de facto, adversely affecting human freedoms. This is deeply ironic given that it was only the freedoms of the West which created a climate in which the private sector could develop such extraordinary data processing capabilities.

If that sounds quite complex, it is because I think it is quite complex. I believe the European Commission has made a praiseworthy start to the endeavour of preserving freedom with the GDPR, irritatingly bureaucratic though many of us find its implementation. I believe the technology is moving so fast and the commercial pressures companies are experiencing to exploit big data are such that more will need to be done soon at an international level. This is difficult territory for both public servants and those in the commercial sector. I don't see many easy answers but I do believe that the politicians of leading countries need to address the clear and present threat which big data can present to human freedom and they need to act without further delay if the human rights we have enjoyed are to be upheld for our children.

**William Mason**  
**Director General**

**9 October 2017**