

## CHAPTER 3

# Big Data: Ethical Debates

In their research, scientists continuously make decisions that need to balance what they can do and what is morally reasonable to do. This applies notably to innovative research at the forefront of technological developments. In research projects located at universities, and in democratic societies, such decisions are commonly not simply made by isolated individuals or research groups. Biomedical research and studies involving human subjects in particular have become increasingly regulated in this respect, with *Institutional Review Boards* (IRBs)/*Ethics Review Boards* (ERBs) and *Research Ethics Committees* (RECs) playing a decisive role.

With regards to regulatory efforts and research ethics, Hedgecoe (2016) observes:

‘The most obvious regulatory growth has been in the bodies responsible for the oversight of research, on ethical grounds, before it is done (a process referred to here as ‘prior ethical review’) – for example, institutional review boards (IRBs) in the United States, Research Ethics Committees (RECs) in the UK, research ethics boards in Canada – which have become progressively more powerful, with more kinds of research falling under their remit and with greater control over the research they oversee.’ (578)

These boards and committees are often established at universities, relying on peer evaluation by scholars with (ideally) expertise in respectively related fields.<sup>26</sup> Governmental funding agencies are especially likely to request such ethical approval, issued by institutional ethics review bodies, prior to the start of research projects. In some cases, intermediate assessments are also required. Likewise, some journals ask for confirmation of the ethical approval of a piece

---

### How to cite this book chapter:

Richterich, A. 2018. *The Big Data Agenda: Data Ethics and Critical Data Studies*. Pp. 33–51. London: University of Westminster Press.  
DOI: <https://doi.org/10.16997/book14.c>. License: CC-BY-NC-ND 4.0

of research (which does not necessarily mean though that they demand written proof of this).

As stressed by Hedgecoe (2016, 578), biomedical research has become more regulated over the last 50 years. This field has a comparatively long tradition in establishing ethical principles. This is arguably different to the more recently emerging applications of data science and big data-driven research. While big data may allow for biomedical insights, their retrieval is not necessarily classified as an approach that falls under regulations that have been established for non-interventional/observational biomedical research.

Since emerging technologies related to big data potentially open up previously unavailable opportunities for research, ethical questions will be also (at least partly) uncharted territory (see e.g. Mittelstadt and Floridi 2016; Zwitter 2014; Swierstra and Rip 2007; Moor 2005). This matter becomes even more complicated when considering that such research does not only take place in university departments. Internet and tech corporations themselves also conduct research, circumventing forms of ethical oversight as they apply to universities (Chen 2017; Rothstein 2015).<sup>27</sup>

Under which conditions and how these dynamics play out in big data-driven public health research and surveillance will be explored in Chapters 4 and 5. As a broader contextualisation however, the following subchapters first examine more generally which ethical issues, values and norms have been at stake when discussing how big data is used in research. For this too, Habermas' theory of communicative action and the notion of discourse ethics is relevant. Both allow for a conceptualisation of how norms and moral values are formed.

As described in the previous chapter, this requires that communicative routines are challenged and debated, potentially re-organised or affirmed. I established that emerging technologies have a key role in triggering such dynamics: 'Emerging technologies, and the accompanying promises and concerns, can rob moral routines of their self-evident invisibility and turn them into topics for discussion, deliberation, modification, reassertion.' (Swierstra and Rip 2007, 6). Norms and values can be considered as tacit, moral assumptions guiding such routines.

One of the reasons why we have recently witnessed broader debates on rights and demands, such as privacy, transparency, security, autonomy, or self-responsibility, is that big data developments have challenged related norms. Therefore, it is relevant to introduce some of these negotiated values more generally before proceeding to more specific conditions and cases. I first provide an overview of privacy, security, transparency, and openness. These have been arguably core (conflicting) values in big data debates. They have been mobilised as justification for big data's relevance, as reasons for inherent risks, and as constraints to public access alike (Puschmann and Burgess 2013; boyd and Crawford 2012). Calls for openness and transparency are also related to the open data movement, which promotes the accessibility of data as a public good.

As I show in the next subchapter, this may conflict on the one hand with corporate data interests and on the other hand raises issues for ensuring individuals' privacy. The last three subchapters depict debates concerning informed consent, (un-)biased data, and corporate data economies. It is particularly highlighted how big data's alleged lack of biases is brought forward in ethical debates concerning the relevance of informed consent. In contrast to the common 'digital positivism' (Mosco 2015) when referring to big data, I stress the role of algorithmic biases and how these reflect the tech-corporate contexts in which large parts of big data are being created.

## Privacy and Security

Privacy and security are arguably among the most extensively discussed concerns regarding big data uses.<sup>28</sup> As I will show further below, they are a well-established, but misleading dichotomy. Privacy denotes individuals' possibilities for defining and limiting access to personal information. This may relate to bodily practices, for example unobserved presence in personal spaces, or to information generated based on individuals' digital traces (see e.g. Lane et al. 2014; Beresford and Stajano 2003).

Regarding individual privacy, big data critics have emphasised individuals' (lack of) control and knowledge concerning the personal information collected when using online services (Tene and Polonetsky 2012; Lupton 2014d). This aspect is also closely related to diverging opinions on individuals' responsibility to protect their privacy, and data collectors' moral liability for fair service conditions (Puschmann and Burgess 2013). While big data proponents, and corporate service providers in particular, insist that users' information remains anonymous (Hoffman 2014), critics have raised doubts about the very possibility of anonymising data of such diverse qualities on such a large scale (Ohm 2010).

In democratic societies, privacy is considered a civic right. The *right to privacy* is (implicitly or explicitly) anchored in many national constitutions (González Fuster 2014; Glenn 2003). The *protection of personal data* tends to be considered as an extension of the right to privacy. However, the Charter of Fundamental Rights of the European Union treats them separately, with Article 8 focusing on data protection, and respect for private and family life being covered in Article 7 (The European Union Agency for Fundamental Rights, n.d.).

More recently established rights, such as the *right to be forgotten*, as established in Argentina and the EU, are closely related to (although distinct from) the right to privacy. In a 2014 ruling, the *Court of Justice of the European Union* decided that '[i]ndividuals have the right – under certain conditions – to ask search engines to remove links with personal information about them' (European Commission 2014, 1-2). This has been described as a strong signal

that ‘privacy is not dead’ and that the EU approach contrasts with US ‘patch-work’ privacy policies (Newman 2015, 507).

Restrictions apply to the right to be forgotten where it conflicts with major public interests. This also implies that it ‘[...] will always need to be balanced against other fundamental rights, such as the freedom of expression and of the media’ (European Commission 2014, 2). The criticism has been made that this decision is partly left to corporations owning respective search engines, notably to market leader Google. Freedom of speech, as well as the right to safety, have been particularly underscored as rights and values countering individual privacy considerations. These balancing acts, weighing individual rights against the public interest, are also characteristic of ethical debates concerning public health surveillance.

Apart from individual privacy, big data have revived attention on the issue of ‘group privacy’ (Taylor, Floridi, van der Sloot 2016; Floridi 2014; Bloustein 1976). This notion implies that privacy is not merely a right which should apply to persons, but likewise to social groups. As Floridi (2014) observes, the value of privacy has been predominantly contrasted with that of (public) security: ‘Two moral duties need to be reconciled: fostering human rights and improving human welfare’ (Floridi 2014, 1). He opposes the assumption, however, that the latter would be a political concern regarding the public at large and the former an ethical issue concerning individuals’ rights.

In the spirit of pragmatist ethics’ anti-dualism, i.e. its suspicion towards dichotomies, Floridi claims that a focus on these two positions of the individual and society overall is too simplistic. Such a limited viewpoint ultimately overlooks aspects relevant to broader societal dynamics. In consequence, the ethical debate lacks consideration for certain validity claims to normative rightness. Not merely individuals, but likewise groups should be considered as holders of privacy rights. This, according to Floridi, is increasingly of importance in an era of open and big data, since individuals (especially in their role as consumers) are commonly targeted as group members.<sup>29</sup>

Balancing privacy and security is closely related to one of the tensions predominantly stressed in public health research and biomedical research more generally: safeguarding individual, civic rights versus public health and wellbeing as a common/public good.<sup>30</sup> With regards to genomics research, Hoedemaekers, Gordijn and Pijnenburg emphasise that ‘[a]n appeal to the common good often involves the claim that individual interests must be superseded by the common good. This is especially the case when the common good is seriously threatened’ (2006, 419).

To determine when a society may be ‘seriously threatened’ (e.g. by a disease) is however not always as clearly discernible as for instance in the case of epidemics/pandemics: for example, when it comes to preemptive measures such as coerced vaccinations. Moreover, the response to a perceived threat depends on the respective understanding of values relevant to the ‘common good’ (London

2003). In this sense, conceptualising data as contribution to the common good becomes a crucial factor in justifying their means of collection. It is therefore particularly insightful and relevant to address how tech corporations take an interest in demonstrating how ‘their’ big data allow for insights beneficial to societies’ wellbeing – with (public) health being a widely acknowledged factor in this.

## Open Data

One can observe controversies around the ‘trade off’ between privacy (commonly depicted as an individual right) and security (commonly depicted as a value related to public welfare, public interest and the common good) vividly with regards to governmental surveillance, as well as tech-corporate support of and acquiescence in such practices (see also Chapter 2). At the same time, transparency has been mobilised in claims to the *normative rightness* of big data practices (Levy and Johns 2016).

Transparency indicates a high degree of information disclosure. It implies openness regarding features and processes: for instance academic, governmental, corporate, or even private practices. The notion is commonly linked to accountability. With the concept of *open data*, transparency has been applied to big data as such: ‘Open data is data that can be freely used, re-used and redistributed by anyone – subject only, at most, to the requirement to attribute and share alike.’ (Open Knowledge International. n.d.; see also Gurstein 2011). The concept applies to data which are comprehensively accessible and technically as well as legally modifiable, allowing for re-use and distribution.

Open data can be seen as a form of output-transparency. They allow for insights into the kinds of data collected by governments or research actors/institutions, granted even to external actors who were not involved in the initial data collection process. Open data emphasise transparency and sharing as a moral duty and quality feature. While acknowledging the potential advantages of open data, authors such as Levy and Johns advise caution when it comes to such claims. They argue that certain actors may also ‘weaponize the concept of data transparency’ (2016, 4). The authors stress that ‘[...] legislative efforts that invoke the language of data transparency can sometimes function as ‘Trojan Horses’ designed to advance goals that have little to do with good science or good governance’ (2; see also Iliadis and Russo 2016, 3ff.).

Openness and transparency have not only been applied to data as product, but also to data collection processes. In data collection – be it for research, commercial purposes, or governmental statistics – transparency regarding procedures and purposes is known to positively influence individuals’ willingness to compromise on privacy (Oulasvirta et al. 2014). For quantitative research, transparency is, moreover, a crucial methodological criterion to ensure the

reproducibility of results (Stodden 2014). Both aspects are challenged in most big data practices however, since the level of transparency is considerably limited.

While open data have gained in importance (World Wide Web Foundation 2016; Kitchin 2014), most corporate data are still inaccessible to civic actors – except if they are paying (advertising) customers or commissioned researchers. Access to big data is in most cases a privilege of actors affiliated with corporations or research projects (boyd and Crawford 2012; Manovich 2011). Such corporate limitations in data access are usually presented as a means for ensuring users' privacy, but have obvious economic advantages too. Data allow for insights into (potential) customers' attitudes and behaviour, ensuring an economic advantage and making these data valuable commercial assets (see also the last subchapter below). Individuals have to rely on assurances that their data are used only in limited ways. Due to this common limit on access to big data for non-corporate, external actors, such as researchers or users themselves, such actors can hardly assess claims regarding how data are anonymised, collected or utilised. In this sense, as long as certain, corporate big data are not indeed published as open data, one may claim openness regarding the processes, but the actual material itself is not transparently accessible.

As mentioned above, it is commonly argued that this lack of transparency is needed in order to safeguard customers' privacy (Puschmann and Burgess 2013; boyd and Crawford 2012). One may query though what other motives are relevant to this mobilisation of privacy, or how this influences, for example, companies' investments in data anonymisation (see also Mattioli 2014). The very possibility of anonymising certain (big) datasets has been fundamentally called into question (Ohm 2010). In light of these challenges, it seems even more worthy of discussion that such data are being collected and used in commercial contexts, among others.

Big data enforce an increased, though neither necessarily deliberate nor conscious, transparency of online users/consumers. The full extent of this transparency is only visible to those actors controlling the main data collecting platforms or gaining external access to these (Andrejevic 2014, 1681). What is ultimately collected here, are vast amounts of personal information, concerning individuals' preferences, attitudes, moods, physical features, and – as emphasised in this book – health status and health-relevant behaviour. With the advent of big data, the notion of transparency has been increasingly applied to and demanded from individuals and their practices (O'Hara 2011).

The delusive expression 'I have nothing to hide' has been popularised in a post-9/11 era when individuals globally felt that their personal integrity should stand back in favour of public welfare and safety (see also Levi and Wall 2004). In this context, similarly to Floridi (2014), Solove (2011) observes that '[...] when privacy is balanced against security, the scale is rigged so that security will win out nearly every time' (207; see also Keeler 2006). In order to weigh

up these complex values though, one needs to be aware of the full implications of privacy breaches. However, considering the lack of consideration for group privacy, many aspects are still neglected in current debates and decision making processes.

While individuals may be more willing to compromise on their privacy when it comes to security and public welfare/common good, this is often not their main motive for providing and producing personal data. It has often been suggested that ‘convenience’ is a main factor for the easiness with which users’ allow access to their personal data. This occurs in some instances in a rather condescending tone (see e.g. the quotes by *Gnip* CEO Jud Valeski in Puschmann and Burgess 2014 or McCullag 2008) or as a comparatively neutral observation (Craig and Ludloff 2011, 1 and 13). Terms such as ‘convenience’, or even ‘ignorance’, should however instead be translated into ‘lack of choice’ and ‘built-in data trades’.

Apart from the decision to opt-in or opt-out, in most situations, users have only marginal leeway in defining which data may be collected. In order to use services such as social networking sites or effective search engines, users have to agree to their data being used by the companies owning these platforms. Opting out of these platforms likewise implies opting out of the social benefits which these offer. Not using a particular search engine may result in a lower quality of information retrieval; not being present on a popular social network may affect a persons’ social embeddedness. In light of the relevance of digital media for individuals’ private and professional life, drawing on such services is no longer a matter of convenience and personal choice, but of societal expectations.

As Andrejevic points out, simplifying users’ behaviour as a well-balanced, conscious trade of privacy in favour of convenience ignores the power/knowledge relations emerging between contemporary digital platforms and users: ‘This framing of the exchange assumes people are aware of the terms of the trade-off and it construes acquiescence to pre-structured terms of access as tantamount to a ready embrace of those terms.’ (Andrejevic 2014, 1682) This is related to the accessibility and intelligibility of terms of services and privacy policies, but also to the seamless embedding of data sharing in digital media use, and the lack of practical insights into its (negative) consequences (ibid.).

The compliance of many users in giving away data to access certain services stands in stark contrast to the lack of public insight into corporate big data practices: into their contemporary collection, documentation, possible ramifications and future uses. Andrejevic speaks fittingly of a ‘big data divide’ (2014), referring to ‘[...] the asymmetric relationship between those who collect, store, and mine large quantities of data, and those whom data collection targets’ (1673).<sup>31</sup> This notion inherently rejects the often implicit assumption that users’ data sharing is simply a matter of well-informed, deliberate choices. Likewise, it

emphasises the non-transparency experienced by those civic actors producing big data, and the power imbalances inherent to datafication.

### Data Asymmetries and Data Philanthropy

Big data are often inaccessible data, especially when it comes to those produced on commercial platforms. While open data are becoming more common for governmental, scholarly or institutional datasets (although resistance is also notable in these domains), this kind of accessibility has not yet taken off among corporations yet: 'Despite the growing acknowledgement of the benefits, we are far from having a viable and sustainable model for private sector data sharing. This is due to a number of challenges – most of which revolve around personal data privacy, and corporate market competitiveness.' (Pawelke and Tatevossian 2013)

The lack of accessibility implies that actors looking at these data from a corporate perspective (or commissioned by respective companies) can assess what kind of information is revealed about the individuals generating these data. Moreover, only those 'insiders' have insights into the possibility of anonymising information concerning users. This lack of accessibility condemns most actors and social groups in contemporary societies to speculation about the possibilities and risks of big data.

Big data function as crucial 'sense-making resources in the digital era' (Andrejevic 2014, 1675). On the one hand, they allow for the production of knowledge concerning, for example, individuals associated with a certain profile (email, social network, etc.) or IP address. On the other hand, they would also allow for a concrete assessment of ethical concerns. This is hindered, however, because big data's accessibility is not systematically granted to company-external actors in, for example, mandatory data audits. Therefore, the big data divide implies power/knowledge conditions that systematically exclude individuals from access to data which would allow them to assess the data generated by corporations, the conditions under which this is done, and how this information is used.

According to boyd and Crawford, the lack of such independent access to big data results in a problematic constellation of 'data rich' and 'data poor actors' (2012, e.g. 674). The authors are notably concerned about the ramifications for research. They argue that the limitations in accessing big, corporate data create a '[...] restricted culture of research findings.' (2012) This may lead to a bias, due to the kinds of (uncritical) questions which are being asked or due to the privilege given to leading, prestigious universities for (good publicity) collaboration. Moreover, boyd and Crawford cite a scholar who suggested '[...] that academics should not engage in research that industry "can do better" (ibid.). While this assessment is problematic as such, since it backs up the aforementioned asymmetries and related risks for research, it also hints at another issue. The research skills necessary for using big data can be mainly trained by company

employees or commissioned scholars. The biased, unregulated accessibility of big data also raises the risk that large parts of the academic community are unable to train skills relevant to assessing these kinds of data.

In this context, one should not only speak of a big data divide, but also scrutinise the risk of data monopolies. The phrase 'big data divide' emphasises the tensions resulting from asymmetries in data access. It calls attention to the biased capacities for gaining insights into this material and assessing its implications. In addition, the term 'data monopolies' stresses that this divide not only characterises customers' lack of agency, but the market dominance of very few internet and tech corporations. Addressing practical challenges in information systems research, Avital et al. (2007) discuss the influence of 'data monopoly/oligopoly' as a sector for data utilisation with high complexity and low (public) availability. It is '[...] populated with large companies or agencies that collect and analyze systematically large datasets for resale or other for-profit activities. (e.g., ITU, IDC, Gartner, OECD, US Census)' (Avital et al. 2007, 4).<sup>32</sup> To this list, one should also add leading tech companies such as Google and its parent company Alphabet Inc., Facebook and subsidiary platforms/technologies such as Instagram, Whatsapp, and Oculus VR, but also increasingly popular apps such as Snapchat (owned by Snap Inc.).<sup>33</sup>

Avital et al. (2007) focus on targeted attempts at collecting data to shape research processes. In contrast, big data collected by companies through search engines, social networking sites, photo sharing sites, messengers, and apps more generally are the result of complex entanglements between commercial interests, interface designs, algorithmic processes and users' indication of preferences, actions or attitudes. This information is a highly profitable asset for advertising customers and for the optimisation of internal services. Legally, these constellations are further complicated by the fact that leading internet/tech corporations are originally based in the United States, while offering their services to users outside the US whose data are likewise collected.

Yet despite the general lack of open (big) data in the private sector, certain data are in fact available to the public. For instance, Twitter Inc. makes user data, which are publicly posted on the microblogging platform, accessible through open application programming interfaces (such as the 'search and streaming' APIs). This includes public tweets, but also favs and retweets of these short posts. Even in this case, as Burgess and Bruns point out, the conditions under which Twitter data could be used have become increasingly restrictive over time (2012; see also Van Dijck 2011). Nevertheless, thanks to the partial availability of this kind of material, Twitter has become a particularly popular subject of many research papers using or reflecting on big data.<sup>34</sup> This development also hints at the benefits which corporations may expect from allowing access to data, going beyond direct, economic incentives: an effect which has been described with the term 'data philanthropy'.

The idea of 'data philanthropy' suggests that there are moral incentives for sharing big data. Their public accessibility is not merely framed as a question of

economic value, but as contribution to the public good. This is closely related to 'open data' or phrases such as 'data commons'. The term was mildly popularised by the *United Nations Global Pulse* initiative, a flagship project promoting the use of big data for sustainable development and humanitarian action (see also Chapter 4). During the 2011 World Economic Forum, Kirkpatrick (on behalf of *UN Global Pulse*) complained that '[...] while there is more and more of this [big] data produced every day, it is only available to the private sector, and it is only being used to boost revenues' (Kirkpatrick 2011). In consequence, the author stated, big data's potential for being employed for the public good was largely neglected. He suggested the notion of 'data philanthropy' with regards to sharing big data generated in the private sector in support of development causes, humanitarian aid, or policy development.<sup>35</sup>

In a blog post following up on his talk, Kirkpatrick briefly referred to economic issues ('business competition') as well as ethical concerns ('privacy of their customers') as challenges to this idea. These were also given as reasons why it was not clear in which directions data philanthropy might develop. Three years later, Pawelke and Tatevossian, also on behalf of *UN Global Pulse*, stated in a blog post on public data sharing that very few datasets are truly publicly accessible (Pawelke and Tatevossian 2013).

In 2011, Kirkpatrick mainly emphasised the sharing of private sector data with the public sector. In 2015, Vayena et al. indicated another variation in which this data sharing may take place. The authors observe that in data philanthropy '[...] public-private partnerships are formed to share data for the public good' (Vayena et al. 2015). Corporations commonly do not simply release big data, but allow for controlled access granted to selected partners. As also mentioned in the above reflections on data monopolies, an ethical issue concerns the fact that access to data, epistemic possibilities, and (scientific) knowledge production are controlled by corporations. Novel constellations in public-private big data research bring up the question to what extent studies drawing on these data inherit ethical issues pertinent to the original data collection. And what does it mean when academic research asserts the credibility of commercial big data practices by fashioning them as a key contribution to the common good? This also raises the issue that not only the practices, but also the ethics of research itself may change (see also Kalev 2016). The latter point has been especially noticeable in debates concerning informed consent.

## Informed Consent

Informed consent is a moral cornerstone for research involving human subjects. Its establishment goes back to the Nuremberg Code (1947), which outlines 10 research ethics principles, the first being dedicated to informed consent. The document resulted from the 1946–1947 trials of doctors who conducted experiments with humans in Nazi concentration camps (Weindling

2001). In terms of the moral considerations regarding individuals' rights and wellbeing, informed consent is crucial for ensuring, in particular, human dignity, the respect for persons, and respect for autonomy (Rothstein and Shoben 2013, 28; Lysaught 2004; Faden and Beauchamp 1986).

There are cases, for example in large-scale epidemiological research, where data have been obtained for research from existing databases without seeking informed consent (Nyrén, Stenbeck and Grönberg 2014, 228ff.). Such decisions are, however, subject to scrutiny by ethics review boards, weighing broader public health risks against harm to individuals. The fact that big data-driven research unhesitatingly forgoes informed consent mechanisms has thus sparked ethical concern among some academics. One reason for this tendency may be that '[...] the precursor disciplines of data science – computer science, applied mathematics and statistics – have not historically considered themselves as conducting human-subjects research' (Metcalf and Crawford 2016, 2). This assumption also applies arguably to some of the biomedical, big data-driven approaches emerging in recent years.

The negligence of informed consent has been especially controversial with regards to experimental, interventional research conducted in private-public partnerships. Entanglements between consent, research ethics and corporate big data practices became obvious in a much-debated study involving Facebook data, known as the 'emotional contagion experiment'. As the authors of the original report on this study describe '[t]he experiment manipulated the extent to which people ( $N = 689,003$ ) were exposed to emotional expressions in their News Feed.' (Kramer, Guillory, and Hancock 2014). The study included a combination of two, parallel experiments during which users were either exposed to a reduced amount of positive emotional content posted by 'friends' on their news feed, or were shown fewer posts with negative emotional content. Posts rated as containing positive or negative content were respectively withheld.

The study design was meant to test whether users' perception of certain emotions in their newsfeed would increase the likeliness of them posting similar emotional (i.e. increasingly negative or positive) content. The latter was interpreted as an expression of the users' mood. This manipulation of users' newsfeeds led to public and academic debates concerning the ethical dimensions of this study (Kleinsman and Buckley 2015; Schroeder 2014; Booth 2014). The experiment was conducted in collaboration between an employee of Facebook's *Core Data Science Team* (Kramer) and two researchers of Cornell University. The report on this study was published in the peer reviewed journal *Proceedings of the National Academy of Sciences of the United States of America* (PNAS). With regards to this experiment, Kahn, Vayena and Mastroianni observe that '[...] the increasing number of public-private partnerships and collaborations involving data uses and reuses will raise challenging questions about balancing privacy and data sharing, as evidenced by the Facebook example and recent calls for large-scale data philanthropy projects' (2014).

What is at stake in this study goes beyond issues of privacy: it demonstrates controversial possibilities for circumventing informed consent. An inquiry by Chambers, a cognitive neuroscientist and contributor to *The Guardian* newspaper, reveals how corporate practices had an impact on decisions concerning its ethical assessment. In an email to the *PNAS* editor responsible for approving the study's original publication and to the authors, Chambers inquired about the interpretation of informed consent in this study. Later he published a screenshot of the inquiry and the editor's reply on Twitter. In particular, he asked for the reasons why the approval of institutional review boards (IRB) was not mentioned in the article, as this is required by the journal's policies.

In response, Fiske, the editor responsible., explained the decision to approve the paper for publication: 'I was concerned about this ethical issue as well, but the authors indicated that their university IRB had approved the study, on the grounds that Facebook filters user news feeds all the time, per the user agreement. Thus, it fits everyday experiences for users, even if they do not often consider the nature of Facebook's systematic interventions.' (Chambers 2014) The answer is insightful, since the reason for giving ethical approval is directly derived from a common corporate practice. In doing so, moral values relevant to the study are inferred from Facebook's corporate rationales and algorithmic approaches to users' news feeds. It was ultimately not confirmed whether this explanation was indeed provided by an IRB, but the dynamics depicted here show a realistic risk: that corporate data practices have a defining influence on research ethics involving related data.<sup>36</sup>

After contradicting statements regarding the IRB approval circulated, an email exchange between Fiske and journalist LaFrance was published in *The Atlantic*:

'When I asked Fiske to clarify, she told me the researchers' 'revision letter said they had Cornell IRB approval as a 'pre-existing dataset' presumably from FB, who seems to have reviewed it as well in some unspecified way... Under IRB regulations, pre-existing dataset would have been approved previously and someone is just analyzing data already collected, often by someone else.' The mention of a 'pre-existing dataset' here matters because, as Fiske explained in a follow-up email, 'presumably the data already existed when they applied to Cornell IRB.' (She also notes: 'I am not second-guessing the decision.')

This case highlights a grey area when it comes to informed consent in the era of big data. It still remains unregulated, and it is unclear whether users' approval of social media privacy policies is sufficient in order to morally justify using their data for research purposes (see Vayena and Gasser 2016, 25ff.; Rothstein and Shoben 2013; Ioannidis 2013).

Beyond this 'emotional contagion' experiment, big data and related research practices have been described as influential factors in recent debates concerning

informed consent. In response to the recent tendency to view informed consent as counterproductive, burdensome, and obsolete, Rothstein and Shoben (2013) provide an overview of the pros and cons pertinent to informed consent. Their article discusses the issue with particular regard to concerns regarding *consent bias*<sup>37</sup>.

The authors emphasise that, from a more practical viewpoint, the extent to which consent bias emerges has been frequently overstated. In addition, they highlight that individuals' trust in research acts as the main factor in counter-acting conditions that might lead to such bias. From an ethical perspective, they state that '[t]he argument that informed consent is incompatible with modern research represents an assault on the societal values on which biomedical research is based.' (Rothstein and Shoben 2013, 34).

Commenting on Rothstein and Shoben (2013), Ioannidis (2013) likewise stresses the potentially damaging consequences of compromised research ethics for the relationship between scientists and the public (Ioannidis 2013, 41). The author argues that attempts to dismantle informed consent are less related to consent bias, but rather motivated by new research possibilities enabled by big data. While such data were not collected for particular research, '[t]he exponential growth of electronic databases, suitable software, and computational power has made it very tempting to use such data for research purposes. If so, non-consenting people may even hinder research progress and undermine the public good' (Ioannidis 2013, 40). In fact, such an accusation and statement was made by data journalist Cukier with regards to not analysing data: 'Not using data is the moral equivalent of burning books' ('Not using data' 2016).

While this is of course an exaggerated, presumably deliberately provocative proposition, it illustrates a recurring line of argumentation and trope: opposing the use of big data is equated with hindering innovation. Comparably, arguments highlighting the relevance of informed consent from an ethical perspective are accused of obstructing possibilities for research. In turn, justifying the obsolescence of informed consent is necessary in order to pave the way for research involving certain kinds of big data. This justification is, for example, approached by highlighting the downsides of informed consent, such as consent bias. Furthermore, this is substantiated by framing material as 'pre-existing data sets', as illustrated with the aforementioned 'emotional contagion' experiment.

### Algorithmic Bias

Informed consent has been criticised for creating 'consent bias,' in turn suggesting that biases do not apply to big data. As already indicated with the notion of 'digital positivism' (Mosco 2015) and 'dataism' (van Dijk 2014), several authors have stressed that '[...] the ideological effect of big data is the denial of the existence of ideology and bias' (Baruh and Popescu 2014, with

reference to Cohen 2013). Despite this tendency, big data create new forms of bias relating back to the (often commercial) conditions under which they have been collected.

Commercial big data are retrieved from individuals that have the necessary resources, plus the skills and an interest, to use certain digital devices and platforms. Although collected in immense quantities, big data may still represent specific populations. Because individuals included in a big data sample tend to represent only those using an expensive/innovative technical device or service, these may be e.g. on average younger or above average physically active. This leads to selection (sampling) bias, also described as population bias (Ruths and Pfeffer 2014; Sharon 2016). Such bias implies that generalising claims based on big data, typically underlined with reference to the popularity of digital devices/platforms, should be treated with caution: the more exclusive (e.g. economically or due to required skills) a technology or platform, the higher the chances for population bias. Yet, '[d]espite these sampling biases being built into platforms used for scientific studies, they are rarely corrected for (if even acknowledged)' (Ruths and Pfeffer 2014)

Since Apple's *Research Kit* was released in 2015, it has been promoted as an efficient, effective possibility for recruiting study participants and collecting data. The Kit is targeted at medical researchers, allowing them to develop apps for iPhone users. These individuals may then take part in medical studies by using respective apps, thereby providing access to data tracked with their mobile devices. Apple advertises the Kit, to users, as follows: 'ResearchKit makes it easy for you to sign up for and participate in a study by using the iPhone that's already in your pocket. You no longer have to travel to a hospital or facility to complete tasks and fill out questionnaires.' ('ResearchKit and CareKit' n.d.). Moreover, it addresses researchers with the promise that '[...] the sheer number of iPhone users around the globe means that apps built on ResearchKit can enrol participants and gather data in bigger numbers than ever'. The implications of who uses and can afford these devices receive little to no attention in this context.

In their assessment of Apple's ResearchKit, Jardine et al. (2015) point out that '[t]he potential for bias is significant' (294). For researchers, this also implies that demographic data need to be collected and possible bias accounted for. Such a 'device-related' population bias may lead to a sample of users with specific demographics. As long as demographic limitations, e.g. with regards to generalisability, are taken into account and acknowledged, these are not necessarily problematic sample features (Chan, Yu-Feng Yvonne et al. 2017). But one should not forget that demographic characteristics are just the tip of the iceberg when it comes to potential bias.

As Baruh and Popescu show, certain users may entirely opt out of using particular services due to privacy concerns. This raises the issue that big data may systematically exclude certain groups for which these concerns are

characteristic. The authors highlight that the common ‘notice and choice’ frameworks of online platforms and their data collection:

‘[...] effectively rationalize market withdrawal for the privacy-conscious individual (the Awareness Paradox), while creating new power imbalances for the individuals that fully rely on the market-produced solutions. The withdrawal, however partial, from the market of those individuals highly intolerant of privacy violations only serves to further skew market signals by legitimizing the argument that ‘digital natives’ have different, laxer privacy expectations’ (Baruh and Popescu 2014, 14).

This argument has two main implications: First of all, little is known about the biases inherent to particular types of big data, especially those collected through corporate services such as social networking sites. Secondly, simply assuming that big data are indeed unbiased is inherently an ethical issue, since this promotes the social values derived from – potentially biased – samples. It is also related to the fallacy that the very fact that these data exist may be used as an argument that individuals should comply with how these have been collected.

Apart from the issue that these individuals have been given very little choice (Wessels 2015; Baruh and Popescu 2015, 8), the conclusions drawn from these datasets merely refer to those users who were willing (and able) to accept data collection conditions applying to a certain web service. As stressed in the abovementioned quote by Baruh and Popescu, this has an impact on the visibility and perception of certain moral values (see also Taylor 2017). While users’ compliance is framed as representative, those who are deliberately more privacy conscious, have more consequent attitudes, or experience less peer-/work-pressure concerning their use of a certain platform, are excluded from the data used to infer this assumption.

The described scenario refers particularly to the extreme case of non-users who entirely opt out of certain services, for example to avoid negative consequences for their privacy and autonomy (see also Oudshoorn and Pinch 2003). In addition, one needs to consider biases which may be fostered by the (algorithmic) conditions of platforms on which respective data were collected. This issue has been coined ‘filter bubble’ by Pariser (2011). With this term, the author/activist-entrepreneur calls attention to entanglements between users’ ‘search and click history’ on certain platforms and content which they are more likely to see in consequence. For example, depending on users’ interactions with content in their Facebook newsfeed, a person is more or less likely to encounter algorithmically curated content posted by certain actors.

Pariser also argues that this may have problematic consequences for the information diversity encountered by users. Effectively, over a longer time period, users run the risk of interacting with an online ‘echo chamber’: an

environment in which their political views, values, or emotions are more likely to be confirmed than opposed, and potentially more likely to be reinforced than reconsidered. This raises the issue of individuals receiving rather one-sided information on, for example, political events, as has been argued with regards to developments such as Donald Trump's election as US president, as well as the outcome of the referendum concerning the U.K.'s withdrawal from the European Union (Jackson 2017). In light of study designs such as the abovementioned emotional contagion experiment, it seems especially precarious that actors who are not affiliated with corporate data collecting entities such as Facebook may not receive unmediated insights into how this possibility is used and to what extent it may influence users' perceptions.<sup>38</sup>

These are crucial deliberations for thinking about individuals' (lack of) possibilities to access diverse content online, and how social media may contribute to the formation of opinions, decision making, and discursive participation. At the same time, they are also relevant for evaluating the data being produced under such conditions (Bozdag 2013). Because users are more likely to encounter certain content, it is also more likely that they will interact with this content. These interactions are documented and translated into data which are then potentially used as a basis for various analytical processes, e.g. to instruct corporate decisions or to conduct research (or both).

However, since algorithms influence what kind of content users may interact with, and impact the data produced, this also increases the likelihood of systematic biases (see also Baeza-Yates 2016). Scholars in software and algorithm studies have long been vocal on the point that the agency of such non-material technological factors needs to be accounted for (see e.g. Manovich 2013, 2011; Friedman and Nissenbaum 1996). These deliberations are likewise relevant for the data resulting from the interplay between users, algorithms, software, platforms and their potentially corporate providers. These kinds of bias are particularly challenging, since the relevant algorithms are commonly difficult to access, in part due to proprietary claims and their being in a constant state of (commercially driven) flux.

As Rothstein and Shoben emphasise in their abovementioned reflections on consent bias, bias is an inherent part of research and altogether unavoidable (2013, 34). It seems crucial to show that, and how, this also applies to big data, since arguments for its epistemic superiority have also been brought forward in order to undermine previous research values. As the authors aptly argue, it is not the realisation of consent bias which is new, rather '[...] what is new is the claim that it constitutes a justification for dispensing with informed consent in one or more types of research' (2013: 34).

Characteristically, these 'types of research' involve big data coming along with their own – commonly downplayed – biases. As shown above, such attempts at mitigating the relevance of informed consent ignore that it goes beyond matters of physical integrity, but aims at safeguarding personal dignity and autonomy. What has been described as 'digital positivism' by Mosco (2015) has a crucial

discursive function in this context: it manifests itself in claims for allegedly overcoming biases pertaining to more traditional data collection. But big data in fact introduce a complex entanglement of novel human-algorithmic biases.

In certain cases, for example, data generated on social networking sites such as Facebook or Google web search logs, the corporate interests in creating data are the main sources of bias, because they are decisive for the implemented algorithms. Therefore, a brief overview of the role of these interests will be covered in the final subchapter. Undeniably, this is a point which could be covered far more extensively, but it is not the aim of the following sections to provide a detailed evaluation of different data-driven business models. Instead, they are meant to examine some of the commercially grounded values related to big data in relation to research and public health information.

### Data Economies

Even before the emergence of so-called ‘Web 2.0’ services allowing users’ to create, publish and exchange content without having to rely on intermediaries, scholars had raised the issue of ‘free digital labour’ (Terranova 2000; see also Trebor 2012). In the late 1990s, online services such as the message boards and chats provided by America Online (AOL) involved users as ‘community leaders’ and administrators who monitored and maintained the quality of content and conversations.<sup>39</sup> Back then, users were charged based on an hourly rate (approx. 3,50€/hour in the early 1990s; see Margonelli 1999). Therefore, users’ unpaid, affective labour as leaders/admins contributed to the profit generated by the company, since these volunteers maintained content in a way which made it more attractive for other, paying users to access AOL. Similarly, customers of more recent services and social networking sites are crucial for creating commercial value, since they generate content which incentivises others to access a platform. This tendency has been hailed as ‘digital prosumption’ in business contexts (see e.g. Tapscott 1996) and was later on more critically described as a form of free labour (Terranova 2000; see also Fuchs 2011; Ritzer and Jurgenson 2010).<sup>40</sup>

Moreover, users act as a target audience for advertisements and additional services offered by tech corporations and their business partners. Users’ interactions with each other and with encountered content are crucial for determining what kind of content they will be offered. For instance, as Fuchs summarises: ‘Facebook’s users create data whenever they are online that refers to their profiles and online behaviour. This data is sold to Facebook’s advertising clients who are enabled to present targeted advertisements on users’ profiles.’ (2014, 14)

These kinds of targeted advertisements, and more generally content which is likely to facilitate users’ attention and contributions, are not limited to the platform through which certain data have been generated. Instead, as Gerlitz

and Helmond (2013) show, they take place in complex entanglements between various platforms and services. The integration of various social buttons and the Open Graph protocol foster 'back end connectivity' between platforms. What the authors describe as a 'Like economy' creates an online environment held together by social buttons: it combines decentralised data collection with recentralised analytics and economic valorisation (see Gerlitz and Helmond 2013, 1361).

While the data generated by users are crucial assets for technology corporations and their networked platforms, it has been critically discussed that corporations' data practices should be regulated more clearly. Common concerns pertain to privacy and the need for current legal frameworks to catch up with technological developments (Crawford and Schultz 2014; Andrejevic and Gates 2014; Tene and Polonetsky 2012). Given the criticism around corporate uses of big data, research involving these data likewise becomes potentially subjected to these concerns.

Big data-driven studies may not only inherit the biases fostered in commercial, online settings, but also involve complex interdependencies between research ethics, data access, corporate practices and norms (see also Zimmer 2010). One may argue that users' acceptance of platforms' use policies is sufficient to justify the negligence of informed consent, especially in light of citizens' proclaimed 'duty to participate' when it comes to ensuring societies' overall wellbeing (Bialobrzeski, Ried and Dabrock 2012)<sup>41</sup>. However, one should not conflate a person's deliberate participation in certain public health measures with their inevitable and involuntary generation of personal, digital data which have not been collected in line with considerations for the public good in the first place.

This is another context in which Lupton's (2014d) reflections on the interplay between digital presumption and the means by which users are addressed online with regards to personal and public health are relevant. The author argues that the commercial ideal of digitally engaged individuals has facilitated a 'digital patient experience economy' in which individuals' willingness to provide data on diseases and treatments has become morally valorised and even monetised (Lupton 2014d). This observation applies notably to patient experience and opinion websites, which require contributions from users. These developments are also reflected in a broader tendency to assume and morally expect users' readiness to contribute personal information in the form of big data for the (alleged) public good.

In conclusion, the broader issues and debates outlined in this chapter provide an overview of norms and values relevant to the use of big data, particularly in research. I have shown how privacy and security have been mobilised as a misleading dichotomy. Moreover, while privacy has been a major concern regarding big data practices, it was likewise used to justify the limited transparency on the part of actors involved in big data collection. The latter issue also points to described data asymmetries. Coming back to Habermas' idea of validity claims,

such aspects are relevant to negotiations involving claims to normative rightness as moral deliberations for balancing society's overall wellbeing and individuals' civic rights.

In addition though, validity claims to truth appear to play an important role, especially considering big data's alleged epistemic superiority and effectiveness. I have illustrated this with regards to informed consent and the issue of 'consent bias'. Arguments concerning informed consent as a source of bias act as validity claims asserting truth. In consequence however, it was stressed that these arguments also have normative implications and an impact on ethical deliberations. The alleged potential of big data to generate less biased results has been advanced as an argument challenging the reasonableness of informed consent. This ignores the fact that informed consent is *a priori* rooted in moral values such as autonomy and personal dignity. But just as importantly, what is neglected in these attempts at justifying the methodologies and ethics of big data-driven research are insights into the biases characteristic of big data.

This chapter therefore also demonstrates that validity claims grounded in truth and normative rightness are complexly interrelated in the discourse concerning big data-driven research and its ethics. Big data's 'digital positivism' (Mosco 2015) and claims for their epistemic superiority are ultimately highly normative. They are therefore implicated in ethical debates, especially when it comes to weighing civic, individual rights and societies' overall wellbeing. The crucial institutional and discursive conditions for such processes in the field of big data-driven health research will be explored in the following two chapters.

