Articles

Some Reflections on Dignity as an Alternative Legal Concept in Data Protection Regulation

By Anne de Hingh[*]

Abstract

As the use of the Internet and online platforms grows, the scale of collecting and processing personal data and turnovers have increased correspondingly.[1] At the same time, public awareness about the Internet turning into a genuine profiling and advertisement machine, as well as a powerful surveillance instrument, grows. More people today are concerned about the ways in which public and private actors store and use private information. Many individuals note that they lose sight of the consequences once they give consent to the collection of their sometimes most intimate personal data. The Snowden revelations and the recent Facebook and Cambridge Analytica scandal have only reinforced this public awareness.

Objections against these data processing practices cannot be explained as breaches of data protection or privacy regulation alone. In this Article, it is argued that recently passed regulations fail to solve the unease of data subjects as other, more fundamental values are at stake here. A different or complementary ethical and legal framework is needed to interpret this generally felt unease vis-à-vis current data practices and secondly to confront future developments on the data market. The concept of human dignity may be a helpful perspective in this respect. In the context of data processing, human dignity is generally interpreted in a quite specific manner, such as contributing to the empowerment and self-determination of autonomous individuals. It can be argued, however, that human dignity—in the context of the commodification and commoditization of online personal data—should be seen in a different, quite opposite, light. In sum, future regulation of privacy and data protection attention should shift towards more constraining dimensions of human dignity.

[*] Assistant Professor of Internet Law, Department of Transnational Legal Studies, Faculty of Law, VU University Amsterdam. E-mail: a.e.de.hingh@vu.nl. The author would like to thank Els De Busser, Ester Herlin Karnell, Galina Cornelisse, Tina van der Linden, and Arno Lodder for their valuable comments.

[1] The growth of the Dutch internet use is reflected in the results of a recent survey: of the 17 million Dutch citizens, 11.5 million use Whatsapp, 10.8 million are on Facebook, 8 million use YouTube, 4.4 million are members of LinkedIn, and 4.1 million people in the Netherlands use Instagram. *See* NEWCOM, NATIONALE SOCIAL MEDIA ONDERZOEK (Jan. 29, 2018), https://www.newcom.nl/socialmedia2018.

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

A. Introduction

Personal data[2] developed from the by-products of computing to the main resources and commodities of online activities.[3] Digital technologies have made it possible to expose, produce, isolate, aggregate, process, analyze, buy and sell, exploit, transfer, and circulate large amounts of data on individual human beings. Data have grown out to be an inexhaustible source of income and power for both private parties—technology companies, online platforms and social media, the advertisement industry and data brokers—and public parties—public administrations, law enforcement agencies and intelligence services. These actors constantly harvest personal data from individual human beings for their own specific purposes: Be it financial gain, political goals or purely governmental purposes like fighting crime and preventing terrorism. This had led up to what is welcomed by some as the new economy of today.[4] Others have criticized this development as a major threat to online privacy, data hunger, a new religion ("dataïsm")[5], big data surveillance,[6] data capitalism,[7] or surveillance capitalism.[8]

The collection, analysis, and trade of online personal data, and the roles of information technology companies and government in this market are highly debated issues. Serious public concerns on these matters grow only with each new revelation, like the 2018 uproar over Cambridge Analytica's massive abuse of Facebook data for political micro targeting. These concerns relate to the disturbing idea that there is a genuine market wholly

[2] "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *See* Art. 4(1) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing the General Data Protection Regulation, Directive 95/46/EC, 2016 O.J. (L119) [hereinafter GDPR].

[3] *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD (2015).

[4] *See* VIKTOR MAYER-SCHÖNBERGER & THOMAS RAMGE, REINVENTING CAPITALISM IN THE AGE OF BIG DATA (2018).

[5] YUVAL NOAH HARARI, HOMO DEUS: A BRIEF HISTORY OF TOMORROW (2015); STEVE LOHR, DATA-ISM: THE REVOLUTION TRANSFORMING DECISION MAKING, CONSUMER BEHAVIOR, AND ALMOST EVERYTHING ELSE (2015).

[6] *See* Surveillance Studies Centre at Queen's University, *The Big Data Surveillance Project*, SURVEILLANCE STUD. CENTRE, http://www.sscqueens.org/projects/big-data-surveillance.

[7] Evgeny Morozov, *Digital Technologies and the Future of Datacapitalism*, SOC. EUR., (Jun. 23, 2015), https://www.socialeurope.eu/digital-technologies-and-the-future-of-data-capitalism.

[8] *See* Shoshana Zuboff, *The Secrets of Surveillance Capitalism*, FRANKFURTER ALLGEMEINE ZEITUNG (Mar. 5, 2016), www.shoshanazuboff.com.

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

dependent upon the trade in personal data, that this market is expanding on a great scale and that it is developing into highly undesirable directions. Personal data that are collected primarily for economic gain are subsequently transferred into other contexts and exploited for other purposes such as for political targeting or surveillance. Thus, data is constantly circulating between contexts or "silos." In this way, personal data is not only commercialized and commodified for their monetary value, but also commoditized as generic mass products.

There are, in my view, good grounds to consider specific developments of data practices as contrary to human dignity. In this Article, I will tentatively explore how the concept of human dignity can be incorporated in the debate on data, specifically big data. Elaborating further on Opinion 4/2015 of the European Data Protection Supervisor, some provisional reflections are presented on how dignity could play a constraining role—not only in the debate on, but also in the regulation of commercialization, commodification and commoditization of personal data.

Two parallel cases illustrate in what ways and to what extent this data ecosystem has developed. First, the recent revelations on the transfer of data from Facebook to Cambridge Analytica prior to the US presidential elections demonstrated the unexpected shape the resale of personal data can take. In this case, the accounts of up to eighty-seven million Facebook users were harvested, analyzed and used to shape voter targeting and messaging for the Republican presidential campaign.[9] Another Dutch example illustrates how the practices of collecting data can take up quite questionable forms. At the end of 2017, it was reported that the Joint Sigint Cyber Unit of the Dutch Intelligence and Security Services—AIVD and MIVD—had in previous years purchased large bulk sets of personal information from illegal origin. These data were stolen, hacked, or leaked and later sold by third parties on the online black market. Each of these datasets comprised names, email addresses, and passwords of more than a hundred million individuals who were not and will not be a direct target of the services.[10]

The cases presented here are just two of many examples revealing the scale by which personal data are treated as tradable goods. In addition, these examples demonstrate the ease with which data circulate and are transferred back and forth between separate parties for different purposes. Often, this takes place without the knowledge—let alone the

[9] Cambridge Analytica approached Facebook users through the Amazon Mechanical Turk platform (mturk.com) and paid them one to two dollars to download and use a personality quiz app (thisismydigitallife). The quiz "scraped" the information from the profiles of 320,000 Facebook users as well as detailed information from the profiles of their friends. *See* Zeynep Tufekci, *Facebook's Surveillance Machine*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html.

[10] The Dutch oversight committee (CTIVD) concluded that one of the data sets was obtained unlawfully, such as without permission of the Minister of Interior Affairs. *See* CTIVD, *Toezichtsrapport nr 55, Over Het Verwerven Van Door Derden Op Internet Aangeboden Bulkdatasets Door de AIVD en de MIVD* (2017), https://www.ctivd.nl/documenten/rapporten/2018/02/13/index.

consent—of the data subjects concerned. Evidently, the boundaries between public and private and between legitimate and illegally obtained data sets are blurring and breaking down.[11]

This paper distinguishes two objections. The first one relates to the process of resourcification, the commodification of personal data, and to the observation that non-saleable things at one point in time became saleable. This Article argues that individuals should not be treated simply as resources of data that can be bought and sold on markets.[12] Selling data for money, I argue, is incompatible with the principle of non-commercialization of parts of the person, even if this person is voluntarily handing over her or his data. It can be defended that, for this reason, personal information should be more fundamentally protected than by data protection regulation alone.

A second objection emerges from the fact that personal data is moved back and forth, thus circulating between different realms or silos that were previously delimited. The blurring of the boundaries between the private and the public and between the legal and the criminal realms—or de-siloization—concurs with an endless recycling of information. In this process, personal data are not merely resourcified or commodified but also "commoditized." Commoditization in this context involves personal information turning into a generic bulk product. As a consequence, its original proper features lose their significance.[13] This development is reflected in the recent May 2017 Europol Regulation which does not focus on separate databases anymore, but on data processing operations.[14]

These and similar big data practices add fuel to the fire of public awareness and uneasiness because they only give a glimpse of the complexity and scale of big data exploitation in current business and surveillance models. Data exploitation "by its very nature has an underestimated impact on the ability of data subjects to understand its consequences and possible harms, and to make informed decisions."[15] Concerns accrue with every year the Internet grows older. On March 12, 2018, the twenty-ninth birthday of the Internet, Sir Tim

[11] *See, e.g.*, Fanny Coudert, *The Europol Regulation and Purpose Limitation: from the 'silo-based approach' to . . . what exactly?*, 3 EDPL 313–24 (2017); N. Purtova, *Between the GDPR and the Police Directive: navigating through the maze of information sharing in public-private partnerships*, 8 IDPL 1, 1–3 (2018).

[12] Beate Roessler, *Should Personal Data be a Tradable Good? On the Moral Limits of Markets in Privacy, in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 141–61 (Beate Roessler & Dorota Mokrosinska eds., 2015); MICHAEL J. SANDEL, WHAT MONEY CAN'T BUY: THE MORAL LIMITS OF MARKETS (2012).

[13] MARTIN GUNNARSON & FREDRIK SVENAEUS, THE BODY AS GIFT, RESOURCE, AND COMMODITY: EXCHANGING ORGANS, TISSUES, AND CELLS IN THE 21ST CENTURY, 9–30 (Martin Gunnarson & Fredrik Svenaeus eds., 2012).

[14] Coudert, *supra* note 11, at 313.

[15] *See* Andrej Zwitter, *Big Data Ethics*, BIG DATA & SOC., 1, 1–2 (2014) ("[T]he very nature of Big Data has an underestimated impact on the individual's ability to understand its potential and make informed decisions.").

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

Berners-Lee, the inventor of the world wide web as we know it, expressed his worries on the concentration of power of a few dominant platforms. In the year before, he had described the loss of control over our personal data as a major threat to the Internet of today.[16]

In short, the exploitation of data seems to put current privacy and data protection regulation under so much stress as to raise serious questions about the effectiveness of these regulations. It can be argued that this is not exclusively about market power and information asymmetry caused by the fact that individual users do not exactly know what it is that they give consent to. After all, even if users were aware of the consequences of their consent, they would likely continue to feel uncomfortable knowing someone has access to their personal information.[17]

Various surveys empirically support the notion that people are discomforted by large social platforms. A recent American poll found that the trust in all three of the major social media companies—Facebook, Twitter, and Google—is rapidly decreasing as mistrust is focused on the companies themselves, not on their technology.[18] Comparable outcomes of a recent Dutch social media survey illustrated that concerns regarding personal data are growing because only one fifth of the users feel they still trust social media—66% of the respondents are especially worried about the subsequent sale of their personal data.[19] A KPMG survey among 7,000 online consumers in twenty-four countries revealed that less than ten percent of the respondents find they have adequate control over the collection and exploitation of their personal data.[20] Respondents are especially worried about their personal data being sold to third parties, and indicate that they prefer a larger control over their personal information at the cost of other possible benefits of online shopping, like speed and convenience.

What legal or ethical interpretation should be given to this nagging unease on the large-scale collection and processing of personal data by companies and governments? It can be argued that the problem of personal data of individuals being exploited both as sources of profit and as continually circulating recycled mass products, protrudes the frame of data

[16] Tim Berners-Lee, *The Web Can Be Weaponised – and We Can't Count on Big Tech to Stop it*, GUARDIAN (Mar. 12, 2018), https://www.theguardian.com/commentisfree/2018/mar/12/tim-berners-lee-web-weapon-regulation-open-letter.

[17] FREDERIK J. ZUIDERVEEN BORGESIUS, IMPROVING PRIVACY PROTECTION IN THE AREA OF BEHAVIOURAL TARGETING 187 (2015).

[18] *See* Kim Hart & Ina Fried, *Exclusive Poll: Facebook Favourability Plunges*, AXIOS (Mar. 26, 2018), https://www.axios.com/exclusive-poll-facebook-favorability-plunges-1522057235-b1fa31db-e646-4413-a273-95d3387da4f2.html.

[19] *See* NEWCOM, *supra* note 1.

[20] *See* KPMG, CROSSING THE LINE: STAYING ON THE RIGHT SIDE OF CONSUMER PRIVACY (2017), https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/11/crossing-the-line.pdf.

protection and privacy issues and touches upon the more fundamental question of what it means to be human. At the same time, it is hard to articulate what exactly the objections against these practices entail. Moreover, it is difficult to translate these ethical arguments into practical, legal ones, as our "data-protection centered vocabulary" might be inadequate for this.

A common explanation would be that massive data collection and processing by both public and private parties could entail an infringement of privacy or might stretch the limits of data protection principles. My position argues that principles of data protection regulation, like consent and purpose limitation, have lost much of their original usefulness. The General Data Protection Regulation (GDPR) that became effective on May 25, 2018, would be the designated legal tool in this respect. The GDPR, however, fails to offer adequate answers to the growing unease among European citizens because it does not appear to be tailored to the digital reality of today.[21] Many assume that autonomy, empowerment and self-determination are central to data protection; however, these principles seem insufficient to understand and address the ethical challenges brought about by recent digital technological developments.

This Article explores in what ways the concept of human dignity—especially through its constraining dimension—could contribute to an alternative legal framework that would set limits to certain data practices. It is structured as follows. Section B discusses Opinion 4/2015 of the European Data Protection Supervisor, the EU's independent data protection authority (EDPS), which is one of the early publications on data and dignity. In this opinion human dignity was interpreted in a very specific and narrow manner that is focused on the empowerment and self-determination of autonomous individuals; therefore, it still heavily relies on data protection principles. Section C elaborates on the thesis that the GDPR, as a regulatory instrument, and the principles of data protection alone do not suffice to cater for these generally felt sentiments of concern and unease with regard to the radical commodification and commoditization of personal data. The two cases mentioned above illustrate this point. In Section D, the possibility to approach these developments from an alternative angle is explored and the recently published report of the Ethics Advisory Group (EAG) of the EDPS is discussed. This report is the next step in the project to introduce ethics and especially the concept of human dignity into the debate on the regulation of big data. In the EAG-report, it is implicitly suggested that the interpretation of human dignity "as constraint" should have a central role in any alternative regulation of data, which is the central theme in this section.

B. The EDPS on Data and Dignity

[21] Regulation 2016/679, of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and Repealing Council Directive 95/46/EC, 2016 O.J. (L119).

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

The concerns with regard to data processing that are highlighted above, evidently are not new but have been a common theme in academic legal literature and semi-scientific publications for quite some time now.[22] One of the contributions to the debate was published by the EDPS. His Opinion 4/2015, titled "Towards a new digital ethics. Data, dignity and technology" appeared in September 2015 when the legislative procedure of the adoption of the GDPR was still under way.[23] The EDPS suggested in the Opinion that taking a radically new approach was indispensable for the development of a more future-oriented regulation of the European data market in light of technological trends like the Internet of Things and the rise of artificial intelligence. According to the EDPS-publication, data market trends raise important ethical and practical questions for the application of data protection principles. The Opinion argues data protection principles, therefore, are aimed at exploring different routes to customize existing data protection principles to fit the global digital arena. The major trends identified, were the large scale of data collection, its ubiquity and power, the often intimate nature of the data in question, and the fact that processing takes place in increasingly opaque and complex ways.[24]

Clearly, a sense of urgency arose from Opinion 4/2015—as if it aimed at raising awareness of the fact that certain data protection principles had lost their impact altogether. In addition, new ethical and legal perspectives were now indispensable to solve current issues of privacy and data protection. It therefore proposed to explore an innovative approach by formulating a new ethical framework in which "better respect for, and the safeguarding of, human dignity could be the counterweight to the pervasive surveillance and asymmetry of power" in the data market.[25] Human dignity "should be at the heart of a new digital ethics," according to the EDPS.[26]

The choice for dignity as a starting point could be seen against the background of human rights protection in Union law in which the inviolability of human dignity plays a pivotal role.[27] The EU Charter emphasizes dignity of a human not only is a fundamental right in itself but constitutes the foundation of fundamental rights, including the rights to privacy and to

[22] *See* NICHOLAS CARR, THE GLASS CAGE: AUTOMATION AND US (2014); SCHNEIER, *supra* note 3; HANS SCHNITZLER, HET DIGITALE PROLETARIAAT (2015); HARARI *supra* note 5; FRANKLIN FOER, WORLD WITHOUT MIND (2017).

[23] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2015 Towards A New Digital Ethics: Data, Dignity and Technology* (2015), https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf.

[24] *Id.* at 6.

[25] *Id.* at 12.

[26] *Id.*

[27] Charter of Fundamental Rights of the European Union, art. 1 (recognizing human dignity as an inviolable right that must be respected and protected).

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

the protection of personal data.[28] Human dignity and data protection law are, evidently, not by definition mutually exclusive and the concept of dignity is, in the words of Floridi, almost "invisibly" present in the GDPR.[29] More specifically, Article 88 of the GDPR prescribes Member States to provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of personal data in the employment context. Article 88 further states that these rules shall include suitable and specific measures "to safeguard the data subject's human dignity, legitimate interests and fundamental rights . . . ."[30] As pointed out by Floridi, it can be deduced from the phrasing of this Article that human dignity is different from "legitimate interests and fundamental rights." According to him, this is indicative of the fact that human dignity is the fundamental concept that provides the framework within which one needs to interpret what the GDPR understands by informational privacy.[31] One might consider designating human dignity as an extra layer that results in a right to privacy 2.0.

As part of the Digital Ethics project, an Ethics Advisory Group (EAG) was invited to consider wider ethical implications of the current personal data use—see also Section D of this Article.[32] Anticipating the outcomes of the deliberations by this EAG, however, the opinion offered a specific interpretation of the concept of human dignity. The opinion interpreted human dignity in the context of personal data processing which appeared to be rather strict, focusing—among others—on values like empowerment, autonomy and informational self-determination of the data subject. The opinion identified the empowered individual as the key factor in the future data protection ecosystem—joined by "accountable controllers and innovative privacy engineering."[33]

It can be argued that the perspective on dignity in the opinion was not that innovative at all. A reason for this is that the contours of the concept of dignity itself are ill-defined and could

[28] *See* Explanations Relating to the Charter of Fundamental Rights (2007/C 303/02). In its judgement in Case C-377/98, Netherlands v. Parliament, 2001 E.C.R. I-7079 para. 70–77, the Court of Justice confirmed that a fundamental right to human dignity is part of Union law. It follows that none of the rights laid down in this Charter may be used to harm the dignity of another person, and that the dignity of the human person is part of the substance of the rights laid down in this Charter. It must therefore be respected, even where a right is restricted.

[29] Luciano Floridi, *On Human Dignity as a Foundation for the Right of Privacy*, 29 PHILOS. TECH. 308 (2016).

[30] GDPR, *supra* note 2, art. 88.

[31] Luciano Floridi, *On Human Dignity as a Foundation for the Right of Privacy*, 29 PHILOS. TECH. (2016).

[32] In the Opinion, it was proposed to set up an advisory group to investigate the relationships between human rights, data technology, markets and business models in the 21st century and "to assess the ethical dimension beyond data protection rules." The EDPS Ethics Advisory Group is composed of six experts: J. Peter Burgess, Luciano Floridi, Jaron Zepel Lanier, Aurélie Pols, Antoinette Rouvroy, and Jeroen van den Hoven. *See* EDPS ETHICS ADVISORY GROUP, TOWARDS A DIGITAL ETHICS (2018).

[33] EUROPEAN DATA PROTECTION SUPERVISOR, *supra* note 23.

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

therefore be defined in a number of ways. Unfortunately, the opinion seems to ignore that human dignity is an idea that appears in very different roles and thus did not explore any of them.[34] With its incomplete interpretation of the concept of dignity, it barely deviated from the guiding principles of the GDPR, which completely revolves around the combination of accountability and compliance on the one hand, and autonomy and empowerment on the other. Instead of choosing the safe and well-known principles of data protection, the EDPS-publication should have explored other dimensions of human dignity as a contribution to the debate. Because the notion of dignity embraces other constraining elements, the EDPS could have made reference to the dimensions of more paternalist forms of protection and dignity as human integrity and respect—for example, to the principle of non-commercialization that follows from human dignity.

On the eve of the GDPR entering into force, the EDPS called into question the effectiveness of the legal instrument itself and favored the approach of exploring the scope of human dignity. Unfortunately, his restrictive interpretation of the dignity-approach towards data processing only confirmed existing principles instead of calling them into question. On the contrary, Opinion 4/2015 was stuck in the well-worn fundaments of common data protection principles and if one had had any prior high expectations of the new dignity-approach, these were eventually not met. A more extensive interpretation would have called these principles into question and offered more room for debate. In the remaining sections, I will try to compensate for this omission. It will hopefully be demonstrated that remedies from a perspective of dignity interpreted as a constraint to the data industry, instead of an empowering tool to data subjects, would have been more fruitful.

C. Data Trade, Blurring Boundaries, and Solutions from Data Protection

In this section, the objections to current practices of data processing are analyzed and reconsidered in order to explore the different dimensions of human dignity. These objections concern, in particular, the trade and therefore commodification of personal data. In particular, these objections highlight further reaching commoditization of personal data by the abandoning of the silo-based approach. This abandonment has resulted in the formation of a global web of personal data exceeding the boundaries between formerly separated silos of data.

For adherents of dignity as empowerment, solutions to allay concerns about these developments could be found within the scope—and the limits—of the GDPR. But, drawing upon the constraining dimension of dignity, I will argue that the principles of data protection and the GDPR as a regulatory instrument are inadequate to address the general unease

[34] *See*, *e.g.,* Roger Brownsword, *Human Dignity, Ethical Pluralism, and the Regulation of Modern Biotechnologies*, *in* NEW TECHNOLOGIES AND HUMAN RIGHTS (T. Murphy ed., 2009).

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

surrounding data processing. It will be concluded that human dignity as a constraint offers a more hopeful perspective for this.

I. Data Trade

Personal data and information undeniably represent commercial value. The early metaphor of personal data as the new oil of the Internet demonstrates how much personal data are valued and justifies fragmentation of persons and their identity into tradable commodities.[35] Meanwhile, all aspects of being and everyday lives are transformed into tradable goods. This could be described as a process of datafication, commodification, and commercialization of individuals where human individuals consecutively become data-subjects, objects of trade and sources of profit.[36]

Virtually all types of companies, be it e-commerce firms, technology platforms, data brokers, or other types of businesses, greatly depend upon the collection, analysis and the exploitation of data for revenue. The analysis and exploitation of data enables these companies to profile their customers, micro-target users with advertisements, and sell profiles and sets of personal data. Data are a lucrative, tradable product from a source that never runs out.[37] It is said that, in the near future, data will become the pivotal asset of any business model and virtually all companies will be technology companies.[38] Most consumers who consent to exchanging personal data for services or goods, for example to get some product or online service for free or merely as an accepted part of any online transaction, consider this as part of the deal and an inevitable consequence of taking part in the digital world of today. As a consequence, their data will circulate online, and will be traded and resold by various parties infinitely—in theory.

For the human dignity as empowerment theorists, these practices can be legitimized by the consent given by the individual data subjects. From the GDPR it follows that "consent" of the data subject means "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action,

[35] European Commission Press Release 09/156, The Roundtable on Online Data Collection, Targeting and Profiling (March 31, 2009) ("Personal data is the new oil of the Internet and the new currency of the digital world.").

[36] Arno R. Lodder & Anne E. de Hingh, *An Analogy Between Data Processing and The Organ Trade Prohibition* (forthcoming).

[37] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, 220 OECD DIGITAL ECONOMY PAPERS (2013), https://www.oecd-ilibrary.org/docserver/5k486qtxldmq-en.pdf?expires=1522591418&id=id&accname=guest&checksum=154F0735253121EAC53377F7E3269D23.

[38] *See* Marco van der Hoeven, *Data Will Be Central to Any Earnings*, EXECUTIVE-PEOPLE (Apr. 5, 2018), https://executive-people.nl/597065/lsquo-data-komt-centraal-te-staan-in-elk-verdienmodel-rsquo.html.

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

signifies agreement to the processing of personal data relating to him or her."[39] The data ecosystem completely depends on the willingness of Internet users. Were it not for their autonomous consent, their personal data could not lawfully be harvested in the first place. This doctrine is based on the assumption that consumers are well-informed, digitally skillful, and autonomous beings who have a choice. Clearly, autonomy and informational self-determination are still the crucial factors in the regulatory approach of data protection and privacy today. Likewise, the right to object to profiling related to direct marketing under the GDPR is based on this conception.[40]

The effectiveness of the principle of consent has been subject to discussion for many years because of several structural problems with the consent-based model of privacy and data protection. One of them is that individuals who consent to the collection, use, and disclosure of their data cannot foresee what it is exactly they give their consent to and are unaware of all the third parties their data are shared with afterwards. Another problem is the fact that individuals in general have no other option than to give their consent because there are no real alternatives. And although the industry will argue that users always have the freedom and choice not to use their services, in reality not using them is for the most part not an option. The issue of coercive bargaining conditions that inexorably lead to a dead end was labelled by Sandel as the objection of "coercion". This forced consent or tainted consent occurs in any context: from the trade of body parts, to schools paying sums of money to children in order to stimulate them to read books. According to Sandel, "we have drifted from *having* a market economy, to *being* a market society, in which the solution to all manner of social and civic challenges is not a moral debate but the law of the market, on the assumption that cash incentives are always the appropriate mechanism by which good choices are made."[41]

[39] GDPR, *supra* note 2, art. 4, § 11.

[40] GDPR, *supra* note 2, recital 70. "Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information." *See also* GDPR, *supra* note 2, art. 4 § 4, where profiling means "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability or behaviour, location or movements."

[41] Sandel distinguishes two objections to the extending of the reach of market valuation and exchange: corruption—i.e. the degrading effect of market valuation and exchange on certain goods—and coercion—i.e. the creation of coercive bargaining conditions, or tainted consent. *See* Sandel, *supra* note 12; *see* also SANDEL, *supra* note 12.

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

Solutions for these problems arising from the consent-based model of data protection—or the perspective of human dignity as empowerment—are numerous. These solutions have in common that they all aim at securing, reinforcing or restoring the autonomy of the individual data subject. Empowering the data subject by strengthening the consent mechanism and giving more responsibility to the individual, is one of them.[42] It has been argued, however, that the introduction of the unambiguous consent—the former explicit consent—in the GDPR will not strengthen the legal protection by empowering the data subject. It will instead further weaken the effectiveness of the consent mechanism, as the responsibility of the user will grow, but not her or his actual negotiation position or power.[43]

Some have suggested a more differentiated system of consent based on the idea that decisions need only freely given, specific, informed, and unambiguous consent when it really matters—for example, when decisions may involve serious risks or consequences for the person who gives consent.[44] It can be argued, however, that in the current opaque data eco-system, these options are no longer feasible, as the uncertainty whether consent really matters lies at the heart of the problem.

Also, designs are proposed in which the user could negotiate the permission to access their personal data. This would solve the problem caused by the fact that the consent mechanism limits the user to a binary decision—either take it, or leave it—and having no fully-fledged alternatives. This solution would present the possibility—for example, to those who prefer not to view ads—to opt to pay an additional fee to view content.[45] A comparable suggestion, made by Berners-Lee, is to explore alternative revenue models like subscriptions and micropayments as this would "put a fair level of data control back in the hands of people."[46] This solution, however, still assumes that data represent economic value and therefore form a legitimate modality to pay for services. The fact that an autonomous choice is offered to the individual data subject between payment with his or her own data or payment with money, does not change the undesirable dimensions of the exploitation of personal information.

---

[42] FREDERIK J. ZUIDERVEEN BORGESIUS, IMPROVING PRIVACY PROTECTION IN THE AREA OF BEHAVIOURAL TARGETING 223 (2015).

[43] GDPR, *supra* note 2, art. 4.

[44] Bart W. Schermer, Bart Custers & Simone van der Hof, *The Crisis of Consent: How Stronger Legal Protection may lead to Weaker Consent in Data Protection*, 16 ETHICS & INFO. TECH. 171, 171–82 (2014).

[45] In practical terms, this would imply that these companies would be forced to offer an opt-out possibility which would enable customers to declare that they do not want to be profiled and receive targeted information. T. BAARSLAG ET AL., NEGOTIATING MOBILE APP PERMISSIONS (2015), https://eprints.soton.ac.uk/377378/1/NegotiatingMobileAppPermissions.pdf.

[46] Tim Berners-Lee, *I Invented the Web: Here Are Three Things We Need To Change To Save It*, GUARDIAN (Mar. 12, 2017), https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet.

Adherents of the consent theory are convinced that the commodification and commercialization of personal information is purely a problem of tainted consent and asymmetric markets. The solutions listed above are all based on the conviction that autonomy, empowerment and voluntary decision-making by the data subject are the key to effective data protection. In addition, the solutions listed above rest on the assumption that the problem can be addressed by simply adjusting the background conditions that markets operate in.

Indeed, in the Cambridge Analytica case hundreds of thousands of data subjects accepted a two dollar offer to participate to a psychology-quiz offered on MechanicalTurk. By accepting the payment, participants consented to Cambridge Analytica harvesting their own data and the data of 87 million of their Facebook friends for practices of political marketing relying on micro targeting. In my view, more precise consumer information about the context and the consequences of the consent transaction would not have had significantly different outcomes. This is directly related to the fact that the Facebook users were not aware of these transactions in the first place. Furthermore, even if they had been aware of it, they could not have opted-out from having their data harvested by a company that offered a small reward to their friends. And, in the theoretical case that they could have given their consent to the collection and reuse of these data by Cambridge Analytica and transparent and fair data processing conditions would have been established, would their concerns about these extreme forms of commodification of data have been laid to rest? Probably not, as in this case, the amount of the data, the intimate character of the data, and the complex and opaque ways the data were collected for specific political marketing purposes must lead to the conclusion that something more fundamental was at stake here.[47]

However upholstered the consent may be, after all, it still does not neutralize the concerns or the fundamental objections one could have with the commodification of personal data. This has to do with the fact that consent-based solutions fail to see that tainted consent is not the real problem here. They fail to understand that commodifying personal data "is a moral dilemma that market liberalization cannot solve."[48] This has to do with what Sandel would define as corruption. He claims that certain moral and civic goods are diminished or corrupted if bought and sold for money.[49] His argument from corruption appeals to the moral importance of the goods at stake, the "ones said to be degraded by market valuation and exchange."[50]

II. Blurring Boundaries

[47] Sandel, *supra* note 12.

[48] *See id.*

[49] *See id.*

[50] *See id.*

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

Like the data industry, governments make ample use of the possibilities of data collection, processing, and analytics. This is especially noticeable as the practice of large-scale data collection and analytics seems to have settled permanently in the practices of law enforcement agencies and intelligence and security services to fight and prevent crime and terrorism.[51] Just like private parties collect data to be able to anticipate preferences and influence future behavior, criminal or terroristic acts of individuals can also be anticipated through data. With increasing Internet use, endless surveillance opportunities are created, and online data and personal information have become a growing source of intelligence.[52]

For this reason, intelligence and security services and law enforcement agencies depend heavily on the personal information and data collected by commercial parties.[53] To improve their information position, the services intercept bulk communication—cable and non-cable-bound—and hack computers. They also actively collect and analyze data from open sources—OSINT or open source intelligence—through cooperation with other bodies, via informants, or by scraping the web. Lastly, they acquire datasets of commercial origin offered by third parties, and sometimes they purchase bulk datasets online that were illegitimately obtained through data breaches—theft—or hacking.

In the years 2016 and 2017[54] the Dutch secret service, AIVD, was an active party on the online stolen data market to acquire bulk sets of stolen and hacked data. It purchased two data sets of criminal origin each containing personal information of around 100 million individuals.[55] This operation demonstrated that the Dutch government does business with criminal parties, and, in doing so, contributes to the maintenance of an online demand and supply system of stolen data and supports the criminal supply of data on the dark web. In addition, other moral objections of a different nature can be formulated.[56]

This case perfectly illustrates on what scale commercial, criminal, and governmental actors exchange personal data and how the present data eco-subsystems are intertwined. It is

---

[51] *See* Els De Busser, *EU-US Digital Data Exchange to Combat Financial Crime: Fast is the New Slow*, 19 GERMAN L.J. (2018).

[52] Arno R. Lodder & Ronald Loui, *Data Algorithms and Privacy in Surveillance: On Stages, Number and the Human Factor*, *in* RESEARCH HANDBOOK OF LAW AND ARTIFICIAL INTELLIGENCE (W. Barfield & U. Pagallo eds., forthcoming).

[53] QUIRINE EIJKMAN, NICO VAN EIJK & ROBERT VAN SCHAIK, *Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act,* INSTITUTE FOR INFORMATION LAW (2018).

[54] More specific information on the period concerned is not available due to the secret nature of the operation.

[55] CTIVD, *Toezichtsrapport nr 55, Over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD* (2017).

[56] Bruce Schneier, *Data Is a Toxic Asset, So Why Not Throw It Out?*, CNN (Mar. 1, 2016), https://edition.cnn.com/2016/03/01/opinions/data-is-a-toxic-asset-opinion-schneier/index.html.

highly relevant, therefore, to establish that the majority of personal data used by governments have their first origin in the data industry. "Governments get themselves a copy of what the corporate world was already collecting," as it was put by Schneier.[57] Some authors suggest that the current under-regulation of online personal data extractions is beneficial for governmental agencies and that "hedged with some caveats, the current willful political neglect to limit personal data hoarding may be linked to a governmental reliance on the same increased efforts to extract and store personal data."[58] Another related question is to what extent an individual could be aware of these blurring boundaries when exchanging his/her data in an online transaction and subsequently becoming the victim of a data breach. Should this individual take into account the possibility of his/her data eventually ending up in the databases of the Dutch security services?

Objections to blurring of boundaries are thus related to the question of improper use, i.e. the fact that data are used for other purposes than expected by the data subject. This was acknowledged by the Dutch oversight committee (CTIVD) that reported that by acquiring and processing, or re-using, these data sets, although considered "open sources,"[59] the secret service had seriously infringed the right to privacy. In addition, the committee concluded the legal guarantees regarding the acquiring and processing of data were clearly insufficient.

The GDPR and general data protection principles do not apply to the processing of data by Dutch security services, as these are excluded from their scope.[60] It should be noted, however, that the general data protection principles from the 1981 Council of Europe Convention apply for all types of data processing in the private and public sector.[61] This is especially relevant with regard to the principle of purpose limitation of Article 5 of the GDPR,

---

[57] SCHNEIER, *supra* note 3; Bruce Schneier, *'Stalker Economy' Here to Stay*, CNN (Nov. 26, 2013), https://edition.cnn.com/2013/11/20/opinion/schneier-stalker-economy/index.html.

[58] *See* Sylvia E. Peacock, *How web tracking changes user agency in the age of Big Data: The Used User*, BIG DATA & SOC., 1, 8 (2014); *see also* Schneier, *supra* note 57, at 94: ("The NSA didn't build a massive eavesdropping system from scratch. It noticed that the corporate world was already building one, and tapped into it . . . . This leads to a situation in which governments do not really want to limit their own access to data by crippling the corporate hand that feeds them."); Lisa M. Austin, *Enough About Me: Why Privacy Is About Power, Not Consent (Or Harm)*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO 3 (2014).

[59] CTIVD, *Toezichtsrapport nr 55, Over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD* (2017).

[60] GDPR, *supra* note 2, art. 2. This Regulation does not apply to the processing of personal data: (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. *See also* Dutch Data protection Act art. 2(2)(b).

[61] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe art. 3, Jan. 28, 1981, E.T.S. 108.

the requirement that data must be collected and processed for a specified, explicit and legitimate purpose only—purpose specification; and the requirement that any further processing must be compatible with the original purpose for which the personal data were collected—compatible use. In other words, secret services must comply with purpose limitation and the exceptions made to purpose limitation, but under the condition that such exceptions are legal, necessary, and proportionate.[62]

Just like objections against data trade were not a matter of tainted consent alone, objections against blurring boundaries and commoditization of data are not, however, purely a matter of purpose limitation. As said, the flow of data from one sphere to the other and the blurring of boundaries between the realms of the private and the public, between the legal and the illegal, the commercial and the political, give rise to concerns that go beyond privacy and personal data protection. Purpose limitation-based solutions fail to see that the absence of a specified, explicit and legitimate purpose is not the real problem here. When data flow from one silo to the other, questions on whether it is Facebook, a criminal organization, or the secret service that is processing the data, whether the data collected are WhatsApp messages or behavioral data, and whether the purpose of processing is advertising or preventing terrorist attacks, are of secondary significance.[63]

The fact that technology companies, social media platforms, the advertising industry, criminal organizations, hackers, governments, and security services, all use and re-use, exchange, and recycle the same data bases, in theory over and over again, results not in centralized forms of surveillance—big brother—, but in different institutions that are all interconnected in exploiting and surveilling personal information of individuals—little sisters.[64] The more fundamental dilemma here is that through this endless re-use or circulation of personal data in bulk, data recycling mechanisms turn personal data into generic mass products. So, not only is personal information commodified by the fact that specific data represent an economic value and are therefore used for profiling, but a process of commoditization takes place during which these personal data risk to lose their particular character and become undifferentiated goods. This is the process of commoditization.[65]

---

[62] *See* EIJKMAN, *supra* note 53.

[63] LOKKE MOEREL, BIG DATA PROTECTION. HOW TO MAKE THE DRAFT EU REGULATION ON DATA PROTECTION FUTURE PROOF 58 (2014) (delivered lecture during the public acceptance of the appointment of professor of Global ICT Law, Tilburg University). *See also* Lokke Moerel & Corien Prins, *On the Death of Purpose Limitation* IAAP (Jun. 2, 2015), https://iapp.org/news/a/on-the-death-of-purpose-limitation/.

[64] For this metaphor and other works of Marc Schuilenburg (VU Amsterdam), see http://marcschuilenburg.nl/.

[65] Arno R. Lodder & Anne E. de Hingh, *An Analogy Between Data Processing and the Organ Trade Prohibition* (forthcoming).

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

It could be concluded that problems that are felt with regard to the blurring of boundaries—and giving up of silo-based approach—cannot be solved by applying general data protection principles alone. Autonomy, informational self-determination, consent, and purpose limitation: These principles all originate from the concept of dignity as a legal tool for empowerment. In the next paragraph it is argued that dignity as empowerment cannot hold as key concept in the discussion on how to curb the excesses of the digital economy.

D. Argument from Human Dignity as Constraint

The cases of Cambridge Analytica and the Dutch security and intelligence services serve as illustrative examples of the current practices within the present data-ecosystem. They, moreover, affirm once again what was demonstrated before by among others the Snowden revelations: That the essence and the origin of the problem are for the most part to be found in the under-regulated collection of personal data by corporate actors. Thus, a different approach in which individual autonomy and the role of the market play a limited role is needed.[66]

Two main concerns related to present day data-driven economy—the data ecosystem—have been presented so far. The first concern was the abundant trade and resulting commodification of personal data by commercial parties—buying, selling, and brokering of profiles and large sets of personal data. Second, the deconstruction of boundaries between industry, crime, and government with regard to personal information—resulting in a firm corporate-criminal-government nexus—leading to the increasing commoditization of personal data.

The objections to these phenomena could be formulated in terms of data protection law, for they stress the limits of data protection principles like autonomous consent, transparency, data minimization, and purpose limitation. The adherents of human dignity as empowerment believe these problems are resolvable by exactly enforcing these data protection mechanisms.

One of the problems that are highlighted in this contribution is the fact that the traditional understanding of informational privacy and data protection does not suffice because it covers only part of the current online reality and ignores large parts of the moral problems presented.[67] Measures from that perspective would therefore fail to remove the objections because they mistake them as a problem of lack of autonomy and individual control, and of coercion of individuals. Instead, they should be considered not as limiting self-determination of Internet users, but as a much more fundamental problem. A process of commoditization

[66] Sylvia E. Peacock, *How Web Tracking Changes User Agency in The Age Of Big Data: The Used User*, BIG DATA & SOC., 1, 1–2 (2014).

[67] *See* Austin, *supra* note 53, at 3.

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

confronts us as individuals are fragmented into bits of information that are multiplied, transferred, sold and brokered, from the timelines of Facebook to the advertising industry, voter-profiling companies, and criminal hackers—and vice versa—and eventually end up in databases of law enforcement agencies or intelligence and security services worldwide. As a result, we are confronted with an ethical and legal challenge that the GDPR will not be able to fix. In that case, other legal answers are needed.

The beginning of an answer could be found in the 2015 seminal opinion of the EDPS which admittedly started a discussion; however, it did not add many valuable new insights on data and dignity because it did not manage to get away from the dignity as empowerment-framework. As a thought experiment, it would have been useful for the opinion to argue by analogy.[68] Admittedly, it is stated in the Opinion that violations of dignity may include objectification, where a person is treated as a tool serving someone else's purposes. But, it could have gone further by exploring examples of the application of the concept of human dignity in other fields of law like in the context of bio-ethical issues, where the emancipatory dimension of dignity is commonly contrasted to its constraining dimension.

To approach moral and ethical issues in the field of biotechnology, traditionally two dimensions of human dignity are discerned: The subjective and the objective dimension or also known as the human rights approach versus the communitarian approach. Beyleveld and Brownsword were the first to discern the distinct and contradictory ways in which the concept is used in bioethics.[69] The subjective dimension considers human dignity as self-determination, emancipation, choice, and autonomy, whereas the objective dimension comprises values as respect, constraint, and collective responsibility.

In biolaw and the regulation of biotechnology, the constraining dimension of human dignity is a predominant factor supporting the legal prohibition of elements of the human body being made into objects and exploited as instruments, resources, and commodities. In general, legislators are reluctant to allow people to turn parts of their body into sources of financial gain. A commodification of the body, viz assigning monetary value to parts of the human body, occurs through illegal trade as well as in legal business but still ethically problematic businesses. Some examples of these problematic legal business include the procurement of tissues and cells from dead bodies, patients, and healthy persons, who, for various reasons, chose to give or sell parts of their body such as blood, hair, sperm, or ova.[70]

[68] Sandel, *supra* note 12 (suggesting we could "begin with moral intuitions we have about certain practices and to see whether or not the practices in question are relevantly similar.").

[69] BERYCK BEYLEVELD & ROGER BROWNSWORD, HUMAN DIGNITY IN BIOETHICS AND BIOLAW (1993).

[70] BRITTA VAN BEERS, *Persoon en Lichaam in het Recht. Menselijke waardigheid en zelfbeschikking in het tijdperk van de medische biotechnologie* (dissertation Vrije Universiteit Amsterdam) (2009); MARTIN GUNNARSON & FREDRIK SVENAEUS, THE BODY AS GIFT, RESOURCE, AND COMMODITY: EXCHANGING ORGANS, TISSUES, AND CELLS IN THE 21ST CENTURY

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

This dignity approach has its origin in the person-thing bifurcation—the Kantian idea that human beings should always be understood at the same time as an end in themselves and never merely as a means. In other words, human beings have their dignity and only things should have a price. The principle that the human body should not be a source of revenue is asserted in numerous national and international legal sources.[71] The prohibition of the commercial selling of one's own organs is an illustrative example of the illegality of commodifying one's body parts because it is incompatible with the objective dimension of human dignity: The human body is *res extra commercium* or beyond price.

Although also in the context of bioethics and biolaw, the conceptual status of dignity is complex and not without controversies. It could still be helpful to take it into account to deepen the discussion on dignity with regard to personal data processing and to explore the loopholes in contemporary data protection and privacy laws.[72] The two-dimensional interpretation of human dignity could contribute to the debate on the commodification and commoditization of personal data, which the EDPS sought to give an ethical dimension. The trade of personal information could indeed be represented as an extension of the trade of body parts. As was so beautifully articulated by Floridi: "My" in my data is not the same as "my" in my car, but it is the same as "my" in my hand.[73] The protection of data could, or should, be interpreted as the protection of personal identity or personal integrity, as personal information plays a constitutive role in who an individual is and can become.[74]

More than two years after Opinion 4/2015 was published, the Ethics Advisory Group published its report *Towards a Digital Ethics*.[75] This publication could be considered as another step forward in the debate on digital ethics, "focusing on how we can make technology work in the interests of human dignity."[76] According to the EAG report, "a re-

(Martin Gunnarson & Fredrik Svenaeus eds., 2012); *see also* Manuel Wackenheim v. France, Communication No. 854/1999, U.N. Doc. CCPR/C/75/D/854/1999 (2002).

[71] *See* Convention on Human Rights and Biomedicine of the Council of Europe art. 1, Apr. 4, 1997, E.T.S. 164; Universal Declaration on the Human Genome and Human Rights, art. 1, 2(a); International Declaration on Human Genetic Data, art. 1; Universal Declaration on Bioethics and Human Rights, art. 2(c), 3(1). *See also* Arno R. Lodder & Anne E. de Hingh, *An analogy between data processing and the organ trade prohibition* (forthcoming) for an elaboration of the analogy between (parts of) the human body and data related to the human individual.

[72] *See*, *e.g.*, NORA JACOBSON, DIGNITY AND HEALTH 186–88 (2012) (noting the objections against the use the concept of dignity in the field of bioethics).

[73] Luciano Floridi, *On Human Dignity as a Foundation for the Right of Privacy*, 29 PHILOS. TECH. (2016).

[74] *Id.*

[75] EDPS ETHICS ADVISORY GROUP, *supra* note 32.

[76] *See* Ethics Advisory Group, *Ethics*, EUROPEAN DATA PROT. SUPERVISOR (2015), https://edps.europa.eu/data-protection/our-work/ethics_en.

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

assertion of fundamental values at the heart of European data protection and other fundamental rights and liberties is needed."[77] In the report, it is again repeated that the right to data protection appears insufficient to understand and address all the ethical challenges brought about by recent digital technological developments and that "personal data protection regimes, like the GDPR, . . . appear inadequate to address the unprecedented challenges raised by the digital turn."[78] The EAG even goes further by suggesting that "In particular, the tensions and frequent incompatibilities of core concepts and principles of data protection with the epistemic paradigm of big data, suggest limits to the GDPR even prior to its application."[79]

In the EAG-report, it is stated that new concepts of data protection will be called for because unprecedented commodification of data gathered from persons, behaviors, and environments can be expected from the new big data ecosystem. Apart from values like freedom, autonomy, solidarity, equality, democracy, justice, and trust, the EAG refers first and foremost to dignity as a core value that will be directly challenged by this new data ecosystem.[80]

Some tentative references to the constraining dimension of human dignity are made by the EAG.[81] This is especially reflected in the "Kant-ian" way the advisors address the commodification of personal data: "When individuals are treated not as persons but as mere temporary aggregates of data processed at an industrial scale to optimize . . . interactions with them, they are arguably not fully respected, neither in their dignity nor in their humanity."[82]

In my opinion, the EAG-report should have concluded that the restriction or ban of at least some of the most excessive business models that are based on the commodification and commoditization of personal data, should be taken into account. As was stated by Berners-Lee,

> Two myths currently limit our collective imagination: The myth that advertising [based on data collection] is the only possible business model for online companies, and the myth that it's too late to change the way

[77] EDPS ETHICS ADVISORY GROUP, *supra* note 32, at 16.

[78] *See id.*, at 7.

[79] *See id.*

[80] *See id.*, at 16.

[81] *See id.*, at 9.

[82] *See id.*, at 17.

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

> platforms operate. On both points, we need to be a little more creative.[83]

Unfortunately, this creative, and normative, leap towards a more constraining data protection regime was not made by the EAG.

E. Conclusion

The scandal with Facebook and Cambridge Analytica and the Dutch security services case demonstrate that misuse of data collection is constantly lurking and principles of data protection law—like the informed and unambiguous consent and the principle of purpose limitation—have mostly lost their meaning.[84] Online data processing practices turning personal information into a commodity interfere with the notion that a person should be *extra commercium*. Moreover, the de-silo-ization of the data market resulting in the ongoing transfer of data between commercial, criminal, and governmental parties has detrimental effects because it commoditizes individuals and their data. Not only does this influence the protection of data and the privacy of individuals, but it has much greater implications for the lives of those individuals. The risks of the data market for individuals are related to their freedom, their feelings of control and power, but also of trust and security, legal certainty, and personal integrity. As noted by Roessler "concern can also focus on the transformation of social relationships, the idea of identity, on issues of justice and equality and on democratic political procedures."[85]

In this Article, it was argued that to address these general concerns a more substantive level of protection from the law would be appropriate, and "a broader legal canvass than simply the idea of privacy or data protection," to paraphrase Austin, is needed.[86] Leaving the solution solely to the autonomous consumer and to principles of data protection will not bring us any further towards an effective solution. Other forms of legislative intervention will be indispensable. If it is agreed upon that what is at stake here, could—at least, provisionally—be legally framed as the right to human dignity as constraint, it could be argued that at least in certain cases a more restrictive regulatory approach would be appropriate. Individuals should, in certain circumstances, be prevented from giving up parts

[83] Berners-Lee, *supra* note 16.

[84] LOKKE MOEREL, BIG DATA PROTECTION: HOW TO MAKE THE DRAFT EU REGULATION ON DATA PROTECTION FUTURE PROOF 58 (2014).

[85] Beate Roessler, *Should Personal Data Be a Tradable Good? On the Moral Limits of Markets In Privacy*, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES (Beate Roessler & Dorota Mokrosinska eds., 2015).

[86] *See* Austin, *supra* note 53; s*ee also* Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 411 (2014) (claiming "if we were designing things from scratch we would almost certainly want to use a word other than 'privacy'").

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press

of their personal information. For not only do they lack any real idea what it is they give their consent for, but by giving this consent, I argue, they jeopardize something much more valuable—in short: Their human dignity. As Schneier proposed in this context: "Why not abolish the data-driven business model of (online) companies and social media by making certain forms of data collection and processing illegal? We can make the business models that involve massively surveilling people the less compelling ones, simply by making certain business practices illegal."[87] A prohibition of the limitless collection and circulation, the transfer of data back and forth between silos, and recycling of bulk sets of personal data could be such a protective measure.

[87] Schneier, *supra* note 56; *see also* SARAH CONLY, AGAINST AUTONOMY: JUSTIFYING COERCIVE PATERNALISM (2013).

https://doi.org/10.1017/S2071832200023038 Published online by Cambridge University Press