Big Data Protection

How to Make the Draft EU Regulation on Data Protection Future Proof

Lecture

delivered during the public acceptance of the appointment of professor of

Global ICT Law

at Tilburg University

on 14 February 2014 by

Prof. Dr. Lokke Moerel

Mr. Rector–Magnificus, my distinguished listeners!

Big Data Protection

How to Make the Draft EU Regulation on Data Protection Future Proof

> We shape our tools and thereafter they shape us
>
> **John Culkin (1967)**

Introduction

That new technologies have an impact on society is intuitively understood.[1] The essence of new technology's transformative power lies in the way it changes "economic trade-offs which influence, often without our awareness, the many small and large decisions we make that together determine who we are and what we do, decisions about education, housing, work, family, entertainment, and so on."[2]

> Technology shapes economics and economics shapes society
>
> **Nicolas Carr, 'The Big Switch' (2013)**

I shall give a simple example.[3] The invention of electricity transformed society because it extended man's physical power. Before electricity, the home was foremost a place to work, mainly done by women. The many common household chores were performed in uncomfortable conditions and demanded considerable strength and stamina. Even households with modest means would hire servants or day labourers to do the heavier jobs. When electricity became available inside homes, many believed that new appliances like vacuum cleaners and washing machines would transform houses into places of ease and that time would be freed up for women's personal development. The first widely purchased appliance was the electric iron which seemed fit to meet this expectation. Instead of heating a heavy wedge of cast iron over a hot stove, and stopping frequently to reheat this, a light weight device could be plugged into the wall. The actual impact was, however, that by making ironing easier, the new appliance ended up producing a change in social expectations about clothing, even children's clothing had to be ironed where before only men's shirts were. As the work became less heavy, many women further no longer felt justified in keeping servants. The end result was that electricity changed the nature of women's work, but not the quantity, and women found themselves more isolated at home.

---

1 This paragraph draws on the 2013 editions of Nicolas Carr, *The Big Switch, Rewiring the World From Edison to Google*, 2013; Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data, A Revolution That Will Transform How We Live, Work and Think,* John Murray publishers 2013; and Eric Schmidt and Jared Cohen, *The New Digital Age*, Alfred A. Knopf publishers 2013. Other sources report similar developments, but are already fully taken into account by these authors. See further also European Commission, *Towards Responsible Research and Innovation in the Information and Communication, Technologies and Security Technologies Fields*, 2011 to be found at http://ec.europa.eu/research/science-society/document_library/pdf_06/mep-rapport-2011_en.pdf (**EC Report on Responsible Research**). The quote of John M. Culkin, is from 'A Schoolman's Guide to Marshall Mc Luhan', *The Saturday Review*, March 18, 1967, at 70.

2 Carr, n 1, at 87. See further Mayer-Schönberger and Cukier, n 1, at 7.

3 This example draws on Carr, n 1, at 99 – 102.

Even with this fairly straightforward innovation of the electronic iron, the future impact could not be foretold. And once embedded in society, it was difficult, in fact impossible to undo. This is coined the Collingridge dilemma.[4]

> Regulators having to regulate emerging technologies face a double-bind problem: the effects of new technology cannot be easily predicted until the technology is extensively deployed. Yet once deployed they become entrenched and are then difficult to change.
>
> **David Collingridge, 'The Social Control of Technology' (1980)**

We are at the eve of a transformation of our society of a scope and impact similar to when electricity became a utility available to all. Where electricity extended man's physical power, information technology will extend man's thinking power.[5] The parallels are compelling. At the early stages of electricity, every factory had its own power generator which was the main business process to facilitate production. When it became possible to transport electricity over larger distances, factories in one area started sharing a joint power facility. When central generating stations started supplying to many buyers, it took a while before factories divested their own generators and accepted their dependence on a third-party supplier for a critical function. The economies of scale were, however, so imperative that no individual factory could match that. A competitive marketplace guarantees that more efficient modes of production and consumption will win out over less efficient ones. The grid always wins.[6] Those involved in IT will recognise this development. Like electricity, information technology over time became a critical business function for companies. In 1960, information technology constituted about 10% of a companies' cost, in 2000 it was 45%, every company owning its own servers, software and PCs.[7] Not surprisingly, we saw at that time (the emergence of) shared service centres where group companies shared IT resources to save costs and the rise in outsourcing transactions where companies outsourced their server management to third parties.[8] And now we see the early signs of information technology becoming a "utility". Suppliers offering "software as a service" (SaaS) based on cloud computing, where suppliers charge this service on a per unit basis (e.g., based on the amount of capacity used or number of transactions).[9] This saves companies the upfront investments in IT hardware and obtaining the required software licences, which make their IT costs predictable. In all likelihood, the coming 10 years will be a transition phase, during which time companies will divest their own IT "power plant" and hook up to the "grid" (i.e., the cloud).

---

4 See David Collingridge, The University of Aston, Technology Policy Unit, in his 1980 book *The Social Control of Technology*, St. Martin's Press; Frances Pinter 1980. The Collingridge dilemma is a basic point of reference in technology assessment debates.

5 Carr, n 1, at 23. Other authors also mark the digital age as being the cause of a major transformation of society. However, each of them gives another explanation for this or makes a different comparison as to earlier landmark technologies having had a similar impact on society. Mayer-Schönberger and Cukier, n 1, at p. 7 mark the possibilities of processing information (i.e. big data, see in detail below) as the beginning of a major transformation of society, but see the cause for this not so much in the "extension of 'man's thinking power', but in three shifts in mindset (i) the ability to analyse vast amounts of data; (ii) the ability to analyse raw data rather than more precise data; and (iii) a move away from the search for causality and accepting correlations (without knowing the cause thereof). The fact is, however, that finding these correlations is beyond man's thinking power and in that respect the authors are more aligned than it may seem at first glance. See also Mireille Hildebrandt, 'Slaves to Big Data. Or Are we?', October 2013, at 7, available at http://works.bepress.com/mireille_hildebrandt/52, at 2 – 3. Eric Siegel, *Predictive Analysis. The Power to Predict who will Click, Buy, Lie or Die*, John Wiley & Sons 2013, at 75, compares the current information revolution with the agricultural and industrial revolution. At 76, he further quotes Erik Brynjolfsson, professor of economics at Massachusetts Institute of Technology (MIT), who considers the new possibilities of data analytics to open up a new window on the world comparable to the revolution in measurement opened up by the invention of the microscope. Schmidt and Cohen, n 1, at 9 – 10 consider the digital age to constitute a paradigm shift comparable to the introduction of television.

6 Carr, n 1, at 16.

7 Carr, n 1, at 51.

8 L. Moerel, B. van Reeken et.al., *Outsourcing, een juridische gids voor de praktijk*, Kluwer 2009, at 1 – 6.

9 Cloud computing is defined by The National Institute of Standards and Technology (NIST) as:
"a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction", to be found at: http://en.wikipedia.org/wiki/Cloud_computing - cite_note-5#cite_note-5. The key characteristic of cloud computing is that the computing is 'in the cloud', i.e., the processing and the related data are not in a specified, known or static place. This is in contrast to a model in which the processing takes place on one or more specific servers that are known.

> Like a force of nature, the digital age cannot be denied or stopped.
>
> **Nicholas Negroponte, 'Being Digital' (1995)**

Information technology will become a general purpose utility.[10] And like electricity, the imperative is that the grid will win.[11] This is despite the fact that currently companies may still be hesitant to divest their proprietary IT assets and become dependent for this critical function on third-party IT suppliers.[12] This technology will further be beyond the control of regulators, in the sense that it cannot be stopped.[13] For instance in January 2011, the European Commission announced it would issue EU cloud regulations in order to ensure a European cloud service offering (rather than the current global cloud services provided by U.S. suppliers). But reality has already caught up with and surpassed such regulation.[14] At this time so many EU companies (including the first European banks)[15] are already using global cloud services offered by U.S. companies that the situation is by now impossible to undo.

> In a society governed by economic trade-offs, the technological imperative is precisely that: an imperative.
>
> **Nicolas Carr, 'The Big Switch' (2013)**

A consequence of information technology becoming a general purpose utility is that companies and individuals will no longer rely on data and software stored in their own computers which are then connected to the World Wide Web, but that everybody will tap into the World Wide **Computer**, with its cloud of data, software and hooked up sensors and devices.[16] Sensors will be present everywhere in the background, detecting motion, and being able to tell where I am at any time. My home will know when I am on the way, so the heating will be switched on and the food for the dog will be defrosted in time. The sensors will also be embedded in objects (the "internet of things") to trace how often they are used, e.g., a sensor on my toothbrush and dental floss, which will be able to monitor my dental care.[17] By means of these sensors there will be many new forms of how to measure and how to record what we measure, which is labelled "datafication".[18]

> Count what is countable, measure what is measurable, and what is not measurable, make measurable.
>
> **Galileo Galilei (1564 – 1642)**

One example is the insertion of a large number of sensors in the back of a car seat which measure pressure. The result is a digital code by which individuals can be identified (e.g., to

---

10 Carr, n 1, at 15.

11 Nicholas Negoponte, *Being Digital*, Alfred A Knopf 1995. 'Epilogue: An Age of optimism', to be found at: http://archives.obs-us.com/obs/english/books/nn/ch19epi.htm.

12 Carr, n 1, at 16.

13 Carr, n 1, at 22.

14 N. Kroes, 'Towards a European Cloud Computing Strategy', speech for World Economic Forum Davos, 27 January 2011, available at http://europa.eu. See further European Commission press release 15 October 2013 'What does the Commission mean by secure Cloud computing services in Europe?', http://europa.eu/rapid/press-release_MEMO-13-898_en.htm.

15 For example the Dutch Central Bank (DNB) approved the use of Amazon cloud services by financial institutions (provided certain conditions are met), see the news items on webwereld and computable, to be found at http://webwereld.nl/beveiliging/78684-dnb-keurt-amazon-cloud-goed-voor-nederlandse-banken and http://www.computable.nl/artikel/nieuws/outsourcing/4792558/1276946/dnb-banken-mogen-in-de-amazoncloud.html. DNB further agreed with Microsoft on the audit rights of DNB in case of the use of Microsoft Office 365 by an insurance company, paving the way for these cloud services for banks and insurance companies, see http://www.dnb.nl/publicatie/publicaties-dnb/nieuwsbrief-verzekeren/nieuwsbrief-verzekeren-januari-2013/dnb283669.jsp.

16 Carr, n 1, at 18. EC Report on Responsible Research, n 1, at 137.

17 See Mayer-Schönberger and Cukier, n 1, at 96.

18 Mayer-Schönberger and Cukier, n 1, at 77 – 78. See Siegel, n 5, at 75 for the quote of Galileo. This quote of Galileo is widely quoted and has many language versions, without anybody having ever found the original source.

prevent car theft) or which can identify dangerous situations (e.g., when the driver slumps from fatigue).[19] This is a major difference from the past where data were a by-product of a service (e.g., online purchase history of customers). With datafication it is the other way around: the data will be first collected, perhaps combined with data from other sources, and subsequently form the basis for the service itself.[20] Example is Google Street View, the extension of Google Maps and Google Earth, which provides for an online search service for views of streets (i.e. 360° panoramic photo views of streets, enabling the user to see every house in a street). The data are not collected in the provision of the service, it is the other way around. The data are collected first in order to deliver the service.

The result of these developments is that we will exist simultaneously in the real world and in a word generated by computers.[21] With the internet of things data will be omnipresent, which is coined by scientists and computer engineers as "big data")[22].....and more importantly we will want the various technologies collecting our data to share these in order to be able to benefit from new services.[23] We will want the sensors to be able to feed our location data into the intelligence of our houses in order to have the heating turned on in time.

Big data can be characterised by the variety of sources of data, the speed at which they are collected and stored, and their sheer volume.[24] But it is the new abilities to analyse these vast amounts of data that will make the real difference. While traditionally analytics has been used to find answers to predetermined questions (the search for the causes of certain behaviour, i.e., looking for the “why”), analytics of big data leads to the finding of connections and relationships between data that are unexpected and where previously unknown. It is looking for the "what", without knowing the “why”.[25] We will know that there is a correlation between a low credit rating and having more car accidents,[26] but will not know why this is the case. But companies and governments will act on these correlations. Based on these correlations predictions will be made. For example, the algorithms of the correlations found will predict the likelihood that one will have car accidents (and pay more for car insurance), default on a mortgage (and be denied a loan) or commit a crime (and receive psychological treatment in advance).[27] This may shift the interests of individuals in respect of processing of their data from data protection to protection against probability: being protected against the application of correlations without knowing the 'why' of this correlation, only that it exists.[28] Rather than deciding for yourself 'who am I' and 'what do I want' (the right to identity), big data creates the risk turning this into **being told** 'who you are' and 'what you want'. This will lead to renewed ethical consideration of the right to

---

19 Mayer-Schönberger and Cukier, n 1, at 77. Datafication is a different process than digitisation where analog information is converted into digital information (e.g. making a digital copy by scanning the original). Datafication of a book would make the text indexable and thus searchable. Datafication of books by Google now makes plagiarism in academic works much easier to discover, as some German politicians have experienced (see at 84).

20 Mayer-Schönberger and Cukier, n 1, at 94 – 97.

21 EC Report on Responsible Research, n 1.

22 See Mayer-Schönberger and Cukier, n 1, for a comprehensive description of what big data means. See for a popular description of the magnitude of the recent worldwide explosion of data collection and sharing, see The Economist 25 January 2010, 'A special report on managing information: Data, data everywhere. Information has gone from scarce to superabundant. That brings huge new benefits, but also big headaches', stating that “Wal-Mart, a retail giant, handles more than 1m customer transactions every hour, feeding databases estimated at more than 2.5 petabytes—the equivalent of 167 times the books in America’s Library of Congress (...). Facebook, a social-networking website, is home to 40 billion photos. And decoding the human genome involves analysing 3 billion base pairs—which took ten years the first time it was done, in 2003, but can now be achieved in one week. All these examples tell the same story: that the world contains an unimaginably vast amount of digital information which is getting ever vaster ever more rapidly. This makes it possible to do many things that previously could not be done: spot business trends, prevent diseases, combat crime and so on. Managed well, the data can be used to unlock new sources of economic value, provide fresh insights into science and hold governments to account. But they are also creating a host of new problems. Despite the abundance of tools to capture, process and share all this information—sensors, computers, mobile phones and the like—it already exceeds the available storage space (see chart 1). Moreover, ensuring data security and protecting privacy is becoming harder as the information multiplies and is shared ever more widely around the world.”

23 Mayer-Schönberger and Cukier, n 1, at 16. See also Evgeny Morozov, 'The Snowden saga heralds a radical shift in capitalism', Financial Times online, 26 December 2013, to be found athttp://www.ft.com/intl/cms/s/0/d2af6426-696d-11e3-aba3-00144feabdc0.html#axzz2pSUhfm5c.

24 Centre for Information Policy leadership, *Big Data and Analytics, Seeking Foundations for Effective privacy Guidance*, a discussion document February 2013, at 1, to be found at http://www.hunton.com/files/Uploads/Documents/News_files/Big_Data_and_Analytics_February_2013.pdf (**CIPL Discussion Document**).

25 CIPL Discussion Document, n 24, at 1. See Hildebrandt, n 5, at 6 – 7.

26 Siegel, n 5, at 83. See for a listing of 'Bizarre and Surprising Insights', at 81 – 88 and further the compendium in the centre of the book: '147 Examples of Predictive Analytics'.

27 Mayer-Schönberger and Cukier, n 1, at 17.

28 See Hildebrandt, n 5, at 6 on the shift from research based on causality to correlation. Evengy Morozov warns that big data analytics may lead to the search and finding of phantom correlations between inherently unrelated phenomena as it overgeneralises which leads to 'hyper inclusion'. See Evengy Morozov, 'Het Data Delirium', *NRC* 7 December 2013.

identity, i.e., should individuals be given a chance to trump the probabilities or should we all be ruled 'by data' (turning our society into a data dictatorship).[29] Currently, we have laws that ban discrimination based on ethnicity, gender, sexual orientation or belief system and which cannot be waived (an employee cannot waive the right to be free from discrimination based on belief system in return for higher wages).[30] Should these rights be extended to be also free from discrimination on other bases, such as genetics or lifestyle?[31] And if so, should this apply unconditionally or should exceptions apply?[32]

> Information technology has changes about everything in our lives [...] But while we have new ethical problems, we don't have new ethics.
>
> **Michael Lotti, 'Ethics and the Information Age' (2009)**

A life example which brings out the full-fledged ethical dilemmas is one discussed by Eric Siegel, in his instructive book on predictive analytics. Judges and parole boards as a matter of course make an assessment of the risk of recidivism when issuing their decisions. The State of Oregon launched a crime prediction tool to be consulted by judges and parole boards.[34] The model is based on processing the records of 55,000 Oregon offenders across five years of data. The model was then validated against 350,000 offender records across 30 years of history. There is no doubt that the predictive model works admirably and is much less arbitrary than the individuals making these decisions. Research shows that judicial decisions are greatly influenced by arbitrary extraneous factors. For instance, hungry judges rule more negatively. Judicial parole decisions immediately after a food break are about 65% per cent favourable, but drop gradually to almost zero per cent before the next break.[35] We have grown accustomed to humans making these judgement calls, however fallible. The predictive model will make wrong decisions, but often proves less wrong than people. But who will be accountable for the wrong decisions and how will it feel for the criminal who is scored as a high-risk recidivist? He will never be able to prove that he would not commit a crime again if he had been released from prison. Are we still evaluating this person as an individual when he is judged based on what other people who share

---

29 Mayer-Schönberger and Cukier, n 1, at 17. Neil M. Richards and Jonathan H. King, 'Three Paradoxes of Big Data', *Stanford Law Review*, 3 September 2013, 66 Stanford Law Review Online, at 41, to be found at: http://www.stanfordlawreview.org/online/privacy-and-big-data/three-paradoxes-big-data, consider this the "identity paradox" as big data seeks to *identify* but also threatens *identity*. The right to identity originates from the right to free choice about who we are. With big data this right will risk turning into being told "what you are" and "what you will like". See further Hildebrandt, n 5, at 7, and Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics', 11 *Northwestern Journal of Technology and Intellectual Property* 239 (2013), at 252, to be found at SSRN: http://ssrn.com/abstract=2149364.

30 Richard H. Thaler and Cass R. Sunstein, *Nudge, Improving Decisions About Health, Wealth, and happiness*, Yale University Press 2008, at 251.

31 Which could include hundreds of variables, such as hobbies, what you eat, the websites you visit, the amount of television you watch, and estimates of income. Mayer-Schönberger and Cukier, n 1, at 57, report that Aviva, a large insurance firm, uses a predictive model based on such lifestyle factors to identifying health risks. See also Hildebrandt, n 5, at 8.

32 The quote from Michael Lotti is from: 'Ethics and the information Age', *Effect Magazine Online*, Winter 2009/2010, to be found at www.larsonallen.com/EFFECT/Ethics_and_the_Information_Age.aspx. See further Jules Polonetsky and Omer Tene, 'Privacy and Big Data: Making Ends Meet', September 3, 2013, 66 *Stanford Law Review* Online 25, to be found at http://www.stanfordlawreview.org/online/privacy-and-big-data/privacy-and-big-data. Polonetsky and Tene indicate that "finding the right balance between privacy risks and big data rewards may very well be the biggest public policy challenge of our time", as it calls for momentous choices to be made between weighty policy concerns on the one hand and individual's rights to privacy, fairness, equality and freedom of speech, on the other hand, and further requires "deciding whether efforts to cure fatal diseases or eviscerate terrorism are worth subjecting human individuality to omniscient surveillance and algorithmic decision making". See further Tene and Polonetsky, n 29, at 251– 256 (see at 265: "where should the red line be drawn when it comes to big data analytics"); and Ira Rubinstein, 'Big Data: The End of Privacy or a New Beginning?', 3 International Data Privacy Law (2013), at 77 – 78. Rubinstein indicates that data mining has been associated with three forms of discrimination: price discrimination, manipulation of threats to autonomy and covert discrimination. See for further literature Rubinstein, at 77, footnote 29.

33 See n 5. See at 11 for a definition of predictive analytics: "Technology that learns from experience (data) to predict the future behaviour of individuals in order to drive better decisions".

34 This tool is on display for anyone to try out, see *The Public Safety Checklist for Oregon*, Criminal Justice Commission, last updated 11 August 2012.

35 Siegel, n 5, at 60, under reference to a joint study by Colombia University and Ben Gurion University (Israel), Shai Danziger, Jonathan Levav, and Liora Avnaim-Pesso, *Extraneous Factors in Judicial Decisions*, edited by Daniel Kahneman, Princeton University, Princeton, NJ, February 25, 2011, to be found at http://lsolum.typepad.com/files/danziger-levav-avnaim-pnas-2011.pdf.

certain characteristics have done?[36] Another flaw detected in the predictive models is that they instil existing prejudices against minorities. The factors taken into account by the predictive model are for instance, age, gender, zip code, prior crimes, arrests and incarcerations. These government models do not incorporate ethnic class and minority status. These, however, do creep into the predictive models indirectly, by e.g., zip code which is both correlated with ethnic class and minority status. But also prior arrests may be indicative of ethnicity, as these are often influenced by ethnic background. By including these factors, racial discrimination at the level of the police forces is inscribed into the future. It is clear that the last word has not been said about these predictive models.[37]

But the biggest shift will be that the World Wide Computer will become a sensing, cognitive device with independent thinking powers which will interact directly with our brains.[38] These "neural interfaces" promise to be a blessing to people afflicted with severe disabilities, but also offer the potential for outside control of human behaviour.[39] Information technology will become more autonomous (ICT-enabled devices making autonomous decisions) and further less visible in its interaction with humans. Interaction will no longer take place via technical devices such as mice, keyboards, screens, but via technical artifacts in the background (miniscule sensors), making it easy to forget their presence and interaction.[40] The ICT-enabled decisions will often have moral qualities (e.g., in healthcare, who gets the transplant organ and who gets priority in rescue situations?) and further raise questions of autonomy of individuals. Implantable devices that communicate with external networks (like the pacemaker today) will in the future use human skin for transmission and will not only be used to address disabilities, but also for enhancement of abilities of healthy individuals (e.g., infrared visibility), which in all likelihood will raise significant resistance due to social, moral, ethical, and religious objections.[41]

> A method and apparatus for transmitting power and data using the human body
>
> **Microsoft US Patent 6, 754,472 June 2004**

It is clear that the new information technologies will bring many benefits.[42] It, however, stands to reason that these new technologies will also create new risks, liabilities and responsibilities, and even will change the very fabric of society. Changes in the way we work, engage in political

---

36 Ian Kerr and Jessica Earle, 'Prediction, Preemption, Presumption: How Big Data Threatens Big Picture', 66 *Stanford Law Review Online*, 3 September 2013, at 67, label this form of prediction 'preemptive predictions' and define these as predictions that are intentionally used to diminish a person's range of future options. Another example of a preemptive prediction is the no-fly list used by the US government to preclude possible terrorist activity on planes. This type of prediction is more invasive than the other two forms Kerr and Earle identify (see at 67): preferential predictions (e.g. predictions by the Google search engine) and consequential predictions (i.e. predictions of the likely consequences of an individual's actions, e.g. by a doctor). These two other forms take the perspective of the individual. The first, however, takes the perspective of someone who wants to preclude certain behaviour of individuals. This form of prediction can result in a violation of the presumption of innocence and associated privacy and due process values (such as the right to a fair and impartial hearing, an ability to question those seeking to make a case against you, access to legal counsel, a public record of the proceedings, published reasons for the decision, and an ability to appeal the decision or seek judicial review (see at 66).

37 Tene and Polonetsky, n 29, at 243 provide as a solution that organisations should disclose the logic underlying their decisionmaking processes and further (see at 264) query "where the red line should be drawn with big data analytics".

38 Ray Kurzweil, Director of Engineering of Google announced in an interview by Keith Kleiner, available at http://www.youtube.co/watch?v=YABUffpQY9w, that his team is trying to create an artificial intellect capable of predicting on a 'semantically deep level what you are interested in'. Kerr and Earle, n 36, at 66, comment that this will "turn the meaning of search on its head: instead of people using search engines to better understand information, search engines will use big data to better understand people".

39 Carr, n 1, at 217, under reference to the *British Government Innovation Survey: Institute for the Future, Delta Scan: The Future of Science and Technology, 2005-2055: Computing on the Human Platform*, to be found at 1 http://humanitieslab.stanford.edu/2/296.

40 EC Report on Responsible Research, n 1, at 27.

41 See the British Government Innovation Survey, n 39, at the Summary Analysis. See Schmidt and Cohen, n 1, at 25 – 26 for a number of examples of implantable devices and electronic pills.

42 See for a host of examples: Schönberger and Cukier, n 1; Tene and Polonetsky, n 29, at 243 – 250, give examples per sector: Healthcare, Mobile, Smart Grid, Traffic Management, Retail, Payments and Online, to be found at http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1; Rubinstein, n 32, at 76; CIPL Discussion Document, n 24, at 3 – 8; and the 2013 World Economic Forum Report *Unlocking the Value of personal data: From Collection to Usage*, to be found at http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf WEF Report (2013) (**World Economic Forum Report 2013**).

activities, and leisure will raise questions about appropriateness of rules and regulations. They may create winners and losers and therefore lead to conflicts that need to be addressed.[43]

This is a glimpse of the possible future. What I am going to discuss today is:

- What will the likely impact of these technologies be on society (what are the downsides, the risks)?
- What will the role of data protection be in all this (if any is left)?
- If a role is left for data protection, do people still care about data protection?
- If people still care, how should data protection best be regulated?
- In this context I will discuss four paradoxes that make regulating data protection a challenge;

I will then tie everything together and make proposals for improvement, which (spoiler alert) will not resemble the proposals as now embodied in the draft EU regulation on data protection[44] which was communicated by the European Commission on 25 January 2012[45] ("**Proposed Regulation**").

1. What is the likely impact of big data on individuals and society?

The age of big data and the internet of things are just emerging and already it is clear that the first predictions what these technologies would bring are proven wrong. At first many thought that the digital age would make society more democratic, information would be accessible to all, providing an egalitarian forum in which all views could get an airing and this to the benefit (also the economic benefit) of all.[46]

> By changing the way we create and exchange information, knowledge and culture, we can make the twenty-first century one that offers individuals greater autonomy, political communities greater democracy, and societies greater opportunities for cultural self-reflection and human connection.
>
> **Yochai Benkler, 'The Wealth of Networks' (2006)**

The first signs, however, already tell a different story, belying that the benefits of the digital age would be for all. To the contrary, the first signs are that the age of big data will bring a larger divide between the have's and the have-not's. I will highlight four observations.

(i) Social production

Rather than the traditional sale of information products, such as movies, news, encyclopaedia (by companies controlling the copyrights), we see in the online environment a gift economy emerging, which results in collaborative free products of individuals.[47] We

---

43 EC Report on Responsible Research, n 1, at 27.

44 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation), COM(2012) 11 final, to be found at http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

45 European Commission, *Communication of the Commission to the European Council, the European Economic and Social Committee of the Regions, Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century*, COM(2012) 9 final (25 January 2012).

46 Carr, n 1, at 159, under reference to Nicholas Negroponte, *Being Digital* 1995, n 11, at 230. See further Yochai Benkler, *The Wealth of Networks – How Social Production Transforms Markets and Freedom*, Yale University Press 2007, at 626, to be found at http://www.sisudoc.org/sisu/en/pdf/the_wealth_of_networks.yochai_benkler.portrait.a5.pdf.

47 Richard Barbrook, 'The Hi-Tech Gift Economy', 2007, at 2: "Despite originally being invented for the U. S. military, the Net was constructed around the gift economy. The Pentagon initially did try to restrict the unofficial uses of its computer network. However, it soon became obvious that the Net could only be successfully developed by letting its users build the system for themselves. Within the scientific community, the gift economy has long been the primary method of socialising labour. Funded by the state or by donations, scientists don't have to turn their intellectual work directly into marketable commodities. Instead, research results are publicised by 'giving a paper' at specialist conferences and by 'contributing an article' to professional journals. The collaboration of many different academics is made possible through the free distribution of information (...)", to be found at: http://www.imaginaryfutures.net/2007/04/19/the-hi-tech-gift-economy-by-richard-barbrook/. See further Don Peppers and Martha Rogers, *Extreme Trust. Honesty as a Competitive Advantage*, Penguin Group 2012, at Chapter 4

see this new model embodied in Wikipedia (where individuals free of charge take responsibility for contributing and monitoring content), in YouTube (where individuals upload video clips) and Flicqr (where individuals upload photo's for everybody to use as they see fit).

> People volunteer, they collaborate, and they share their own time and energy with others, not in return for some market payment, but for the personal satisfaction of creating and sharing, or enjoying the goodwill of others, or simply feeling more connected.
>
> **Don Peppers and Martha Rogers, 'Extreme Trust. Honesty as a Competitive Advantage' (2012)**

You would expect these new services to pose a threat to the corporations who initially controlled the copyrights in these products such as the producers of newspapers and encyclopaedia.[48] The threat by "social production" appears, however, not to be to the big corporations. It is in fact Google that profits off the efforts of amateurs posting video clips on YouTube and it is Yahoo that profits off the millions of users generating content for Flickr.[49] This free content attracts many visitors, which enables these companies to generate advertising income. The data collected from visitors to these websites is valuable as it enables advertisers to target their communications to the preferences and profiles of these visitors, which is obviously more effective than general advertising, and which pays for hosting the content and added services.[50]

> The internet of free platforms, free services, and free content is wholly subsidized by targeted advertising, the efficacy (and thus profitability) of which relies on collecting and mining user data.
>
> **Alexander Furnas, 'It's Not All About You: What Privacy Advocates Don't Get about Data Tracking on the Web' (2012)**

The category that loses out in this "social production" model is the individual professionals, journalists, photographers, moviemakers, and editors whose work product is replaced by the free products supplied by the masses. This erodes the middle-class and widens the divide between the haves and the have nots.[51] This effect is increased by the offshoring of

---

'Sharing: not just for Sunday school'. See at 18 for why people contribute to the gift economy. See further Carr, n 1, at 141 and Noreena Hertz, *Eyes Wide Open, How to Make Smart Decisions in a Confusing World*, William Collins Publishers 2013, at 133.

48 Copyright and other intellectual property rights do not sit well with the internet and the gift economy. See Barbrook, n 47, at 3: "As Tim Berners-Lee - the inventor of the Web - points out: “Concepts of intellectual property, central to our culture, are not expressed in a way which maps onto the abstract information space. In an information space, we can consider the authorship of materials, and their perception; but ... there is a need for the underlying infrastructure to be able to make copies simply for reasons of [technical] efficiency and reliability. The concept of ‘copyright’ as expressed in terms of copies made makes little sense. Within the commercial creative industries, advances in digital reproduction are feared for making the ‘piracy’ of copyright material ever easier. For the owners of intellectual property, the net can only make the situation worse. In contrast, the academic gift economy welcomes technologies which improve the availability of data. Users should always be able to obtain and manipulate information with the minimum of impediments. The design of the Net therefore assumes that intellectual property is technically and socially obsolete." Schmidt and Cohen, n 1, at 99 – 100, are less pessimistic, but admit that a lot has to happen and that in particular China should be forced to enforce their intellectual property laws.

49 When Yahoo in 2005 acquired the photo-sharing site Flickr for an estimated EUR 35 million (with fewer than 10 people on the payroll), Yahoo executive Bradley Horowitz indicated that Yahoo was motivated by harvesting all the free labour supplied by Flickr's users and that if they could repeat that trick with the Yahoo user base and achieve the same kind of effect, that they were on to something. See Steven Levy and Brad Stone, 'The New Wisdom of the Web', *Newsweek* April 3 2006, to be found at http://karbowski.us/Handouts/Week13/TheNewWisdomoftheWeb.pdf.

50 As quoted by Siegel, n 5, at 43, under reference to Alexander Furnas, 'It's Not All About You: What Privacy Advocates Don't Get about Data Tracking on the Web', *The Atlantic*, March 15, 2012, to be found at www.theatlantic.com/technology/archive/2012/03/its-not-all-about-you-what-privacy-advocates-dont-get-about-data-tracking-on-the-web/254533/.

51 Carr, n 1, at 142 – 143. Tene and Polonetsky, n 29, at 254 – 255, indicate that also the benefits of analytics of the personal data accumulated by companies "accrue to (...) big business, not to the individual – and they often come at the

labour to low income countries and the lack of 'digital resilience' of the workforce whose jobs are relocated.[52] According to economists, this trend is permanent and irreversible, resulting in a widening divide between a relatively small group of extraordinarily wealthy individuals and a very large group with eroding earning capacities.[53]

> In the YouTube economy, everyone is free to play, but only a few reap the rewards
>
> **Nicolas Carr, The Big Switch (2013)**

(ii) Cultural impoverishment

Another unforeseen consequence is what is called the "unbundling" of content. Many services on the internet are free (think of Google, Facebook, YouTube, free news sites) and the companies providing these services are paid out of advertising income. As advertisers want to pay by the click, what is published will be determined by what raises advertising income. That is often not the high-quality content, but the flimsier popular fare, while the hard journalism tends to be the more expensive to produce.[54] This has made transparent that e.g., newspapers functioned on an invisible system of cross-subsidisation between certain parts of the newspapers.[55] Similar effects are to be seen in TV programming, where there is also a cross-subsidisation between popular movies and documentaries. Now that programs are becoming available on a pay-per-view basis, it is becoming uneconomical to produce e.g., expensive documentaries, which leads to cultural impoverishment.[56]

> How do we create high-quality content in a world where advertisers want to pay by the click, and consumers don't want to pay at all?
>
> **Martin Nisenholtz (2006)**

(iii) Social fragmentation

The sensitive search technology on the internet feeds our existing preferences back to us. As it further has become easier to find like-minded people, people are supported in their existing views, and become convinced that these are right.[57] This leads over time to a

---

individual's expense (...) In the words of the adage, if you're not paying for it, you are not the customer, you're the product".

52 Negroponte, n 11, at 1: "As we move forward towards such a digital world, an entire sector of the population will be or feel disenfranchised. When a fifty-year-old steelworker loses his job, unlike his twenty-five-year-old son, he may have no digital resilience at all. When a modern-day secretary loses his job, at least he may be conversant with the digital world and have transferrable skills."

53 Carr, n 1, at 147, under reference to Chris Anderson, *The Long Tail. Why The Future of Business is Selling Less of More*, Hyperion Books 2006.

54 Schmidt and Cohen, n 1, at 24, indicate that it will become more difficult to make content of high quality, but easier to compose teams with the required expertise as experts can be involved from all over the world.

55 Carr, n 1, at 155.

56 Carr, n 1, at 156. The quote from Martin Nisenholtz is from his opening speech at the 'Online Publishers Associaton (OPA) '06: Forum for the Future', 1- 3 March 2006, as reported in a blog of the Guardian, to be found at http://www.theguardian.com/media/organgrinder/2006/mar/02/opaconferenceisdigitalthe.

57 Carr, n 1, at p. 165 – 167; Cass Sunstein, *Republic.com*, Princeton University Press 2001, at 192; Hertz, n 47, at 267 – 269 ('the dangers of narrowcasting'); and Schmidt and Cohen, n 1, at 35. This issue should not be underestimated. Sunstein at 191 cites John Stuart Mill, one of the great theorists of freedom and democracy. The quote is a bit out of context as it relates to the importance of contact with other state nations, but seems to equally apply in a national context: "It is hardly possible to overrate the value, in the present low state of human improvement, of placing human beings in contact with persons dissimilar to themselves, and with modes of thought and action unlike those with which they are familiar. Commerce is now what war once was, the principle source of this contact. (...) And commerce is the purpose of the far greater part of the communication which takes place between civilized nations. Such communication has always been, and is peculiarly in the present age, one of the primary sources of progress", see *The Principles of Political Economy* (1848), Chapter 17 'Of International Trade', to be found at http://ebooks.adelaide.edu.au/m/mill/john_stuart/m645p/complete.html.

reinforcement and even magnification of our existing bias,[58] insulating people from opposing points of view. This results in a loss of shared experiences by all (who still watches TV with his/her children?) which poses a threat to the structure of democratic societies.[59]

> A market dominated by countless versions of the "Daily Me" (...) would reduce, not increase freedom for the individuals involved [and] create a high degree of social fragmentation.
>
> **Cass Sunstein, 'Republican.com' (2001)**

(iv) The ultimate control apparatus.

The internet started out as a free haven where you could remain anonymous and beyond territorial jurisdiction. In 1996 internet evangelist John Perry Barlow published the "Declaration of the Independence of Cyberspace", declaring the internet to be a "new home of [the] Mind" in which governments would have no jurisdiction.[60]/[61]

"On the internet, nobody knows you're a dog."

But governments and companies quickly caught up with the "techies",[62] transforming the internet into the ultimate apparatus for political and social control by monitoring speech, identifying dissidents and disseminating propaganda.[63] And not just by countries like China and India[64] as we now know.[65] As one author remarks "in the past you had to get a

---

58 Schmidt and Cohen, n 1, at 35 call this the 'confirmation bias'.

59 Carr, n 1, at p. 166.

60 John Perry Barlow, 'A Declaration of the Independence of Cyberspace. Elec. Frontier Found', 8 February 1996, to be found at https://projects.eff.org/~barlow/Declaration-Final.html.

61 The cartoon is allegedly the first cartoon about the internet and is from Peter Steiner, *The New Yorker*, 69(20), at 61, 5 July 1993.

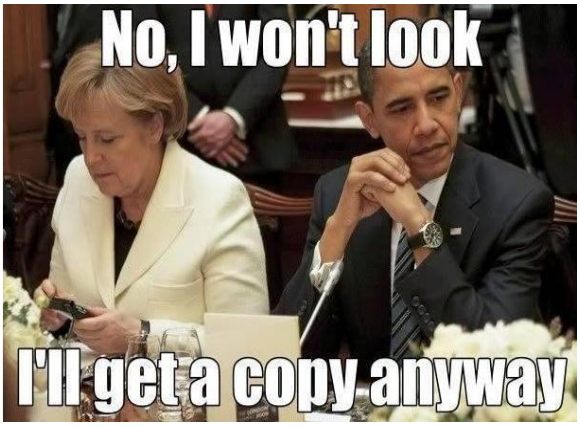
62 Carr, n 1, at 242.

63 Richards and King, n 18, call this the 'power paradox' and give the following example: "Many Arab Spring protesters and commentators credited social media for helping protesters to organize. But big data sensors and big data pools are predominantly in the hands of powerful intermediary institutions, not ordinary people. Seeming to learn from Arab Spring organizers, the Syrian regime feigned the removal of restrictions on its citizens' Facebook, Twitter, and YouTube usage only to secretly profile, track, and round up dissidents". See further Schmidt and Cohen, n 1, at 83 – 96 ('the police state 2.0') who discuss how repressive regimes try to localise the internet for their respective regions, labelled 'balkanisation' (see at 85) and further abuse hand held devices to spy on their citizens (at 60). See further at 89 – 97 'the police state 2.0'.

64 China, for example, requires service providers doing business in China to reveal data to Chinese law enforcement authorities. E.g., in January 2010 Google threatened to withdraw from China referring to China-based cyberattacks on its databases and the e-mail accounts of some users, and China's attempts to 'limit free speech on the Web,' as the reasons for its decision. See The New York Times Google Inc. profile at <http://topics.nytimes.com/top/news/business/companies/google_inc/index.html?scp=2&sq=china%20google%20yahoo&st=cse>. An example for India is the refusal of India to allow Blackberry handheld devices because the data are encrypted, demanding that entities offering communication services in India should also maintain communications equipment there, facilitating real-time access to corporate messages. See Daniel Emery, 'India threatens to suspend Blackberry by 31 August,' *BBC News Online*, 13 August 2010, available online at <http://www.bbc.co.uk/news/technology-10951607>. See for further examples Schmidt and Cohen, n 1, at 72 – 74.

65 The increase in surveillance is not limited to the US. This is also an issue within the EU. For an overview of the EU security data exchange policies and the data protection implications, see *Tenth Annual Report of the Article 29 Working Party on Data Protection*, at 7 – 8 (to be found at

warrant to monitor a person or a group of people. Today, it is increasingly easy to monitor ideas. And then track them back to people." The result is a reversal of the burden of proof, which undermines the fundamental democratic principle of the presumption of innocence.[66]



2. What is the role of data protection in all this?

Data have become the currency of the internet. As indicated, many services on the internet are free and the companies providing these services are paid out of advertising income.

> *Personal data is the new oil of the Internet and the new currency of the digital world.*
>
> **Meglena Kuneva, European Consumer Commissioner (2009)**

But this does not only apply to online free services. Also for companies selling products and services, such as Amazon.com, the value is in the analysing of their customers purchase histories. Amazon makes 35% of its revenues from suggestions made to customers based on analytics of purchase preferences of other buyers.[67] According to Eric Siegel,[68] the current value of the personal data of one individual for companies represents $ 1,200. European Commissioner Viviane Reding reported that in 2011 the net worth of the data of all Europeans amounted to € 315 billion.[69] The prediction is that companies like Google and Yahoo will likely be eager to supply us with all-purpose utility services, possibly including a thin-client device to hook on to the cloud for free in return for the privilege of showing us advertising.[70]

<http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm>). See also Carr, n 1, at 198 – 200.

66 Carr, n 11, at 188, citing Tom Owad, 'Data Mining 101: Finding Subversives with Amazon Wishlists', January 4, 2006, to be found at: http://www.applefritter.com/bannedbooks. Schmidt and Cohen, n 1, at 62, even indicate that users of the internet domiciled in repressive regimes can even be 'guilty by association', e.g., by being depicted on a photo with a dissenter. See also n 36.

67 See blog dated 8 August 2013, at flow20, 'What Most Retailers Can Learn From Amazon.co.uk', to be found at: http://www.flow20.com/what-most-online-retailers-can-learn-from-amazon-co-uk/, under reference to a survey of Internet Retailer which is no longer available on the net. See also Mayer-Schönberger and Cukier, n 1, at 52, who report that for Netflix, an online film rental company, three-fourths of new orders come from recommendations.

68 Siegel, n 5, at 42, under reference to Alexis Madrigal, 'How Much Is Your Data Worth? Mmm, Somewhere Between Half a Cent and $ 1.200', *The Atlantic*, 19 March 2012, to be found at www.theatlantic.com/technology/archive/2012/03/how-much-is-your-data-worth-mmm-omewhere-between-half-a-cent-and-1-200/254730/.

69 Viviane Reding, 'Data protection reform: restoring trust and building the digital single market', 4th Annual European Data Protection Conference/Brussels, 17 September 2013, to be found at: http://europa.eu/rapid/press-release_SPEECH-13-720_en.htm. See at 2: "Data is the new currency: the value of EU citizens' data was €315 billion in 2011. It has the potential to grow to nearly €1 trillion annually in 2020. But trust in the data-driven economy, already in need of a boost, has been damaged. 92% of Europeans are concerned about mobile apps collecting their data without their consent. 89% of people say they want to know when the data on their smartphone is being shared with a third party". Reding refers for the estimates to a report of the Boston Consulting Group, which is not available on the internet.

70 Carr, n 1, at 81.

The question is whether data protection has here a role to play? Why would it, the data are mostly freely given, or at least with clicking blindly "ok" for accepting terms and conditions and privacy statements.

The reason why data protection has a function is because there are no rules regulating ownership of data. There is no property right in data, as you can only have property rights in a tangible good. Data are also not protected by intellectual property rights, like books, movies and software are protected by copyright against copying. You can only have factual possession of data, and the one having factual possession has the power to keep the data for him or herself or to give a copy to someone else.[71] Therefore the only law that regulates the use of personal data is data protection. Data protection rules determine whether data can be used for certain purposes and whether data can be transferred to another party. Data protection thus by default have become the organising principle of the economics of the internet.[72] As such data protection rules has an impact on the value of the personal data that a company has in its possession. This is the reason why although Facebook's total profit in 2011 was only $ 1 billion, the company was valued at $ 104 billion at its IPO in 2012. The difference was attributable to its 901 million member database and the information pertaining to these members.[73]

This is why personal data are often described as “the lifeblood or basic currency of the information economy, being arguably a key asset, a central organising principle and a critical enabler for business competitiveness in today’s world.”[74] The World Economic Forum (**WEF**) even considers data as a new production factor on par with labour and capital.[75]

> Beyond it sheer volume, data is becoming a new type of raw material that's on par with capital and labour.
>
> **World Economic Forum 'Personal Data: The Emergence of a New Asset Class' (2011)**

And this is also why the new EU Regulation on Data Protection is so heavily lobbied (3999 amendments were proposed),[76] there are strong economic interests at stake. Given the potential downsides I discussed of the new economy for individuals and society at large, it is also understandable why the European Parliament and the governments of the individual Member States take such an extreme interest in the new Regulation.[77]

Should data protection be replaced by property rights in data?
Given the role of data as a currency, it may not be surprising that the WEF suggested replacing data protection by an "end user centric system", which seems to amount to the recognition of a

---

71 EC Report on Responsible Research, n 1, at 105: "On the other hand, the generation of data gives the owner of data power – or in other words control over people and time as Giddens (1992) describes it in his theory of structuration."

72 Rand Europe, *Review of the European Data Protection Directive, Technical Report* dated May 2009 ("**Rand Report**"), at 12.

73 See article on Forbes website of Tomio Geron, 'Facebook Prices Third-Largest IPO Ever, Valued at $104 Billion', to be found at http://www.forbes.com/sites/tomiogeron/2012/05/17/facebook-prices-ipo-at-38-per-share/.

74 Rand Report, n 72, at 12. See in similar terms Mayer-Schönberger and Cukier, n 1, at 16.

75 See World Economic Forum Report 2011 *Personal Data: The Emergence of a New Asset Class*, at 7 (under reference to the article in the Economist: 'Data, Data Everywhere', n 22), to be found at: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf. See also Mayer-Schönberger and Cukier, n 1, at 101.

76 European Commission, Press release, 'LIBE Committee vote backs new EU data protection rules', 22 October 2013, MEMO/13/1923, to be found at http://europa.eu/rapid/press-release_MEMO-13-923_en.htm.

77 Latest status is that the EU Council has announced that it may postpone its vote to 2015, which would entail that the vote would take place after a new EU Parliament is elected (European Commission, Press release, 'Conclusions 24/25 October 2013, to be found at http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf). However, the LIBE Committee has made substantive progress by adopting its compromise text, which grants a mandate to their Rapporteurs to negotiate with the EU Council (reference 72). Despite the reluctance within the EU Council, EU officials believe timely adoption – before the EU Parliament's elections in May 2014 – is still possible, see Jeremy Fleming, 'EU to push ahead on data protection despite UK opposition', 28 October 2013, to be found at http://www.euractiv.com/specialreport-digital-single-mar/commission-push-ahead-data-prote-news-531357). See for the unofficial consolidated version of the compromise text adopted by LIBE, http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf) (**LIBE compromise text**).

property right in personal data, which individuals can subsequently commercialise. [78] I agree that to the extent asking consent from individuals for the use of their data for commercial purposes is concerned, the system of a property right where an individual can 'sell or license his data' is more intuitive for most people than the rules on data protection. People consider data about them as their property. [79] The idea is persuasive if only for that reason.[80] However, the underlying rationale for data protection is to protect individuals against all types of direct and indirect harm (such as identity theft, information inequality and abuse, see further below), for which a property right is not intuitive and less suitable.[81] Exploitation of property rights further requires what Thaler and Sunstein label the *homo economicus (econs)*, people who oversee their choices and act predictably in their own interest. Most of us are, however, regular *homo sapiens* and unlike econs, humans predictably err and often act against our self-interests.[82] Social science research shows "that in many cases humans make pretty bad decisions, decisions they would not have made if they had paid full attention and possessed complete information, unlimited cognitive abilities and complete self-control".[83] (see further below). As to data protection there is a growing concern that individuals may not understand what they are consenting to,[84] that when consent is asked, there are often no meaningful default options available, so consent is not really "freely given",[85] and finally that the granting of consent becomes a mechanical matter of "ticking the box", i.e., becomes subject to 'routinisation' and therefore meaningless.[86] This means that also if property rights are granted, extensive rules will

---

78 World Economic Forum Report 2011, n 75, at 10, 15, 16, 17 and 19. Similar suggestions are made by Tene and Polonetsky, n 42, at 263 – 264, who propose a 'sharing the wealth' strategy where data controllers provide individuals with access to their data in a 'usable' format and allow them 'to take advantage of applications to analyze their own data and draw useful conclusions' from it (e.g., consume less protein). They argue that the creation of value to individuals is likely to re-engage consumers who until now have 'remained largely oblivious to their rights'. "This 'featurization' or 'appification' of data (see also at 268) will unleash innovation by allowing software developers to create a single version of their product that will work for all utility customers across the country." If individuals can reap benefits of some of the gains of big data, they would be incentivized to actively participate in the data economy (see at 245). Rubinstein, n 32, at 81, takes the 'sharing the wealth' model of Tene and Polonetsky one step further and proposes a fundamental shift in the management of personal data "from a world where organizations gather, collect and use information about their customers for their own purposes, to one where individuals manage their own information for their own purposes—and share some of this information with providers for joint benefits". This presupposes 'Personal Data Services' or PDSes (see at 82 for the eight elements of PDSes: individuals as the center of control of their data, selective disclosure, signaling (a means for individuals to express demands for services), identity management, security, data-portability, accountability and enforcement). At 83, Rubinstein signals there are a host of obstacles for PDSes: 'ranging from the technical (adequate security, establishing a new permission model based on meta-tagging, preventing re-identification); to the legal (establishing a legal framework supporting propertised personal information, developing a co-regulatory approach that incentivizes, rather than penalizes, new business models, harmonizing international legal rules); to a variety of business and social tasks implicit in creating a new ecosystem.' See for an earlier publication on propertisation of personal data Paul M Schwartz, 'Property, Privacy, and Personal Data', (2004) 117 *Harvard Law Review*, nr 7, at 2055 – 2128. See for a sampling of earlier publications of those opposed to propertisation, Schwartz at 2057, footnote 4, and for a sampling of views of those advocating propertisation, at 2057, footnote 5.

79 World Economic Forum Report 2011, n 75, at 16. See Christopher Rees, 'Tomorrow's privacy, personal information as property', *International Data Privacy Law* vol. 3 number 4, November 2013, at 220 – 221: "In any case the underlying rationale [of personal information as property] is one that complies with most people's conception of the arrangement they are making with search engines and social media sites when they are using them: people talk of 'my' data. It is never the search engine's".

80 Nadezhda Purtova, *Property Rights in Personal Data: a European Perspective*, diss. TILT, Boxpress 2011 , at 265 – 266, concludes that the idea of property rights in personal data in Europe is not only formally possible, but offers some advantages in dealing with the personal data problem as it introduces ultimate clarity as to the allocation of the data protection obligations. Property rights are *erga omnes* (against an indefinite number of people), which will mean that an individual will not have to search for a controller to enforce his rights. The resulting system will resemble consumer protection: if one bought a product that does not work, one can address the shop where the product was bought or the manufacturer.

81 Schwartz, n 78, at 2076 – 2090, identifies three main concerns with a property based system: (i) propertisation will exacerbate privacy market failures: 'because the gatherers have greater power to set the terms of the bargain and to shape the playing field that guides individual decisions, at the end of the day negotiations in the privacy market may fall short' (see at 2081 – 2082); (ii) propertisation will neglect important social values that information privacy should advance (see at 2084); and (iii) propertisation invites free alienability of personal data; once information is propertised, it will be difficult to limit an individual's right to sign a way his interest (see at 2090), which is problematic for reasons of secondary use of personal data (see at 2090) and the difficulty of estimating the appropriate price for such secondary use (see at 2091). See for an overview of pro's and cons of property rights in personal data: Corien Prins, 'When personal data, behaviour and virtual identity become a commodity: Would a property right approach matter?', (3) *SCRIPT-ed* 2006-4, at 270 – 303.

82 Thaler and Sunstein, n 30, at 6 – 7.

83 Thaler and Sunstein, n 30, at 5.

84 Lokke Moerel, *Binding Corporate Rules, Corporate Self-Regulation of Global Data Transfers*, Oxford University Press 2012, at 44 – 45, under reference to Roger Brownsword, 'Consent in Data protection Law', in Serge Gutwirth et. al. (eds.), *Reinventing Data Protection?*, Springer 2009, Chapter 2, at 90, who rightfully notes that "until background rights, including the background informational rights have been established, consent has no reference point."

85 Moerel, n 84, at 45 referring for the risks of routinisation of consent, to Roger Brownsword, n 84, Chapter 2, at 90.

86 This is well illustrated by the model for propertisation proposed by Schwartz, n 78, see introduction at 2055 and in depth at 2094 – 2115. After having discussed the main concerns with a property-based theory (see for these concerns n

have to be developed in which cases these property rights will be inalienable, what the extent is of any licence given, limitations on secondary use, etc).[87] We therefore will end up with similar protection rules we now have under data protection law, but just starting from another premise. Any system based on trading of property rights further requires service providers providing a safe trading infrastructure and services to individuals.[88] At this time it is impossible to foretell whether such infrastructure and services will indeed be possible and commercially viable.[89] My expectation is that such third party trade services will emerge also under current data protection laws (based on consent)[90] and that this does not require a data property right system to be implemented first.[91] For these reasons, I will here take the existing data protection system as a starting point for evaluation and suggesting potential improvements.

3. How to regulate the ungovernable future?

Given the Collingridge dilemma, how do we imagine that the complex relationship between IT and society should be regulated? Indeed through data protection regulation? Leave it to the courts? Through the marketplace or through technology itself (the solution of IT is in the IT)?[92]

What are the experiences till now? With the emergence of the internet, all advanced industrial societies faced essentially the same dilemma of how to regulate the amounts and cross-border flows of personal information, but their governments have chosen substantially different solutions to do so.[93/94] Any government regulation in the area of data protection needs to balance the interests of organisations (companies and governments) that use personal data against the potential harm such use could cause individuals.[95]
Within the EU, the regulation of data protection is based on the precautionary principle, which is deeply embedded in EU law.[96] The protection of individuals prevailed and the rights of individuals in respect of processing of their personal data have become a fundamental human right and freedom.[97] This is what is called "rights" based legislation. Other countries, and foremost the US, have taken a limited approach to data protection.[98] The limited regimes[99]

---

78) Schwartz offers 'a model for propertization of personal data that will fully safeguard information privacy.' He subsequently suggests five rules to overcome these shortcomings, which are not more intuitive or less complicated than current data protection rules: (i) limitations on an individual's right to alienate personal information; (ii) default rules that force disclosure of the terms of trade; (iii) a right of exit for participants in the market; (iv) the establishment of damages to deter market abuses; and (v) institutions to police the personal information market and punish privacy violations.

87 Rubinstein, n 32, at 14.

88 Rubinstein, n 32, at 14, considers it "too soon to say whether firms will embrace these new business models, especially if they entail satisfying the stringent security and privacy requirements identified above. Nor is it clear that consumers would be better off if PDSes become prevalent—perhaps data-driven businesses will find ways to circumvent these protections.' Rubinstein concludes by recommending that EU regulators foster new business models that support individual empowerment and thereby may accomplish by other means many of the same goals of EU data protection regulation. I agree with this recommendation, but I fail to see why this would require the introduction of property-right based legislation first. These new business models can also be achieved under current rules.

89 See for a number of examples Joseph Jerome, 'Buying and Selling Privacy: Big Data's Different Burdens and Benefits', 66 *Standford Law Review Online* 47, 3 September 2013, at 49 (see for details footnote 13) who mentions the Harvard Berkman Center's "Project VRM". VRM stands for Vendor Relationship Management and has as a goal to provide customers with both independence from vendors and better ways of engaging with vendors. Tene and Polonetsky, n 42, at 266, give other examples among which the start-up personal.com, that enables individuals to own, control access to, and benefit from their personal data. See Meet the Owner Data Agreement, available at https://www.personal.com/legalprotection.

90 Mireille Hildebrandt, 'Privacy en identiteit in slimme omgevingen', *Computerecht* 2010, at par. 2.2., to be found at http://works.bepress.com/mireille_hildebrandt/36.

91 Mireille Hildebrandt, n 90.

92 EC Report on Responsible Research, n 1, at 74.

93 This paragraph draws on my earlier publication Moerel, n 84, Chapter 3 (The Worldwide Data Protection Landscape) and para. 4.1 (Increasing Tension between Different Regulatory Systems). See Joel Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace,' [2000], *Stanford Law Review*, at 1315, 1318.

94 For a comprehensive overview of different data protection regimes, see Abraham L. Newman, *Protectors of Privacy, Regulating Personal Data in the Global Economy*, Cornell University Press 2008. The distinction between 'comprehensive regimes' and 'limited regimes' as used in here was initially introduced by Newman. See also Corien Prins, 'Should ICT Regulation Be Undertaken at an International Level?', in Bert-Jaap Koops et. al. (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, TCM Asser Press 2006, para. 6.4.3.

95 Moerel, n 84, at 37.

96 EC Report on Responsible Research, n 1, at 10, 18.

97 Moerel, n 84, at 37, indicating in fn 3 that this was a long process. See on the development of data protection as a constitutional right in the EU, P. De Hert and S. Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action,' in Serge Gutwirth et. al. (eds.), *Reinventing Data Protection?*, Springer 2009, Chapter 1, at para. 1.1.2.

98 Moerel, n 84, at 58, indicating in fn 152 that during the 1970s and 1980s, the comprehensive systems and limited systems were in relative parity. Countries which initially took a limited approach but that have now moved to

mostly focus on the public sector (shaping the processing and transfer of personal data among governmental agencies) and a select number of sensitive industries (most notably healthcare and telecommunications).[100] These limited systems generally permit the processing and transfer of personal data and rely on market mechanisms to check inappropriate processing activities. In these countries the protection of personal data is left to be driven by consumer demand in case of excesses and by industry self-regulation.[101] If governments are called to regulate, this is "harm"-based[102] as opposed to "rights"-based. In the literature, this divide is labelled as the "West Coast code" (i.e., the US) and the "East Coast code" (i.e., the EU), where the West Coast is flexible, decentralised, open and evades regulation and the East Coast is strongly top-down and seeks to impose regulation on the Wild West.[103]

It is no secret that for a decade this divide has been causing great tension between the EU and the US. With the digital era, the different systems came increasingly in contact with one another and the differences in approach have become an increased source of economic and security disputes between nations.[104] The economic debate concentrates on the limited regimes claiming that the future of e-commerce depends on the free flow of data; the comprehensive regimes claiming that the future of e-commerce depends on individuals being prepared to participate in e-commerce activities only if their data protection rights are guaranteed against business and government surveillance.[105] After 9/11 this economic debate transformed into a security debate about the information requirements of the war on terrorism. Tension between the US and the EU was raised when the US introduced the Patriot Act, expanding the state policing powers to counter terrorism and later by introduction (amongst others) of the Foreign Intelligence Surveillance Act ("**FISA**"), FISA Amendments Act 2008 ("**FISAA**"), and the Electronic Communications Privacy Act ("**ECPA**"), which extend the surveillance beyond (just) interception of communications with prior court authorisation with a new procedure for targeting non-US persons abroad without individualised court orders by means of access to all information stored e.g., by US cloud providers.[106] This tension has now come to a peak with the

---

comprehensive systems are: Australia, Canada, Japan, Czech Republic, Switzerland, Lithuania, New Zealand, and Slovakia. Countries considering legislative reform based on the Directive include Hong Kong and several jurisdictions in Latin America, such as Chile and Ecuador. Limited systems are still in place in the US, Korea, and Thailand. For a comprehensive description of systems with a comprehensive approach and systems with a limited approach, see Newman (n 94), Chapter 2. For a further comprehensive overview of the 60 countries that have data protection laws, see Miriam Wugmeister, Karin Retzer, Cynthia Rich, 'Global solution for cross-border data transfers: making the case for corporate privacy rules,' [2007] *Georgetown Journal of International Law*, Vol. 38, at para. II A.

99 Moerel, n 84, at 58, indicating in fn 153 that many (further) categorisations are possible. See for instance Cécile De Terwangne, 'Is a Global Data Protection Regulatory Model Possible?', in Serge Gutwirth et. al. (eds.), *Reinventing Data Protection?*, Springer 2009, Chapter 10, at para. 10.3, using a further categorisation of the limited systems alongside the comprehensive model (the piecemeal model, the sector-oriented model and the risk-burden balance model).

100 Moerel, n 84, at 58.

101 Moerel, n 84, at 58, under reference to Newman, n 94, at 24. For a comprehensive overview of the US on the "patchwork of privacy regulation and the lack of a dedicated privacy enforcement agency," see Kenneth A. Bamberger and Deirdre K. Mulligan, 'Privacy on the Books and on the Ground', in *Stanford Law Review*, Vol. 63, January 2011; UC Berkeley Public Law Research Paper No. 1568385, available at SSRN: <http://ssrn.com/abstract=1568385, at 103 – 114>. Also in the US is a strong call for adopting 'omnibus privacy statutes' based on the model adopted throughout Europe, see Bamberger and Mulligan (above), at 104. For further reading on the US approach of relying on a combination of sectoral law, market forces and self-regulation, reporting that the Department of Commerce and the Federal Trade Commission expressly favour a self-regulatory approach, see Ira Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes* (March 1, 2010), NYU School of Law, Public Law Research Paper No. 10-16. Available at SSRN: <http://ssrn.com/abstract=1510275>, at 2.

102 In the US privacy and data protection law is essentially tort law, see Omer Tene and Jules Polonetsky, 'To Track or 'Do Not Track': Advancing Transparency and Individual Control in Online Behavioral Advertising', *Minnesota Journal of Law, Science & Technology*, Vol. 13, No. 1, 2012, at par. 6.1, and literature referred to in footnote 189, electronic copy available at https://ssrn.com/abstract+1920505.

103 EC Report on Responsible Research, n 1, at 75.

104 *Moerel, n 84*, at 61, referring for the recent increase in surveillance across countries, to the study by Privacy International, *European Privacy and Human Rights 2010*, to be found at http://www.privacyinternational.org/ephr.

105 Moerel, n 84, at 37, under reference to Newman, n 94, at 12 – 14. See for the EU position: *Communication of the Commission to the European Council, the European Economical and Social Committee of the Regions, Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century*, COM(2012) 9 final (25 January 2012), at 1: "Lack of confidence makes consumers hesitant to buy online and accept new services. Therefore, a high level of data protection is also crucial to enhance trust in online services and to fulfill the potential of the digital economy, thereby encouraging economic growth and the competitiveness of EU industries. Modern, coherent rules across the EU are needed for data to flow freely from one Member State to another. Businesses need clear and uniform rules that provide legal certainty and minimise the administrative burden. This is essential if the Single Market is to function and to stimulate economic growth, create new jobs and foster innovation."

106 See for a comprehensive discussion of the relevant US acts and provisions regarding the US surveillance powers: Instituut voor Informatierecht, Universiteit van Amsterdam, *Cloud diensten in hoger onderwijs en onderzoek en de USA Patriot Act*, September 2012, to be found at http://www.ivir.nl/publicaties/vanhoboken/Clouddiensten_in_HO_en_USA_Patriot_Act.pdf.

Snowdon disclosures of surveillance of non-US nationals.[107] The internet thus became a zone of strong contestations, not simply over technology, but over the many areas with which it interacts.[108]

As a true European, the US approach to regulating the internet did not sit well with me. I considered it unthinkable that a democratic country would not provide for comprehensive data protection. I still am of this opinion, and find justification in the fact, that the US is now, step by step, moving towards more comprehensive data protection, as testified by the US Online Privacy Bill of Rights.[109] However, from thinking it incredulous that the US does not cater for proper rights for individuals, I have moved to thinking maybe the "harm-based" system may not be all comprehensive, but sometimes is actually very effective. In fact, in certain respects the harm-based approach has proven to be significantly more effective than the EU Data Protection Directive. It is an open secret that the EU Data Protection Directive has not achieved the envisaged material data protection in practice.[110] To illustrate this, I discuss two examples where the US reactive legislation has proven very effective (and the Directive less so) and two examples where the precautionary approach of the Directive has proven very ineffective.

Example 1: EU comprehensive data security obligation versus US data breach notification obligation

---

[107] See for an overview of the Snowden disclosures: http://www.theguardian.com/world/the-nsa-files and for a timeline: http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html. This increase in surveillance is not limited to the US. This is also an issue in the EU. For an overview of the EU security data exchange policies and the data protection implications, see the *Tenth Annual Report of the Article 29 Working Party on Data Protection*, at 7 – 8 (to be found at <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm.

[108] EC Report on Responsible Research, n 1, at 75.

[109] The Consumer Privacy Bill of Rights is outlined in a report released on 23 February 2013 by the White House *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, to be found at: http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights. The Consumer Privacy Bill of Right is non-binding, but is intended to serve as the basis for subsequent self-regulation by US industry organisations. The rights are:
Individual Control: Consumers have a right to exercise control over what personal data organisations collect from them and how they use it.
Transparency: Consumers have a right to easily understandable information about privacy and security practices.
Respect for Context: Consumers have a right to expect that organisations will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
Security: Consumers have a right to secure and responsible handling of personal data.
Access and Accuracy: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data are inaccurate.
Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
Accountability: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.
See for a report on the first privacy multi-stakeholder meeting: http://www.ntia.doc.gov/blog/2012/putting-consumer-privacy-bill-rights-practice under reference to http://www.ntia.doc.gov/other-publication/2012/first-privacy-multistakeholder-meeting-july-12-2012.

[110] Rand Report, n 72, at 35. Douwe Korff, *EC Study on implementation of the Data Protection Directive, Comparative study of national laws*, September 2002, Human Rights Centre University of Essex, at 209, to be found at <http://papers.ssrn.com>, notes that "the powers now vested in the data protection authorities, as currently exercised, have not been able to counter continuing widespread disregard for the data protection laws in the Member States." See further Omer Tene, *For Privacy, The European Commission Must Be Innovative*', Centre for Democracy & Technology, 28 February 2011, to be found at http://www.cdt.org/blogs/privacy-european-commission-must-be-innovative: "Enforcement is a sore issue for the EU DPD. It is an open secret that the framework is largely not enforced. Indeed, implementation of the EU DPD is probably highest among US based multinationals, which implement strict compliance programs for risk management purposes and as part of overall corporate governance schemes"; and "Commentary in Response to the European Commission's Communication on 'A comprehensive approach to personal data protection.'" Centre for Information Policy Leadership, January 2011, to be found at <www.huntonfiles.com> (Opinion on the Communication of the Commission on the revision of the Directive), at 12: "Articles 25 and 26 of the existing Directive have been simultaneously its most controversial and most burdensome provisions. It is also arguable that they have been the least effective if full account is taken of current volumes of international transfers. (…). The result is the paradox that substantial resources are expended by some organisations to try "to get it right" whilst there is an unmeasured non-compliance by other organisations which ignore the requirements." See further on non-compliance with the EU data transfer rules: Commission of the European Communities, *First Report on the implementation of the Data Protection Directive (95/46/EC), 15 March 2003*, COM/2003/265 final ("**First Report on the Directive**"), at 19. National DPAs are supposed to notify the Commission when they authorise a transfer under Article 26(2) Directive. The Commission notes that it has received only a "derisory number of notifications compared with what might reasonably be expected." The Commission further notes that "combined with other evidence pointing in the same direction, this suggests that many unauthorised and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate protection."

One of the fundamental principles of EU data protection law is the obligation of the controller of personal data to ensure that personal data are adequately secured.[111] US law does not have such a general obligation (except in specific laws for e.g. health data). However, in 2007, after some extensive data security breaches (e.g. hackers stealing credit card data)[112] had featured the headlines of the US newspapers, the first US state introduced a so-called data breach security notification law, imposing notification obligations on organisations that discover a data security breach.[113] By now another 45 States have similar data breach notification laws.[114] These data breach notification requirements have proven a strong driver for US companies to improve data security and data compliance in general (such as data minimisation, use of encryption and increase of security in an effort to try to prevent data security breaches (and subsequent reputational exposure) rather than address these after the fact.[115] In the US privacy rights' advocacy organisations ensure instant worldwide publicity of these breaches by publishing these collectively on their websites together with a forum for instant criticism and debate.[116] In that sense, it is frequently commented that there is no "hiding place" for multinationals.[117] As "brand value" is an increasing component of the market value of a company, so too is reputation.[118] Outsourcing does not diminish this reputational exposure[119] as in practice any mistakes made by sub-contractors are attributed in the press to well-known brand holders, as they are easy targets for criticism (a phenomenon which has been labelled the "brand boomerang").[120] Research shows that even in the case of data breaches in respect of which a multinational is not to blame whatsoever (for instance if criminal hackers have stolen data), data breach notifications in respect of confidential data (like credit card data) have a serious impact on the stock prices of listed companies.[121] This reputational exposure of multinationals for data protection and

---

111 Article 17 Directive, cf Article 30 Proposed Regulation.

112 A data security breach means any unauthorized acquisition, access, use or disclosure of unencrypted personal data that compromises the security or privacy of such data.

113 Moerel, n 84, at 89, indicating that these state security breach notification laws are understood to be modelled on the California Security Breach Notification Act, which came into force in July 2007 (Cal. Civ. Code § 1798.82 (LEXIS through 2007, Ch. 12, June 7, 2007).

114 See for a summery overview of data breach notification requirements around the world: Karin Retzer and Joanna Łopatowska, 'Dealing with Data Breaches in Europe and Beyond', *PLC Cross-border Data Protection Handbook 2011/12*.

115 This paragraph (including footnotes) is a summary of Moerel, n 93, at 92 – 94. See Bamberger and Mulligan, n 101, at 106, who report their results of empirical research in the US which shows that introduction of the US data breach notification laws has been a main driver for what he calls substantial 'privacy on the ground' compliance by US companies: "While individual US sectoral statutes and the EU Data Protection Directive were credited in some instances for firms' initial commitment of resources and personnel, and for the establishment of a regulatory floor, the path these professionals would take was influenced by two other regulatory developments, notably: the rise of the Federal Trade Commission's role as an 'activist privacy regulator' advancing an evolving consumer-oriented understanding of privacy; and the passage of state Security Breach Notification (SBN) laws as a means for binding corporate performance on privacy to reputation capital."

116 For an overview of worldwide data security breaches, see <www.privacyrights.org> and www.attrition.org (reporting 850 major data breaches since 2001). Many more may be found by simply searching for 'data breach security.'

117 See on the phenomenon that due to new technology there is no hiding place for multinationals as to corporate responsibility, Doreen McBarnet, 'Corporate social responsibility beyond law, through law, for law: the new corporate accountability', in McBarnet, Voiculescu, Campbell (eds.), *The New Corporate Accountability, Corporate Social Responsibility and the Law*, Cambridge University Press 2007, at 15.

118 McBarnet, n 117, at 16, referring to the analysis of FTSE 100 companies in 2005, which found that 60% of the companies' market value had to be categorised as 'intangible' and 53% under US Fortune 500 in 2006. An interesting perspective on the value of reputation of a company is provided by Lorenzo Sacconi, 'Corporate Social Responsibility (CSR) as a Model of 'extended' Corporate Governance: an Explanation Based on the Economic Theories of Social Contract, Reputation', in Fabrizio Cafaggi, *Reframing Self-Regulation in European Private Law*, Kluwer Law International 2006, at 317, who explains the crucial role the reputation mechanism plays in economic theories, in particular the 'trust game': "Reputation is one of the most valuable, albeit intangible, of the firm's assets. It is reputation that induces the stakeholders to trust the firm and consequently to cooperate with it, so that transactions come about at low costs of control or bargaining." See Sacconi, at 18 for an explanation of how the trust game functions as to CSR which includes privacy.

119 In the case of outsourcing data processing operations, data security offered by the outsourcing supplier is often better than when the company itself processed the data (in my experience as a practitioner, this is often one of the reasons to outsource). In that sense, outsourcing does not create additional exposure for the company.

120 An example is the public attack on H&M and C&A in the Dutch newspapers (*Volkskrant* dated 3 September 2010) for breaching human rights when it was revealed that a manufacturer they both use in India violates the rights of (all female) textile workers by not offering an employment contract and prohibiting contact with labour unions. The women are *de facto* locked up in housing on the walled manufacturing property, 25% of their wages is withheld for their dowry to be paid only after three years of service and payment of a wedding, which will only induce workers to work extremely long hours. Additionally, the manufacturer only pays overtime after 3 years of employment. For some other examples see McBarnet, n 117, at 16.

121 Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb and Lei Zhou, 'The economic cost of publicly announced information security breaches: empirical evidence from the stock market', *Journal of Computer Security* 11 (2003), at 443 – 445, which reports that they "find a highly significant negative reaction [on stock prices] for those breaches that relate to violations of confidentiality"; and L. Murphy Smith and Jacob L. Smith,

security breaches has had a stronger impact on data security than the EU fundamental data protection laws has ever had.

Example 2: EU information obligations and purpose limitation versus US prohibition of unfair trade practices

EU law requires controllers to obtain consent for many types of data processing and further to disclose to individuals what data they collect and for which purposes these are processed. The US has Section 5 Federal Trade Commission Act ("**FTC Act**"), which prohibits unfair or deceptive trade practices. In the past ten years the Federal Trade Commission ("**FTC**") has used its authority under Section 5 FTC Act, to take action against companies that misrepresent their data protection practices to consumers.[122]/[123] This enforcement power has proven very effective in practice. Providers like Google and Facebook know exactly which data processing practices their customers consider "creepy" and they try to hide these in their data protection policies. That is subsequently exactly what the FTC prosecutes and fines them for. Enforcement feels spot on. For instance, the FTC fined Google, based on deceptive tactics and violation of its own privacy promises to consumers when it launched its social network, Google Buzz, in 2010. On 30 March 2011, the FTC announced[124] that Google accepted the FTC settlement order barring the company from future privacy misrepresentations, requiring it to implement a comprehensive privacy program, with regular, independent privacy audits for the next 20 years. A result which we have not remotely been able to achieve in the EU, despite each and every Member State having a Data Protection Authority with enforcement and fining powers and all individuals having extensive data protection rights.

And now two examples where the proactive precautionary approach of the EU, trying to regulate new technology, has proven very ineffective (being a case in point of the Collingridge dilemma).

Example 3: EU rules on digital signatures are obsolete

At the onset of the internet, the EU identified as a potential obstacle to the development of e-commerce that most Member States had national requirements that contracts required a written signature. The EU tried to facilitate online contracting by imagining under what circumstances a digital signature could be considered equal to a written signature, so contracts could also be

---

'Cyber Crimes Aimed at Publicly Traded Companies: Is Stock Price Affected?', at 12, to be found at the site of Texas A&M University http://www.tamu.edu/: "Results suggest that costs of cybercrime go beyond stolen assets, lost business, and company reputation, but also include a negative impact on the company's stock price, at least in the short run." See further Annex 6 for a table with effect on stock prices in 10 cases.

122 An overview of FTC enforcement cases in respect of data protection policies can be found at <www.ftc.gov>. This is an example where a public agency is not only tasked with enforcement of administrative or criminal legislation but also tasked with monitoring and enforcement of businesses to act consistently with their private law obligations, see Colin David Scott, *Enforcing Consumer Protection Laws* (July 30, 2009), UCD Working Papers in Law, Criminology & Socio-Legal Studies Research Paper No. 15/2009, available at SSRN: <http://ssrn.com/abstract=1441256>, at 7, also published in: Howells, Geraint, Iain Ramsay and Thomas Wilhelmsson (eds), *Handbook of International Consumer Law and Policy*, Edward Elgar 2010.

123 The FTC also enforces a number of sector-specific statutes that include data protection provisions, including the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Act (COPPA), the CAN-SPAM Act and the Telemarketing and Consumer Fraud and Abuse Prevention Act (Do Not Call Rule). See the Fair Credit Reporting Act, 15 U.S.C. para. 1681 (2010) (regulating the reporting on consumer credit history); Gramm-Leach-Bliley Act, 15 U.S.C. paras. 6801-6809 (2010) (regulating consumer financial data); COPPA, 15 U.S.C. paras. 6501-6506 (2010) (regulating information about children); CAN-SPAM Act, 15 U.S.C. paras. 7701-7713 (2010) (regulating unsolicited electronic messages); and Do Not Call Rule, U.S.C. paras. 6101-6108 (2010) (regulating telemarketing calls).

124 See press release dated 30 March 2011 'FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network. Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data', to be found at <http://ftc.gov/opa/2011/03/google.shtm>. The FTC announced that Google agreed to settle charges that it used deceptive tactics and violated its own privacy promises to consumers when it launched its social network, Google Buzz, in 2010. According to the FTC's complaint (i) Google led Gmail users to believe that they could choose whether or not they wanted to join Google Buzz, while the options for declining or leaving Google Buzz were ineffective; (ii) for those who joined Google Buzz, the controls for limiting the sharing of their personal information were difficult to locate and confusing; (iii) Google violated its privacy policies by using information provided for Gmail for another purpose – social networking – without obtaining consumers' permission in advance; and (iv) Google misrepresented that it was treating personal information from the EU in accordance with the US Safe Harbor Framework because it failed to give consumers notice and choice before using their information for a different purpose from that for which it was collected. The settlement requires Google (i) to obtain consumers' consent before sharing their information with third parties if Google modifies its sharing practices; (ii) to establish and maintain a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information; and (iii) to obtain initial and biennial assessments for 20 years from an independent auditor to ensure that it is following the required comprehensive privacy program.

validly entered into online.[125] The technical requirements the EU legislators set for digital signatures were, however, so strict that these never became widely used, making this an obsolete piece of legislation. The issue of the requirement that certain contracts require a written signature is solved in practice by having these contracts signed in writing and subsequently scanned and electronically stored. The original copy is then destroyed. In case of a dispute about the validity of the contract, the digital scan serves as proof of the fact that the contract was validly entered into by means of a written signature.

Example 4: the EU cookie rules are ineffective
Recently the EU updated the cookie rules.[126] The EU cookie rules require opt-in consent of users for placing a cookie on their computer, with very narrow exceptions only. In practice all websites use cookies, often as many as 10-20, which also include types of cookies that individuals do not really care about, as these just facilitate a good website user experience and tailor content on a site to their interests (derived from earlier visits). As a result users have to provide consent to many cookies and, as a rule, accept all cookies in one go.[127] They do not bother to differentiate between the different cookies, also providing opt-in for cookies they do care about, such as cross-site tracking cookies. Research shows, however, that most users seriously object to being tracked across sites for advertising purposes by use of tracking cookies.[128] By giving users too many rights (requiring opt-in's for too many cookies), the cookie rules become ineffective.[129] Again, most of us are not *econs*, but *humans* and do not always act in our own self-interest. Here an opt-in (or even an opt-out) just for cross-site tracking cookies would probably have proven more effective. This is in fact a harm-based approach, the opt-in requirement is limited to objectionable cookies only. This comes close to the proposal by the FTC in 2010 to introduce a Do-Not-Track mechanism for online behavioural advertising (requiring cross-site tracking cookies), which opt-out possibility has to be provided 'at a time and in a context in which a user is making a decision about his data'.[130]

What is the lesson from these examples? Abandon the EU system and adopt the US system? A bit more thinking is required. If it was that simple we would have got it right the first time. Hereafter, I will explore what the concept of data protection is (or what is left of it); and (ii) whether people still care. Before making suggestions to improve EU data protection law, I will discuss four paradoxes which make data protection difficult to grasp and regulate. Thereafter I will try to tie everything together and assess whether data protection is indeed fit to act as the organising principle of big data and make a proposal on how to improve EU data protection laws in order to achieve better results.

4. What is the concept of data protection?

Data protection is a social construct and as such subject to continuous change.[131] An example is that individuals used to consider as very sensitive whether a worker was a trade union member. Their income was, however, fixed and known to all. Now trade union membership is commonly known, but people are very private about their income and health data.[132] This is not problematic. The concept has just evolved over time. In 1890, Warren and Brandeis wrote the

---

125 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 013, 19/01/2000.

126 Article 5(3) of the Directive on privacy and electronic communications, OJ 2002 L 201, as revised by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (**e-Privacy Directive**).

127 Tene and Polonetsky, n 102, at par. 2.1,

128 The *Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing*, May 2011, at 15, reports on a survey that shows that nearly 75% of respondents were either not very comfortable or not comfortable at all with tracking-based advertising, to be found at https://www.priv.gc.ca/resource/consultations/report_201105_e.asp. See further Tene and Polonetsky, n 102, at par. 3, under reference to Joseph Turow, Jennifer King, Chris Hoofnagle, Amy Bleakley and Michael Hennessy, 'Americans Reject Tailored Advertising and Three Activities that Enable It', Sept. 29, 2009, http://repository.upenn.edu/cgi/viewcontent.cgi?article=1138&context=asc_papers, reporting that 66% of adults in the US do not want websites to show them tailored advertising; 75% do not want ads based on websites they visit; and 87% do not want ads based on websites they have visited.

129 Tene and Polonetsky, n 102, at paras. 1 and 6.1.

130 See Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, December 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. See on the legislative initiatives and developments on the Do-Not-Track proposal, Tene and Polonetsky, n 102, at paras. 5.1 – 5.3.

131 EC Report on Responsible Research, n 1, at 102.

132 EC Report on Responsible Research, n 1, at 102.

first publication on privacy, describing privacy as "the right to enjoy life, the right to be let alone."[133]

> In very early times, the law gave a remedy only for physical interference with life and property. [...] Gradually the scope of these rights broadened; and now the right to life has come to mean the right to enjoy life – the right to be let alone
>
> **S.D. Warren, and L.D. Brandeis, "The Right to Privacy", *Harvard Law Review Boston, 1890***

After World War II, a number of European countries extended the right to privacy to include protection of personal data. During the war, governmental registries of personal data of EU citizens were used to segregate populations, target minority groups and facilitate genocide, evidencing the risk of abuse of personal data.[134] The various data protection laws of European countries were subsequently harmonised in the EU data protection Directive. The Directive is based on the concept of "informational privacy" which regulates how individuals relate and control access to information about them which is processed by companies and governments.[135] Now, with the emergence of social media, we suddenly see that, in its turn, this concept of informational privacy is under pressure.

In 2010 Mark Zuckerberg (CEO and founder of Facebook) caused quite a stir when he publicly said:[136]

> People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.
>
> **Mark Zuckerberg, CEO Facebook (2010)**

Is he right? History shows that whenever a new technology is introduced, society needs time to adjust. As a consequence, at this time the internet is still driven by the possibilities of technology rather than social and legal norms.[137] This inevitably leads to social unrest and a call for new rules.[138] This assumes that the current rules are not adequate, but are they? Why our data protection laws are under pressure was well phrased in 2008 by the International Working Group on Data Protection in Telecommunications:

---

133 See S.D. Warren & L.D. Brandeis, 'The Right to Privacy', *Harvard Law Review* 1890-5, at 193. See also EC Report on Responsible Research, n 1, at 134 citing Alan Westin: "privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".

134 After World War II, a number of international conventions on human rights were adopted all of which recognise the right to privacy and data protection. See Article 12 of the Universal Declaration of Human Rights (1948); Article 8 of the European Convention on Human Rights (Council of Europe, 1950); Article 17 of the International Covenant on Civil and Political Rights (UN, 1966). With the increase in use of information and communication technology in the 1970s, the risk of personal data being abused increased further and more tailored regulation was required. This resulted in adoption on the international level of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) and the Council of Europe Convention 108 for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981). At the EU Member State level France, Germany and Sweden introduced comprehensive data protection laws. On the other hand, Spain, Italy, Portugal, Greece and Belgium had no data protection laws at all. This diversity constituted a barrier to the development of the EU internal market. In this context the Data Protection Directive was created in 1995. The Directive harmonised the various national data protection laws already in force in some EU Member States. Since introduction of the Directive, the world has moved on to a networked society where personal data are continuously collected, enhanced, exchanged and reused. This has led EU legislators to embark on a revision of the Directive. At the time this report was finalised, the status on the thinking of the Commission on revision of the Directive is reflected in the Proposed Regulation, n 44.

135 See the Rand Report, n 72, at 1 – 10.

136 B. Johnson, 'Privacy no longer a social norm, says Facebook founder', *The Guardian* 11 January 2010, www.guardian.co.uk/technology/2010/jan/11/facebook-privacy.

137 Schmidt and Cohen, n 1, at 59.

138 M. de Cock Buning, *Auteursrecht en informatietechnologie: over de beperkte houdbaarheid van technologiespecifieke regelgeving*, diss. Amsterdam UvA, Otto Cramwinckel 1998, at 214 ff.

> 'With respect to privacy, one of the most fundamental challenges may be in the fact that most of the personal information published in social networks is being published at the initiative of the users and based on their consent. While "traditional" privacy regulationis concerned with defining rules to protect citizens against processing of personal data by the public administration and businesses.'[139]

As to social media users themselves publishing their information, Facebook initially contested that it was subject to EU data protection laws. However, by now also Facebook acknowledges that the EU data protection laws apply to its platform.[140] In 2009, this became clear in a landmark opinion of the advisory committee to the European Commission on data protection ("**WP29**"),[141] confirming that Facebook and other social networks should be considered to be the "controller" of the personal data published on their platforms and in that capacity should cater for "privacy friendly default settings". This means that these platforms should protect their users by having as a default setting that their data are shared with their selected friends only (rather than set on 'sharing with all members of Facebook', or even: 'searchable by Google').[142] If people agree to sharing with everybody on Facebook or being searchable by Google, this should require an active change of the default setting by a user. This therefore requires active opt-ins, the possibility to opt-out is not sufficient. This enables individuals to create different circles, different contexts.[143]

This opinion of the WP29 on social media amounts to what is called 'contextual privacy'. What is shared in one context is not necessarily public in another. This is considered crucial in legal theory as someone's identity is determined by the context in which he/she operates.[144] In other words, individuals have the right to behave differently (and thus creating a different identity) with friends, the soccer club, or family. This is an expression of the fact that data protection is not only a fundamental right but also a freedom.[145] This may have been a matter of course in the physical world, but this is not a given in the online world where (if you do not take care), everything can be found by Google. [146]

The freedom of unreasonable restrictions on the construction of your own identity

Philip Agre & Marc Rotenberg, 'Technology and Privacy: The New Landscape' (1997)

This is not new. From the first publication on privacy of Warren and Brandeis it can already be derived that privacy is a contextual concept.[147] The authors reported on a court case in which the

---

139 International Working Group on Data Protection in Telecommunications, *Report and Guidance on Privacy in Social Network Services - Rome Memorandum*, 4 March 2008 ("**Rome Memorandum**"), at 1. to be found at www.cbpweb.nl/downloads_int/opinie_social_network_services.pdf.

140 Facebook, 'Response to European Commission Communication on personal data protection in the European Union', ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/facebook_en.pdf, at 10; Facebook Safeharbor Certification, safeharbor.export.gov/companyinfo.aspx?id=12058.

141 The Working Party 29 is established as an advisory body to the European Commission under Article 29 of the Directive. The Working Party 29 has advisory status only and acts independently, see Article 29(2) Directive. Members are representatives of each of the DPAs, the European Data Protection Supervisor and the European Commission.

142 Also in the US Facebook was prosecuted. The Federal Trade Commission ("**FTC**") considered that Facebook did not adhere to its own Privacy Policy, which was therefore considered misleading. In 2011 Facebook settled the issue with the FTC, agreeing that for the coming 20-years an independent third party will perform a privacy audit. See FTC, 'Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises', 29 November 2011, www.ftc.gov/opa/2011/11/privacysettlement.shtm; See also FTC, 'Statement of the Commission in the matter of Facebook', Inc., COM(2012)4365www.ftc.gov/os/caselist/0923184/120810facebookstmtcomm.pdf.
The comment of Jon Leibowitz, Chairman of the FTC: 'Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions of users. Facebook's innovation does not have to come at the expense of consumer privacy. The FTC action will ensure it will not.'

143 Article 29 data protection Working Party, Opinion 5/2009 on online social networking, to be found at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

144 Philip E. Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape,* MIT Press 1997, at 7, to be found at http://mitpress.mit.edu; see also Hildebrandt, n 90, at 172.

145 Hildebrandt, n 144, at 172. See also H. Nissenbaum, 'A Contextual Approach to Privacy Online', *Daedalus*, 2011-4, 140: "we must establish respect for the boundaries of context and associated information norms"; EHRM 7 February 2012 (Von Hannover/Germany), par. 95.

146 Hildebrandt, n 90,at 172. Schmidt and Cohen, n 1, at 55 indicate that this will be the first generation of people with an indestructible archive.

147 See Warren and Brandeis, n 133, at 193.

plaintiff opposed to publication of his portrait which had been made without his consent by means of a portable camera. This had not been possible before, since until then making portraits required long exposure and special studio light. The authors start with a general reflection on the law, which is as apt now as it was in 1890:

> "Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society.'[148]

The authors subsequently consider privacy as a contextual concept, whereby publication in one context cannot automatically be considered as a publication to the public at large. The right to privacy in that case remains applicable:

> 'The common law secures to each individual the right of determining [...] to what extent his thoughts [...] shall be communicated to others. [...] the individual is entitled to decide whether that which is his shall be given to the public'.

> 'The right to privacy ceases upon the publication of the facts by the individual, or with his consent [...] whereby a private communication of circulation for a restricted purpose is not a publication within the meaning of the law.'[149]

A similar opinion, but from a different discipline, is heard in recent US literature. The complaint is that currently the internet is driven too much by technology rather than governed by social norms and that this leads to unacceptable consequences. The internet should not be a universal free haven. Also on the internet there are different social contexts, which should be governed by the social norms which would govern the offline equivalent. In the words of Helen Nissenbaum[150]

> The context in which activities are grounded shape expectations that, when unmet, cause anxiety, fright, and resistance.
>
> **Helen Nissenbaum, 'A Contextual Approach to Privacy Online' (2011)**

The conclusion is that Marc Zuckerberg's statement that people have become more comfortable in sharing their personal data is true, but this does not necessarily mean that data protection is thus obsolete.
Actually it is the contrary. The rationale for data protection is especially to protect individuals against violations of their right to behave differently in different context, i.e. their right to self-identity (also labelled the right to moral autonomy).[151] Without this right, having a profile on Facebook or other social media would automatically result in one omnipresent profile across the internet. I indicated in the introduction that this right of moral autonomy is also threatened by the new ability to analyse vast amounts of data which lead to the finding of correlations which lead to predictions that one will e.g., have a heart attack. With such predictions, the right to identity, the right to decide for yourself 'who am I' and 'what do I like' risks turning into **being told** "what you are" and "what you will like".[152] The conclusion is that data protection does indeed have an important role to play in the online environment, probably even more so than in the physical world where context is mostly a given.

---

148 See Warren en Brandeis, n 133, at 193.
149 Warren en Brandeis, n 133, at 193, 198, 214 en 218.
150 Nissenbaum 2011, n 145, at 38.
151 See the Rand Report, n 72, at 16. The Rand Report also notes that in addition to the protection from harm to individuals, data protection also has an inherent value to society which should not be overlooked. "Exercising such freedoms as the freedom of speech, freedom of association and the freedom to practice religion in a meaningful way requires that the individual has a suitable personal sphere to develop his or her convictions and decide how to exercise these. Privacy rights thus can act as a vehicle to exercise other rights. Privacy protection is therefore not only essential as a safeguard for personal wellbeing, but also to ensure the needed freedom and creativity that may benefit society as a whole. Thus, for the purposes of defining more or less stringent data protection rules, the debate cannot be posed purely in terms of trading personal freedom for societal benefit. Privacy and data protection should not be characterised as a zero sum gain where an individual gain means a societal loss or vice versa."
152 Richards and King, n 29.

The same applies to the other forms of direct and indirect damages data protection is designed to protect individuals against. Also these are as relevant (and even more so) in this age of big data:

Information-based harm: an obvious example is identity theft (leading to credit card or other frauds), which has become one of the key concerns in the online environment.[153]

Information inequality: when information about an individual is used without the individual knowing this. An example is where employers turn down job candidates based on information on social media without informing the candidate of this and providing him/her with an opportunity to correct the information or put it in context. This becomes even more pressing now a study shows that a job-candidates profile on Facebook is better at predicting job performance than IQ tests.[154] With predictive analytics enabling companies and governments to predict what e.g., the chance is that individuals will succeed at their jobs, default under their mortgage, this will become more and more of an issue if companies and governments are not at least forced to inform individuals of their use of predictive analytics.

Information injustice: where information collected in one context is used in another. For instance, registration of payment history on a loan is used to reject insurance or a mortgage, etc. Information injustice is often preceded by information inequality, if the relevant individual is not informed of the fact that information collected in one context is used in another. This category also includes the example of preemptive analytics assessing the risk that a convict will offend again, which results are used for sentencing and parole decisions. The incarcerated person will have no recourse to prove this assumption unjust, as how would he prove what his future behaviour outside prison would be?[155] Another form of information injustice is where the increased predictive analytics leads to 'pigeonholing' individuals into pre-determined categories, which are difficult to get out of as content and services presented to a category are narrowed down, and any subsequent choice confirms the earlier predictions. Predictive analytics thus becomes a self-fulfilling prophecy[156] and favours the established classes (as these have good credit scores and good consumption profiles). An invasion of their data protection will be to their benefit. The lower classes and vulnerable groups (susceptible to disease, crime, or other socially stigmatizing characteristics or behaviours) will be more likely to feel the negative impact from big data.[157] 'In the end the worry may not be so much about having information gathered about us, but rather being sorted in the wrong or disfavoured bucket'.[158]

The conclusion is that the right to data protection is not only still relevant but will be crucial to address the potential harms of big data and analytics. The law is just (as always) slow to catch up with technology. Data protection will, however, not help against some of the other downsides of the new economy, such as the risks of social fragmentation, cultural impoverishment, and a potential increasing income divide between the have and the have nots due to the gift economy. That is outside the realm of data protection. That being said, there is no doubt a role to play for data protection.

5. Do (especially young) people care about data protection?

Research shows that data protection remains an important value and that there is a baseline of personal life which comprises very personal, intimate data, which people (as a matter of principle) consider should be free from any surveillance.[159] A US study further shows that the attitudes towards data protection expressed by young adults (18-24) (*Digital Natives*) are not nearly as different from those of older adults (*Digital Immigrants*), as is often suggested. An important difference is, however, the higher portion of 18-24 year olds that incorrectly believe

---

153 Carr, n 1, at Chapter 9 'Fighting the Net' discusses the threats to the net and individuals using it. Carr signals that the very qualities that make the world wide computer so useful to many (its universality and openness) make it dangerous as well. Schmidt and Cohen, n 1, at 39, predict that a black market will become available for stolen or fake identifies as well as kidnapping of identifies of rich people which will only be returned against payment of a ransom.

154 Donald Kluemper, Peter Rosen and Kevin Mossholder, 'Social Networking Websites, Personality Ratings, and the Organizational Context, More than Meets the Eye?', *Journal of Applied Social Psychology*, Vol. 42, issue 5, at 1143 – 1172, to be found at http://onlinelibrary.wiley.com/doi/10.1111/j.1559-1816.2011.00881.x/full.

155 Siegel, n 5, at 59 – 62. See on preemptive predictions, Kerr and Earle, n 36.

156 Tene and Polonetsky, n 29, at 254.

157 Tene and Polonetsky, n 29, at 252 – 253.

158 See Jerome, n 89, at 50 – 51, under reference to Omer Tene, 'Privacy: For the Rich or for the Poor?, Concurring Opinions' (July 2012), to be found at http://www.concurringopinions.com/archives/2012/07/privacy-for-the-rich-or-for-the-poor.html.

159 EC Report on Responsible Research, n 1, at 40.

that their online and offline privacy is better protected than it actually is.[160] This calls for education of our children on how to navigate the electronic highway just as we teach them how to navigate regular traffic. We do not forbid them to ride a bike, we teach them how to ride a bike.[161] Another study shows that for Digital Natives, privacy is developing towards a right to "flexible audience management"; they decide what kind of information they want to share with whom. Research shows that most have their privacy settings such that they only share with friends and not with Facebook as a whole. They also do not post their real address, email-address and phone number.[162] This is also my own experience. Every time I teach a new class I ask the students 1. Who of you is on Facebook (98% yes); 2. Who has tuned his privacy settings (85%). Who has his parents as a friend? (only 15% yes). They know when, with whom and what to share![163]

6. Four paradoxes

Paradox – trust

We just saw that EU regulators claim that the future of e-commerce depends on individuals being prepared to participate in e-commerce activities only if their data protection rights are guaranteed against business and government surveillance.[164] The European Commission[165] expresses this rationale as follows:

> "In this new digital environment, individuals have the right to enjoy effective control over their personal information. Data protection is a fundamental right in Europe [...]. Lack of confidence makes consumers hesitant to buy online and accept new services. Therefore, a high level of data protection is also crucial to enhance trust in online services and to fulfil the potential of the digital economy, thereby encouraging economic growth and the competitiveness of EU industries."

Surprisingly, a similar sentiment was recently expressed by US President Obama when presenting his new Online Privacy Bill of Rights:[166]

> "American consumers can't wait any longer for clear rules of the road that ensure their personal information is safe online. As the Internet evolves, consumer trust is essential for the continued growth of the digital economy. That's why an online privacy Bill of Rights is so important. For businesses to succeed online, consumers must feel secure. By following this blueprint, companies, consumer advocates and policymakers can help protect consumers and ensure the Internet remains a platform for innovation and economic growth."

However, for consumers to trust companies, companies have to establish a relationship with consumers. Trust is what companies earn "by actively watching out for [their] customers'

---

160 EC Report on Responsible Research, n 1, at 141.

161 The lack of data protection on the internet is for some experts an occasion to urge the government to issue a prohibition on children becoming a member of social media sites. See S. van Vloten and J. Nijssen, 'Interview Bernt Hugenholtz, professor information law, University of Amsterdam: 'Enforcement of copyright in music is senseless', *Amsterdams Balie Bulletin*, March 2012: "If people do not realise they play with fire, then it must be forbidden to play with fire. Just in the manner as the use of fireworks is regulated' (translation by the author), to be found at www.baliebulletin.nl/PDF/2012/Maart2012/ABB_maart_2012_interview_Hugenholtz.pdf.

162 EC Report on Responsible Research, n 1, at 141

163 See on the topic whether consumers care about their privacy extensively Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change, A proposed Framework for Business and Policymakers,* December 2010, at 28. The FTC provides some illustrative facts and figures, such as that 35% of Facebook's 350 million users customised their privacy settings when Facebook released new privacy controls in December 2009; and the fact that 77 million Mozilla Firefox users downloaded NoScript, a privacy- and security-enhancing tool that blocks Javascript commands. See further references in n 128.

164 Newman, n 94, at 12 - 14.

165 European Commission, C*ommunication of the Commission to the European Council, the European Economic and Social Committee of the Regions, Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century*, COM(2012) 9 final (25 January 2012), at 1.

166 Press release White House, '*We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online',* 22 February 2012*, to be found at* http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

interests, taking action when necessary to protect those interests".[167] This requires proactive steps to ensure that customers do not make mistakes, overlook a service or benefit, e.g. a telecom subscription which would better fit their calling pattern. In the words of Pepper and Rogers: "Knowing that a customer's interest is not being well served and doing nothing about it is untrustable. Not knowing is incompetent".[168] For "knowing" you need to analyse your customer data, to know when a subscription is up for renewal, what type of subscriptions a customer has (mobile, fixed) and the data use patterns, in order to match the best subscription package. But, the more customer data a company processes, the more the customers feel they're being watched, which may have a negative impact on trust. So the question is: How to get to know your customer, without losing trust? This question is getting more urgent every day as big data applications are increasingly applied in practice, without individuals knowing. We already have come to the point where if companies and governments would be really transparent about the data sets they collect, combine and the purposes of use, this would in all likelihood cause public consternation similar to that of the Snowden disclosures. The trust paradox may therefore also be named the "transparency paradox". Big data evangelists promise to make the world more transparent and tout the "end of privacy", while at the same time the big data revolution occurs mostly in secret. [169]

> Too much transparency too soon presents as much a risk to destabilising the personal data ecosystem as too little transparency.
>
> **World Economic Forum Report 2011**

Paradox - security

Regulators want more security on the internet, but security measures such as access controls require the processing of a login name and password, or even a fingerprint, to authenticate users for access. However, the more data are processed, the larger the risks that data are lost, compromised or hacked. Another example is that implementing certain privacy controls actually requires the processing of more personal data. For example, a ban on the processing of data of children requires the processing of more information to ensure that website visitors are indeed not children. And even a more fundamental security paradox: if for security purposes employees and individuals are monitored (e.g., by their employer or the NSA) they feel they're being watched and controlled, which makes people feel less secure. The latter is, however, not a necessity if done properly, since security and privacy do not always need to be a zero sum game.[170]

Paradox – control

Research shows that if you provide individuals with more control over their information (i.e., increasing their data protection), they actually end up providing you with more personal information (decreasing their data protection). For example, if you provide an individual with access to his profile (i.e., we think you have two children and a dog), individuals actually correct this information and as a result *de facto* provide you with more and better information. Another example is that if individuals feel that they have control over their data (just imagine a company actually gets proper data protection compliance in place) they are inclined to entrust more data to such company which *de facto* leads to less protection.[171] A similar paradox is known from other fields. An example here is the introduction of the safety belt legislation. This did not lead

---

[167] Peppers and Rogers, n 47, at 21.

[168] Peppers and Rogers, n 47, at 6 and 24.

[169] See Richards and King, n 63, who call this the "transparency paradox, where big data promises to use this data to make the world more transparent, but its collection is invisible, and its tools and techniques are opaque, shrouded by layers of physical, legal, and technical privacy by design. If big data spells the end of privacy, then why is the big data revolution occurring mostly in secret?"

[170] EC Report on Responsible Research, n 1, at 41.

[171] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein, *Misplaced Confidences: Privacy and the Control Paradox:* "in announcing 'more privacy options' and settings that users could control, Facebook's official blog stated: "Today, we are introducing privacy changes that work towards our goal of giving you the control you need in order to share information comfortably on Facebook." Our results, however suggest that affording more control to users may not necessarily help them to better protect their privacy, but rather it may induce them to reveal more sensitive information.", to be found at http://www.futureofprivacy.org/wp-content/uploads/2010/09/Misplaced-Confidences-acquisti-FPF.pdf.

to the expected reduction in fatalities, as people felt more secure with their safety belt and drove less carefully.[172]

Paradox - more is less

The more rights individuals get, the less they seem to care. The EU cookie law I just discussed is an example par excellence. The EU cookie rules provide opt-in rights for cookies that individuals do not really care about. As a result they as a rule accept all cookies in one go, not bothering to differentiate between the different types of cookies. However, if asked, most individuals will say they seriously object to being tracked across sites by means of tracking cookies. In other words, what people actually do is at odds with what is in their self-interest. This is not a new phenomenon. A director of the Dutch financial markets regulator AFM recently said in a leading Dutch newspaper (translated and paraphrased by the author):

> "Initially we believed that more transparency and better product information would protect the consumer adequately against abuse by financial institutions. But we realise now that transparency is not sufficient. The consumer acts irrationally. People do not read the mandatory financial information leaflets; they find these too complicated. People also show habitual patterns, such as an aversion to losses. This means that information alone is not sufficient. We have to adapt the financial products themselves".[173]

This is exactly what the emerging field of behavioural economics is about. The standard economic theory is based on the assumption about human nature that we are capable of making the rational decisions about ourselves (the *homo economicus*). And that if we make a mistake, market forces will correct these and set us back on the right track.[174] Behavioural economists, however, have shown that people are far less rational than standard economic theory assumes. They are *homo sapiens*. Moreover, these irrational behaviours of humans are neither random nor senseless. They are systematic, and since we repeat them again and again, predictable."[175] We should take the predictable irrational behaviour of the *homo sapiens* as a starting point for the choices regulators have, rather than the rational self-interest of the *homo economicus*. Two factors play a role in the predictability of the irrational behaviour. The first is the "inertia of the installed base" or the "status quo bias", meaning basically that people have a strong tendency to do nothing and go along with the default settings.[176] For example, a mobile phone comes with many choices for settings, from the ring tone, the background to the number of times a phone rings before going to voicemail, etc. Many people do not change these, they cannot be bothered.[177] This principle applies also if the stakes are higher than the choice of a ring tone, such as data protection. One of the causes for the inertia of the installed base is lack of attention. People are too busy trying to cope in a complex world in which they cannot afford to think deeply about every choice they have to make.[178] Situations in which people are least likely to make good choices (and that are relevant here) are:

- if the information to be digested is complicated (e.g., the use of cookies fits this criterion);
- if there are benefits now and the cost will come later (the cookies example also fits this criterion: acceptance of all cookies gives the quick win of access to the website which has the information I was looking for and desperately need, and the cost will come later: my data being used for irritating advertising when I visit other sites);[179]
- if a certain choice requires more effort, the path of least resistance is chosen (also applicable to cookies: implementing the cookie settings is time-consuming, much more so than just accepting them);[180] and a related one:

---

172 W. Janssen, Seat belt wearing and driving behaviour: An instrumented-vehicle study', Apr. 1994; Vol 26(2) *Accident Analysis and Prevention*. at 249 – 61, which showed that introduction of seat belt legislation did not lead to a less-than-expected fatality reduction. See for a summary of the study at http://www.ncbi.nlm.nih.gov/pubmed/8198694?dopt=Abstract.

173 Interview with Theodor Kockelkoren, board member of the Netherlands Authority for the Financial Markets – AFM, 'Consumenten zijn niet opgewassen tegen de groeidrift van de financiele sector', *Volkskrant* 31 August 2013. See on loss averseness Thaler and Sunstein, n 30, at 33.

174 Dan Ariely, *Predictably Irrational*, HarperCollings publishers 2010, at Introduction, at xix - xx.

175 Thaler and Sunstein, n 30, at 8.

176 Thaler and Sunstein, n 30, at 7.

177 Thaler and Sunstein, n 30, at 8.

178 Thaler and Sunstein, n 30, at 37.

179 A related principle is that "when it comes to things that affect us directly, it seems that many of us dismiss information that suggests that bad things will happen to us, and only pay attention to the good stuff", an unconscious process in our brains determines to show us a rosy glow, see Hertz, n 47, at 34.

180 Thaler and Sunstein, n 30, at 83.

- the more options that are provided, the less likely people are to make a choice. This is not surprising, the more options there are, the more confusing and time-consuming the selection process becomes and people refuse to choose at all.[181]

If these factors are present, providing choice to individuals provides fraught choices, and more or better information will not help.[182] The perfect is here the enemy of the good",[183] more is actually less. People therefore need a "nudge", i.e., the choice architecture for cookies has to be changed, so the default settings can do their work.[184] So instead of providing people with extensive privacy information and opt-ins for 10-20 cookies (which they predictably irrationally will ignore, even if they hate cross-site behavioural targeting), they should be provided with a proper default setting: all cookies that do not present any serious harm to individuals should be accepted by default, and the opt-in right should apply to the targeting cookie only. The decisions on what proper default settings are (i.e. the choice architecture) belong with regulators making policy decisions based on which activities are socially acceptable and which not, rather than 'passing the bucket' to the individuals by granting them meaningless consent rights.[185]

The paradox 'more is less" also applies to the obligations side of data protection. If you impose too many requirements on companies, which create unnecessary administrative burdens without any added value as to material data protection in practice, this is a recipe for non-compliance by companies. Structural non-compliance undermines the legitimacy of the material data processing principles which these norms aim to protect, i.e., "more is less".[186] Such requirements should be avoided at all cost.

7. How to regulate data protection?

What I observe is that the European Commission when drafting the Proposed Regulation has kept the EU system and adopted on top of that the US parts that have proven effective in practice. The Proposed Regulation:

- is still fully rights based. Controllers require a legal basis for each processing, which legal grounds have become stricter in many respects;
- still contains the principle of "purpose limitation";[187]
- broadens and strengthens the information and consent rights of data subjects;[188]
- prohibits certain types of processing, such as being subject to a measure based on profiling solely based on special categories of data; for those types of processing a controller cannot ask consent;[189]

---

[181] Thaler and Sunstein, n 30, at 110. The World Economic Forum Report 2013, n 42, at 11 reports that "The torrent of data being generated from and about data subjects imposes an undue cognitive burden on individual data subjects. Overwhelming them with notices is ultimately disempowering and ineffective in terms of protection – it would take the average person about 250 working hours every year, or about 30 full working days – to actually read the privacy policies of the websites they visit in a year."

[182] Thaler and Sunstein, n 30, at 73. See also Tene and Polonetsky, n 102, at para. 1 and 6.1.

[183] Sunstein, n 57, at 190.

[184] Thaler and Sunstein, n 30, at Chapter 5 'Choice architecture'.

[185] See Tene and Polonetsky, n 102, at paras. 1 and 6.1: "In the context of online privacy, this implies emphasis should be placed less on notice and choice and more on implementing policy decisions with respect to the utility of given business practices and on organizational compliance with fair information principles (FIPs). In other words, the focal point for privacy should shift from users to (a) policymakers or self-regulatory leaders to determine the contours of accepted practices; and (b) businesses to handle information fairly and responsibly."

[186] Moerel, n 84, at 212. That an overly strict approach undermines the credibility of the Directive is acknowledged in Commission of the European Communities, *First Report on the implementation of the Data Protection Directive (95/46/EC),* 15 March 2003, COM/2003/265 final ("**First Report on the Directive**"), at 19: "An overly lax attitude in Some Member States [as to data transfers] (…) risks weakening protection in the EU as a whole, because with the free movement guaranteed by the Directive, data flows are likely to switch to the "least burdensome" point of export. An overly strict approach, on the other hand, would fail to respect the legitimate needs of international trade and the reality of global telecommunications networks and risks creating a gap between law and practice which is damaging for the credibility of the Directive and for Community law in general." A similar observation is made by Christopher Kuner, 'Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 2)', (October 1, 2010), *International Journal of Law and Information Technology*, Vol. 18, 2010. Available at SSRN: http://ssrn.com/abstract=1689495, at 13, noting that "when the jurisdictional scope of the law is much broader than the chance that the law will be enforced, there is a risk that respect for the law will be diminished", and at 15: "a low chance of enforcement may cause controllers to regard data protection rules as a kind of bureaucratic nuisance rather than as 'law' in the same category as tax laws, employment laws, etc."

[187] Article 5(b) Proposed Regulation.

[188] Article 7 Proposed Regulation.

[189] Article 20(1) and (3) Proposed Regulation and article 9 Proposed Regulation on special categories of data. LIBE has added as a prohibition: profiling that has the effect of discriminating against individuals on the bases of race or ethnic

- is still based on the precautionary principle:
    - ex-ante consultation and authorisation requirements for specific more sensitive data processing activities;[190]
    - prescriptive documentation requirements for controllers and processors;[191] and
- codifies the proportionality requirement as a data minimisation principle[192] (controllers are not allowed to collect more data than strictly necessary for the purpose for which they collect the data) and a requirement of "data protection by design".[193]

And on top of that the US extras:

- data security breach notification requirements;[194]
- higher penalties, latest status is 5% of annual worldwide turnover;[195] and
- an "accountability" obligation (i.e., the responsibility of the controller to comply with the Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance).[196]

8. Why these proposals will not work

Assessing these proposals in light of what I presented today, the conclusion is that we are again going to fail.

1. The broadening and strengthening of the "informed consent" requirements will not work. There will be too many choices for individuals to make, which require too much complicated information for individuals to digest, while there are short-term benefits and the costs are long term.

2. The ex-ante prohibition of certain types of processing will not work. The Proposed Regulation provides e.g., that individuals must have the right not to be subject to a measure based on profiling which is based solely on automated processing of 'special categories' of data.[197] It is, however, not possible to foretell why certain processing activities should never be allowed (i.e., the Collingridge dilemma). For example, it is very easy to imagine conditions under which the profiling based on health data would be to the benefit of individuals and society as a whole, e.g., if this is done to detect correlations for behaviour and diseases at a later age.[198] Also, processing of website visitor data and profiling them in order to ensure that children can be recognised and excluded from a site is fine. Processing of children's data to sell them products that are not in their interest is, however, not. Here a balancing of interest has to take place, which, I fully agree, will in most cases weigh in favour of the privacy interests of children.[199]

3. Violation of more is less. If the Proposed Regulation imposes (i) extensive documentation requirements, (ii) ex-ante Data Protection Impact Assessment (DPIA) requirements, (iii) ex-ante requirements to consult and even obtain authorisation of the Data Protection Authority in respect of certain more sensitive data processing operations (precautionary prescribing in

---

origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity (see article 20(3) of the LIBE compromise text). See also CIPL Discussion Document, n 24, at 13.

190 Article 33 Proposed Regulation.

191 Article 28 Proposed Regulation.

192 Article 5(c) Proposed Regulation.

193 Article 23 Proposed Regulation

194 Article 31 and 32 Proposed Regulation.

195 Article 79 Proposed Regulation provides for a fine up to 2% of the annual global turnover, which by LIBE has been increased up to 5%, see for the LIBE compromise text, n 77.

196 Article 22 Proposed Regulation. See also Article 11(1) Proposed Regulation.

197 See n 189.

198 See the following example in the 2013 World Economic Forum Report *Unlocking the Value of personal data: From Collection to Usage*, to be found at http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf WEF Report (2013), at 8: "For example, using a robust database of 3.2 million individuals, Kaiser Permanente addressed the biologic factors linking parental antidepressant drug use to childhood autism spectrum disorders (ASDs). Analysis of data taken from the personal medical records of related family members from 1995 through 2002 showed that children exposed prenatally to their mother's use of antidepressants had more than twice the risk of developing ASDs. The results of the study and this rate of impact may affect the care of children and parents drawn from a total of over 4 million births per year in the US, and over 5 million births per year in EU countries together."

199 See also the WP29 opinion 03/2013 on purpose limitation, adopted on 2 April 2013, WP203 00569/13/EN ("**WP Opinion on Purpose Limitation**"), at 25, footnote 69, where the WP29 indicates that it cannot be excluded that even highly sensitive data may be further processed, provided that the processing meets the criteria for the compatibility assessment, and in particular the reasonable expectations of the data subjects are respected.

detail what companies have to do) and on top of that a general accountability requirement to implement a proper compliance program, this is simply piling up requirements.
I do not dispute that the requirements listed in the Proposed Regulation such as documentation and DPIA requirements should as a rule be part of a data protection compliance program, but I do not recommend specifying these requirements in the Proposed Regulation. The main reason for this is that the requirements are too specific and have as an inherent danger working as a "tick box" list for compliance measures regardless of their actual impact on compliance.[200] It should be left to companies how to best achieve compliance in their organisation, for which they should be accountable. Regulators should not prescribe the "how". Prescribing the "how" creates undue administrative burdens without any added value as to material data protection.[201] As indicated before, this is a recipe for non-compliance which in turn undermines the legitimacy of the material data processing principles which these norms aim to protect (i.e., more is less).

4. The principle of "purpose limitation"[202] and in its wake the concepts of "informed consent" and "data minimisation"[203] are at odds with the reality of big data.[204] "Purpose limitation" consists of two elements: (i) "purpose specification": data may be collected and processed for specified, explicit and legitimate purposes only;[205] and (ii) "compatible use": data may not be further processed in a way incompatible with those original specified purposes.[206] These concepts rely on the old idea that it is possible to decide on the purposes of a certain data processing beforehand (and provide the disclosure necessary for fully informed consent) while the added value of big data resides in the potential to uncover new correlations for new potential uses once the data have been collected.[207] These therefore may have nothing to do with the original purposes for which the data were collected.[208] There may not even have been an original purpose, the data may have been collected just for the sake of potentially discovering later whether there was some purpose for collection in the first place. This is at odds with the concepts of data minimisation, purpose limitation and informed consent. These concepts therefore start from the wrong premise. They are trying to hold off the future, which is impossible to do. It is against the technical imperative. The world will be about big data and the internet of things with sensors collecting data just for the sake of collecting the data, to detect new correlations in order to develop new services. This is not going to go away because there is a principle of purpose limitation,[209] a requirement of informed consent[210] and a data minimisation requirement[211] in the Proposed Regulation. The Google Street View example given earlier is a case in point. The data for Google Street View are not collected in the provision of a service, it is the other way around. The data are collected first in order to deliver the services. If you apply the data minimisation principle and require "informed consent", Google Street View would not have been possible. Google Street View would have required prior consent of all individuals involved (i.e., everybody around the world), which is evidently impossible. This while

---

200 Jaap Winter, 'Geen regels maar best practices', in: *Willems' wegen, Opstellen aangeboden aan prof.mr. J.H.M. Willems*, Kluwer 2010, at 464.

201 Moerel, n 84, at 199.

202 See on the concept of purpose limitation the WP29 in its Opinion on Purpose Limitation, n 199.

203 Article 5(1)(c) and (e) Proposed Regulation. The data minimisation principle seems an alternative manner of expressing the proportionality principle of Article 6(1)(c) Data Protection Directive and seems further to have been implemented in the new obligation of the controller of data protection by design and default as provided in Article 23 Proposed Regulation.

204 See Rubinstein, n 32, at 74: "My contention is that when this advancing [big data tsunami] wave arrives, it will so overwhelm the core privacy principles of informed choice and data minimization on which the [Data Protection Directive] rests that reform efforts will not be enough." Rubinstein's solution is that EU legislators should combine legal reform with the encouragement of new business models premised on consumer empowerment and supported by a personal data ecosystem. See further Hildebrandt, n 5; World Economic Forum Report (2013), n 198; CIPL Discussion Document, n 24, at 11 - 13; Polonetsky and Tene, n 29, at 242 and 259, consider purpose limitation and data minimisation antithetical to big data'.

205 Article 6(1)(b) Directive (compare Article 5(b) Proposed Regulation).

206 See Hildebrandt, n 5, at 16 and World Economic Forum Report (2013), n 198, at 11.

207 See Hildebrandt, n 5, at 17.

208 See Hildebrandt, n 5, at 15.

209 CIPL Discussion Document, n 24, at 13.

210 See on consent also CIPL Discussion Document, n 24, at 11 – 12. Additional issues presented by informed consent are that users of data analytics may not be able to locate individuals to obtain consent, particularly when carrying out longitudinal studies that may span a significant period of time. Consent may further not be appropriate in cases where the analytics supports activities that are recognized to provide broadly accepted public benefits (e.g., scientific or healthcare research). The research may then not be complete and representative. Requiring opt-in or allow opt-out will then compromise the study.

211 CIPL Discussion Document, n 24, at 13.

Google Street View has benefits to offer. Data minimisation and "informed consent" therefore do not work.[212] The grid always wins. Jane Yakowitz even states that as society as a whole can gain from the analysis of aggregated sets of data on health, crime, finances, and other personal characteristics, people have "a civic duty to participate in the public data commons".[213]

It is as The Economist[214] rightfully noted:

> "Managed well, the data can be used to unlock new sources of economic value, provide fresh insights into science and hold governments to account. (...). It has great potential for good—as long as consumers, companies and governments make the right choices about when to restrict the flow of data, and when to encourage it".

9. Suggestions for improvement of the Proposed Regulation

To ensure that companies and governments (as The Economist says) manage the data flows well and make the right choices about when to restrict or encourage the flow and use of data, I propose to delete from the Proposed Regulation the:

- purpose limitation principle;
- data minimisation principle;
- storage minimisation principle;[215]
- prohibition on the processing of the special categories of data unless one of the limitative grounds is available;
- prescriptive documentation requirement;
- right to object to profiling;
- ex-ante consultation and authorisation requirements of the Data Protection Authorities for more sensitive data processing operations.

Instead I suggest:

- **Extending the "legitimate interest ground" to the processing of all categories of data and further to all phases of the life-cycle of data**
  Personal data may be collected, used (which will include profiling), merged, transferred and destroyed if there is a 'legitimate interest of the controller which does not outweigh the privacy rights of the individuals'. This balancing test should be 'harm-based' and further based on a cost-benefit analysis, where data protection risks are balanced against potential benefits for individuals, companies and society as a whole.[216] This balancing test would (as

---

[212] See also the World Economic Forum Report (2013), n 198, at 17: that identifies as a candidate for reconsideration the notion of 'notice and consent': "In particular, reliance on mechanisms of "notice and consent" to ensure individual participation is seen as increasingly anachronistic. The current manifestation of the principles through notice and consent as a binary, one-time only involvement of the individual at the point of data collection was identified in the dialogue as an area ripe for reconsideration to better empower individuals, build trust in the system, and encourage the reliable, predictable and more valuable flow of data into and within the system."

[213] Carr, n 1, at 242.

[214] See n 22.

[215] See article 5(e) LIBE compromise text.

[216] Polonetsky and Tene, n 32, are also of the opinion that the rewards of big data must be taken into account when deciding on the legitimacy of a data processing. See at 26, where they indicate that the "current privacy debate methodologically explores the risks presented by big data, [but that] it fails to untangle commensurate benefits (...) Yet accounting for costs is only part of a balanced value equation. In order to complete a cost-benefit analysis, privacy professionals need to have at their disposal tools to assess, prioritize, and to the extent possible, quantify a project's rewards big data the currently the positive". Polonetsky and Tene note that this fits in neatly with both the 'legitimate interests of the controller' in the Directive and further with the powers of the authority of the FTC to prohibit 'unfair trade practices', which is defined as a 'practice that causes or is likely to cause substantial injury to consumers which is not easily avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition.' (see 15 U.S.C. par. 45(n)). See also Tene and Polonetsky, n 29, at 244. See also Ann Cavoukian, *Privacy by Design: The Seven Foundational Principles*, Info. Privacy Commissioner, Ontario, Canada (Jan. 2011), to be found at http://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf. See the fourth principle: "Full functionality – Positive-Sum, not Zero-Sum: Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum 'win-win' manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made.' The WP29 in its Opinion on purpose limitation, n 199, has also given an opening for allowing big data analytics based on the positive effects on individuals or society. See at 3, where the WP29 states that further processing for a different purpose does not necessarily mean that it is incompatible with the original purpose: compatibility needs to be assessed on a case-by-case basis which requires an assessment of all relevant circumstances and in particular assessment of the following key factors:

is the case now) include a proportionality test.[217] Proportionality will entail that each phase needs to comply with 'protection by design and default' requirements'.[218] The result of this balancing test may be different for each of the phases.[219] For example, for analytics purposes perhaps more data and more types of data may be collected and used (i.e., data minimisation does then not necessarily apply).[220] However, data protection by design and default may entail that the data are pseudonimised at the point of collection, with the key locked away, so the impact of the analytics on individuals is minimised if not eliminated completely.[221] As the 'deployment phase' is concerned, this may entail that results of the analytics may not subsequently be used to take decisions if these have a material detrimental effect on individuals. However, if the effects are negligible, neutral or positive for individuals, or any negative impact on individuals is outweighed by the benefits to society as a whole, the balancing test may go the other way.[222]

Each of the phases of the data lifecycle will further have to be evaluated in context. Context will depend on:

- the role of the data controller (is it your doctor or Facebook or the NSA);
- the manner of collection (was the data shared by the data subject, observed by the controller, obtained from a third party or inferred by analytics?);
- the type of data (are the data heath data, WhatsApp messages or surfing behaviour data);
- the purpose of the processing (is it used for improving your health, preventing terrorist attacks, or for advertising?);
- the channel of collection (were the data collected via a mobile device, online or in a face-to-face conversation); and

---

- the relationship between the purposes for which the personal data have been collected and the purposes of further processing;
- the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use;
- the nature of the personal data and the impact of the further processing on the data subjects;
- the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.

See further at 25, where the WP29 indicates that for assessing the impact on the further processing both positive and negative consequences should be taken into account. See further Annex 4, examples 6 and 11, where the WP29 takes into account the positive impact on individuals for the assessment of compatibility. The WP29 subsequently advises to delete article 6(4) Proposed Regulation as this gives a too broad basis for further processing, which is indeed deleted in the LIBE compromise text.

[217] Siegel, n 5, at 43 discusses these requirements from the perspective of predictive analytics and comes to the following: "Each organisation must decide data's who, what, where, when, how long, and why:
Retain – What is stored for how long.
Access – Which employees, types of personnel, or group members may retrieve and look at which data elements
Share – What data may be disseminated to which parties within the organisation and to what external organisations
Merge – What data elements may be brought together, aggregated, or connected
React – How may each data element be acted upon, determining an organisation's response, outreach, or other behaviour.
To make everything even more complicated, add to each of these items "...under which circumstances and for what type of intention or purpose."

[218] See also article 23(1) LIBE compromise text, n 77.

[219] Tene and Polonetsky, n 29, at 257, propose in fact a similar flexible system, but propose to use the (in their case US Fair Information Practices Principles (FIPPs) as a 'set of levers which can be modulated to address big data by relaxing the principles of data minimisation and individual control while tightening requirements for transparency, access and accuracy.' See at 260, where e.g. measures to minimise the risk of de-identification of data are then an important accountability measure (which may count towards mitigation of the requirement of data minimisation). At 242 – 243 and 270 -272, the authors suggest that mitigating levers for allowing big data are a combination of (i) providing individuals with meaningful access to their data in a usable, machine-readable format (as this will stimulate user-side applications which will enable individuals to share in the gains of big data); (ii) requiring companies to disclose the logic underlying their decision-making processes. At 262 – 263, the authors indicate that requesting consent should not be used as the main basis for legitimising all instances of data use. Depending of the type of use and the benefits, the role of consent should vary from not required to assumed, but subject to a right of refusal, and for specific cases consent should be required to legitimise use.

[220] CIPL Discussion Document, n 24, at 14.

[221] See on the issue that even if identifyers are removed from data sets in order to create anonymised data, often individuals can still be re-indentified by cross-referencing these anonymised data sets with related sets of data in the public domain that includes identifyers. See Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', (2010) 57 *UCLA Law Review*, at 1716 – 1731, discussing inter alia the relative ease with which de-identified search queries of users of the AOL's search engine were re-identified, see for the press release exposing certain individual users: Michael Barbaro and Tom Zeller, 'A Face Is Exposed for AOL Searcher No. 4417749', *N.Y. TIMES* Aug. 9, 2006, at A1 and Rubinstein, n 32, at 78.

[222] See n 216 for the references which indicate that also the benefits of big data should be taken into account when making the balancing test.

- was there any value exchange between controller and individual (did the individual get free services or was there no value in the processing for the individual or is the processing only in the commercial interest of the controller).[223]

This should not be taken to mean that a data minimisation requirement will never apply. Depending on the context,a data minimisation requirement may apply to the collection of data (e.g. in case of a face-to-face consult with your psychiatrist), but not always.[224] This should also no be taken to mean that consent as a legal ground for data processing no longer has a role to play. Instead it means that requesting consent should not be used as the main basis for legitimising all instances of data use.[225] Depending on the outcome of the balancing test per phase, mitigating measures may entail that consent is not required or that a right to opt-out will suffice. Example here is the collecting of data by means of cookies. For example, collection of data by cookies for purposes of website analytics, fraud prevention, legal compliance, first party marketing on the site that is visited, should pass the legitimacy test. The outcome of the legitimate interest test will, however, probably be that consent should be required for cross-site behavioural targeting.

Norm setting in respect of how the legitimate interest ground should be applied should be with EU legislators. It should be regulators making policy decisions based on which activities are socially acceptable and which not, rather than (as indicated before) 'passing the bucket' to the individuals by granting them meaningless consent rights.[226] Given the quick pace of the online developments, these decisions should not be regulated in EU legislation (as is done now for cookies). More detailed norm-setting can and should be delegated to the European Commission in accordance with recently introduced Articles 290[227] and 291 TFEU[228] in order to ensure that these remain more adaptable to changing circumstances and insights.[229] This is not a new insight, but has also been the trend in other areas of law, like company and financial markets law.[230] The role of the WP29 (as it has been in the past) will be to give further detailed guidance to companies on how the legitimate interest ground should be applied to the different types of collection and use.[231]

- **Transparency requirement for choices made and meaningful access**
Companies should have an obligation to make their choices in respect of each of the phases of the life-cycle of data transparent[232] (including the fact that automatic decision-making

---

[223] World Economic Forum Report (2013), n 198, at 11.

[224] I therefore am not in favour of moving from 'collection to usage' requirements only, as seems to be advocated in the World Economic Forum Report (2013), n 198, at 12.

[225] Currently consent is a key legal ground (and in some Member States the preferred legal ground) under article 7 of the Directive. See Article 29 Working Party, Opinion 15/2011 on the Definition of Consent, 13 July 2011, at 7. Tene and Polonetsky, n 29, at 260 indicate that in the US "notice and consent" has been the central axis of privacy regulation for more than a decade, but that a shift away is underway, as reflected in the Consumer Privacy Bill of Rights (see n 109) and the Federal Trade Commission Report, P*rotecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), to be found at http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[226] See n 185.

[227] Article 290(1) TFEU provides that EU legislative acts may "delegate to the Commission the power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of the legislative act" (i.e. 'delegated acts').

[228] Article 291(2) TFEU provides that EU legislative acts may “confer implementing powers on the Commission”, “where uniform conditions for implementing legally binding Union acts are needed” (i.e. 'implementing acts').

[229] The European Data Protection Supervisor in its Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - “A comprehensive approach on personal data protection in the European Union”, at paras. 106 and 114, recommends to delegate specific tasks to the European Commission in order to supplement the basic criteria on for instance accountability, privacy by design etc.

[230] See Moerel, n 84, at at 177, under reference to *The Report of the High Level Group of Company Law Experts on a Modern Regulatory Framework for Company Law in Europe*, Brussels, 4 November 2002, to be found at <http://ec.europa.eu/internal_market/company/modern/index_en.htm>, at para. 2:
“We noted that the system of harmonising company law through Directives – that have to be implemented by Member states – may have led to a certain “petrifaction”. Once Member States have agreed to an approach in an area of company law and have implemented a Directive accordingly, it becomes very hard to change the Directive and the underlying approach. Simultaneously however, there is a growing need to continuously adapt existing rules in view of rapidly changing circumstances and views (...) Secondary regulation by the government, based on primary legislation in which broad objectives and principles are laid down; the secondary regulation can be amended more quickly when circumstances require change. (This process also often enables more effective consultation and reflection of an expert consensus).”

[231] As the WP29 already did in its Opinion on the concept of purpose limitation, n 199.

[232] See Hildebrandt, n 5, at 21 for a similar suggestion, but from a different perspective, discussing the question what information and choices should be in the limelight and which should be in the darkness, as the current informed consent requirements create an information "buffer overflow".

takes place and any logic underlying such decision-making).[233] In general, the transparency principle is a good guideline for constraining and implementing choices of companies and governments.[234] When companies have to reveal their methods and motives this mostly leads to a policy that a company is able and willing to defend publicly. The idea here is that "sunlight is the best of disinfectants".[235] These general transparency requirements should be accompanied by a 'meaningful' right of access.[236] Meaningful is not the general right of access individuals have under the Directive, but a right of access to their data built into the relevant online platform by design. For example, by including a profile settings dashboard on a social media website where the relevant profile characteristics are displayed and can be tailored by the individual.[237] Another example is the insertion of icons in advertising where the profile characteristics are displayed which triggered the advertising, which can be tailored by the individual.[238]

- **Accountability for the whole life cycle of data**
  The accountability principle should explicitly extend to all phases of the data life-cycle. Controllers should be accountable for implementation of an internal data protection compliance program ensuring that the choices made are actually implemented in the practices of the company. Therefore, no prescribed documentation and ex-ante consultation and authorization requirements should be imposed.[239]

- **Technology Impact Assessments rather than a Data Protection Impact Assessment**
  Part of the accountability obligation is to perform a Data Protection Impact Assessment[240] when implementing new data processing operations.[241] I propose to extend this obligation to performing a more encompassing **Technology** Impact Assessment. Research shows that if you wish to navigate the Collingridge dilemma, you need to address the impact of new technology in the design stage, not by prescribing the outcome but by requiring companies and governments, who implement a new technology, to evaluate the data protection aspects as part of the design/planning stage (data protection by design and default), e.g. by means of a Data Protection Impact Assessment.[242] However, as the future technology will not only present data protection issues, but also numerous ethical issues that are currently less visible and for which we do not yet have good answers, companies and governments should also address any ethical dilemmas expected to be presented by the relevant new technology (ethics by design).[243] They will further have to implement a "good choice architecture" according to principles of behavioural sciences. In other words, companies and

---

233 Article 12(a) Directive / 15(1)(ha) LIBE compromise text, n 77, grant the data subject the right to obtain knowledge of the logic involved in any automated decisions concerning him. This requires however that the individual is first aware of the fact that automatic decision making has taken place. This is remedied in the LIBE compromised text, new article 20(1) prescribing that the data subject shall be informed about the right to object to profiling (and thus the profiling itself) in a highly visible manner. See on this topic Hildebrandt, n 90, at para. 4.3; and Rubinstein, n 32, at 79.

234 Thaler and Sunstein, n 30, at 245.

235 This quote is attributed to US Supreme Court Justice Louis Brandeis, see Sunstein, n 57, at 174.

236 See also Mireille Hildebrandt, 'Who is Profiling Who? Invisible Visibility', in S. Gutwirth et al. (eds), *Reinventing Data Protection?*, Springer 2009, at 249, who recommends an effective right of access to profiles that match with one's data and are used to categorise one, including the consequences this may have. See further Tene and Polonetsky, n 29, at 242 – 243 and 270 -272, who suggest providing individuals with meaningful access to their data in a usable, machine-readable format. This will stimulate user-side applications which will enable individuals to share in the gains of big data. To minimise profiling concerns companies should further disclose the logic underlying their decision-making processes.

237 See for instance the privacy settings dashboard at Facebook.

238 See for instance the Interactive Advertising Bureau (IAB) *Self-Regulatory Program for Online Behavioral Advertising*, July 2009, advocating 'enhanced notice' to consumers achieved by placing a special icon on or near targeted ads, to be found at http://www.iab.net/media/file/ven-principles-07-01-09.pdf,

239 The amendments adopted by LIBE, n 77, seem to be on a similar basis. LIBE deleted article 22(2) which prescribed certain accountability measures; included a new article 23 "Data protection by Design and Default", providing for an obligation to apply principles of data protection by design and default to all phases of the life cycle of data; deleted the specific documentation requirements (see amendments article 28); deleted the ex-ante consultation and authorisation requirement of the DPA of the Data Protection Impact Assessment to be performed for more sensitive processing activities (which can now be addressed by the data protection officer); and extended the Data Protection Impact Assessment requirement to the whole life cycle of the data (new article 33).

240 See for the history and definition of Privacy Impact Assessments: Roger Clarke, 'Privacy Impact Assessment: Its Origins and Development', *Computer Law & Security Review* 25, 2 (April 2009) 123-135: "Privacy impact assessment (PIA) is a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme", to be found at http://www.rogerclarke.com/DV/PIAHist-08.html.

241 The amendments adopted by LIBE n 77, also envisage a broad scope of DPIA, see new article 33, which requires controllers to perform an assessment of the "impact on the rights and freedoms of the data subject, including the risk of discrimination being embedded in or reinforced by the intended data processing operation (see new article 33(3)(c))."

242 EC Report on Responsible Research, n 1, at 112, 208.

243 EC Report on Responsible Research, n 1, at 12 and 30.

governments need to be able to do a proper Technology Impact Assessment.[244] This requires lawyers to broaden their horizons and get acquainted with many new concepts such as "surprise minimisation",[245] "responsible research and innovation",[246] "creepiness threshold"[247] and "good data stewardship".[248] Personally I am looking forward to it.

Closing words

I am at the end of this lecture and at the beginning of an academic career. My gratitude is to the Executive Board of the University, the Board of the Faculty, the Rector Magnificus Philip Eijlander and in particular the Dean of the Law Faculty Corien Prins, for having the foresight to establish a chair Global ICT Law and for your trust in me and charging me with this task. . If I strived to make anything clear today is that we are at the eve of a data revolution that will utterly change society as we know it now. Any law attempting to regulate these new technologies has to operate in context and in a global environment that is ever changing. To regulate requires 'understanding society' in the broadest sense: the technologies, the new business models and changing economic trade-offs, the impact on individuals, how individuals will react and behave, consequences for society at large, new ethical dilemmas', renewed balancing of human rights issues, and regulatory governance and this all in a global environment. If ever a topic fits Tilburg University's motto 'Understanding Society' and its interdisciplinary approach to research and teaching, it is this chair Global ICT Law. Being a practitioner and assisting multinationals in their global implementation of ict's, data compliance, new business and big data solutions, the concept of 'global law in context' is a given. To be able to pursue my academic interests on a similar footing is more than I could have asked for.

My mentor! Corien, a special word for you as you are the first person in my life who I consider a mentor. You breathe Tilburg's motto Understanding Society and begin with the people around you, which is a great place to start. You have adopted the interdisciplinary and global law approach from the outset of your career, which has given TILT a head start, which others find hard to catch up with. Unnecessary to say I am delighted to become your colleague.

My students! I can say that as *digital natives* you embody the age of big data and participate in the gift economy without a second thought. In that sense I learn as much from you as I hope you will learn from me. I use and will continue to use you as guinea pigs to test new apps, hypothesis and assumptions and let you explain how new business-models work, and are looked upon. I look forward to the many practical research projects I am sure we are going to undertake jointly with the many innovative multinationals surrounding Tilburg University.

My firm has my gratitude for being the firm it is: an environment of learning and excellence where having a broader view than your area of expertise and the law is encouraged and appreciated. I find it hard to imagine being where I am today if I had not joined De Brauw. Special thanks for Stephen, who as always has edited my English and teaches me along the way and Mieke for assisting me with the publication.

My dad, I am so glad you made it here today. My mum and Marguerite, without you two the children would not be turning out as fine as they are, for what can I be more thankful?

My children, Julius, August and Fien. What can I say? I am so proud of all three of you, growing up like you do and each standing your ground and fighting your battles in your own special way. I am so glad to be your mum!

---

[244] EC Report on Responsible Research, n 1, at 9 for the conclusion that responsible research and innovation requires a broader technology assessment. Polonetsky and Tene, n 32, at 30 – 31, signal that these decisions transcend data protection law and that deciding on the balancing of various social values and interests should not be left to data protection regulators alone, as these 'would become the de facto regulators of all things commerce, research, security, and speech' and would 'have as a perverse result that given even constitutes a fundamental right, it is not an '*über-value*', that trumps every other social consideration.' This is undoubtedly correct, but lacking credible alternatives, currently data protection regulators seem to be best positioned to make such decisions.

[245] See for the first mentioning of this concept the 35th Annual Privacy Commissioners' Conference: *DPAs Resolutions, Warsaw declaration on the "appification" of society*, to be found at https://privacyconference2013.org/web/pageFiles/kcfinder/files/ATT29312.pdf.

[246] EC Report on Responsible Research, n 1, at 72.

[247] See Tene and Polonetsky, n 29, at 253, see for the origin of the term, their footnote 79.

[248] See for example the "Data Stewardship Principles" of Intuit Inc, an online financial service provider, to be found at http://security.intuit.com/privacy/data-stewardship.html.

My husband, Jaap, where shall I start? Never a dull moment, that is for sure. I am glad we are this task-force of two to tackle these three kids and having fun and a continuing conversation along the way.

I have spoken.