Do Algorithms Dream of "Data" Without Bodies?

J Savirimuthu*

Pre-print accepted version

Always cite published version in International Review of Law, Computers and Technology 1-20 (20 pages) 15 Mar 2017

Abstract

The question whether algorithms dream of 'data' without bodies is asked with the intention of highlighting the material conditions created by wearables for fitness and health, reveal the underlying assumptions of the platform economy regarding individuals' autonomy, identities and preferences and reflect on the justifications for intervention under the General Data Protection Regulation. The article begins by highlighting key features of platform infrastructures and wearables in the health and fitness landscape, explains the implications of algorithms automating, what can be described as 'rituals of public and private life' in the health and fitness domain, and proceeds to consider the strains they place on data protection law. It will be argued that technological innovation and data protection rules played a part in setting the conditions for the mediated construction of meaning from bodies of information in the platform economy.

Keywords: Algorithms, Data Protection, Health, Privacy, Platforms, Wearables

I. Introduction.

The question whether algorithms dream of 'data' without bodies is not intended to anthropomorphise software. It is asked with the intention of highlighting the material conditions created by wearables for fitness and health, so as to reveal the underlying assumptions of the platform economy regarding individuals' autonomy, identities and preferences and ensure that the justifications for intervention under the General Data Protection Regulation 2016 ('GDPR') are carefully scrutinised. The mediatisation of health and fitness through affordances such as software applications ('apps') and self-tracking devices undoubtedly raises important questions about security, design and their

* Senior Lecturer in Law, School of Law and Social Justice, University of Liverpool. E-mail: jsaviri@liverpool.ac.uk

responsiveness to customer sensitivities such as consent, and expectations that processing of personal information is fair and legitimate. One important issue that must be considered is whether the blurring of boundaries between analogue and algorithmic computation of meaning relating to bodies of information in platform infrastructures requires additional strands of understanding to ensure that analysis of concepts such as profiling and automated decision-making are given greater regulatory emphasis. This immediately raises the related question whether the long-established distinction made in data protection law between personal data and non-identifiable data, which relied on boundary management norms and with an eye towards constraining information processing pathologies in State and commercial contexts, can continue to provide a coherent framework for regulating algorithmic construction of individual's digital identities, behaviour and preferences in health and fitness domains. The article begins by highlighting key features of platform infrastructures and wearables in the health and fitness landscape, explains the implications of algorithms automating, what can be described as 'rituals of public and private life' in the health and fitness domain, and proceeds to consider the strains they place on data protection law (Papacharissi 2015, 10). It will be argued that technological innovation and data protection rules played a part in setting the conditions for the mediated construction of meaning from bodies of information in the platform economy. If data protection rules are to provide a democratic and sustainable system not just for corporate elites, there is an urgent need to reassess how best a just and democratic society can benefit from the lexicon of classification, standardisation and reification of persons by the algorithmic hand driving the platform economy - *l'esprit algorithmes*.

II. Health Platforms and Fitness Wearables Infrastructure.

One way to grapple with the significance of platform infrastructures and wearables in structuring individuals' personal information for our understanding of data protection policy-making would be to reflect on its technological, computational and social layers which not only provide the 'building blocks of social action' but also define the contexts within which agency is experienced (Couldry and Hepp 2016, 141).

A. Nature of Health and Fitness Platforms and Wearables.

Platforms are the latest iteration of corporate actors, technological innovators and health organisations, harnessing the value of infrastructures and data processes to structure

economic and social relations. The following description of platforms provides a useful commencing point for the analysis to follow:

> Technologically speaking, platforms are the providers of software, (sometimes) hardware, and services that help code social activities into a computational architecture; they process (meta)-data through algorithms and formatted protocols before presenting their interpreted logic in the form of user-friendly interfaces with default settings that reflect the platform owner's strategic choices. (Van Dijk 2013, 29)

Van Dijk's account of platforms is illuminating in two ways. First, it draws attention to the importance of not restricting our understanding of technological infrastructures to the *form* and *content* of interactions taking place within these environments for communication. As sophisticated software technologies enable platforms to identify, classify and evaluate information generated in these spaces, an understanding of *how* and *why* technological and design infrastructures make remediation possible are equally important to understanding the role of the GDPR in grappling with algorithmic decision-making. Second, this framing of platforms complements Hildebrandt's observation that analytically, infrastructures also reinforce new forms of technological, cultural and economic logics which go unnoticed and the risk this poses for the rule of law (2015, 179–181). Consequently, understanding the interplay of automation, networked knowledge and calculated publics becomes relevant since control over information flows has consequences for individuals in the way autonomy and agency are exercised. Platform infrastructures, to extend van Dijck's insights, may be viewed as spaces of computed sociality where individuals are provided with affordances and tools in embodied contexts (Tempini 2015). Platforms are therefore not simply friction-free spaces for connectivity bridging online and offline environments, but they also construct contexts through which individuals now view their agency, experiences and interactions within a social and cultural milieu. Quantified self-communities, patient advocacy groups like PatientsLikeMe and communities of fitness-tracking enthusiasts are contemporary examples of networked publics made possible by technological infrastructures, enabling individuals and communities to be readily connected anytime, anywhere and from any device (Gilmore 2015). Health service providers make available to users a centralised portal of resources, which can be accessed

easily through convenient web interfaces and mobile interfaces.[1] Platforms also provide new participatory and collaborative opportunities, as costs for collection, storage and use of data are reduced. Archives and data sets provide repositories for reducing storage, search and information costs and the efficiencies generated help create and sustain collaborative partnerships for research, investment and innovation. Platforms such as the HealthSuite owned by Philips Healthcare's illustrate how platform ideas and logic contribute to the automation of information flows, development of networks of collaboration between manufacturers, suppliers, health professionals and patients and use of personal data.

Wearable technologies merit consideration in the discourse on platform economy and agency, as sensor technologies, smartphones and mobile broadband speeds provide continuous interconnectivity, bringing together the digital economy, health and fitness eco- system and the practice of everyday life. Wearable technology can be defined as devices which incorporate sensors and smart technologies and can be worn on the body or integrated into clothing (EDPS Opinion 4/2015, 7). Wearables are sociotechnical affordances, which enable individuals as well as patients with opportunities to gain insights and understanding of their bodies and social and environmental conditions. User interfaces are designed to mobilise individuals and create another stream of information flowing through the technological infrastructure. With the domestication of wearable technologies, health organisations such as the NHS and corporate actors such as Apple, Google, Samsung, Fitbit and Garmin have seized societal desire for self-knowledge, measurement and personalisation to promote a culture of well-being and commercial goals, respectively. Technologies for tracking and measuring emotional, biological and physical conditions also make possible large amounts of data as a resource for innovation, research and the delivery of personalised healthcare (NDG 2016). Corporate actors, on the other hand, have aggressively promoted health platforms and wearable technologies as lifestyle-enhancing opportunities. Agency, access to networked publics and benefits of crowdsourced knowledge form the spine of marketing and advertising campaigns in shaping societal and consumer expectations. These opportunities are realised in many of ways. Context-aware mobile technologies used in monitoring patients or for recreational and fitness purposes illustrate how miniaturised electronics and sensors enable information about the user's

[1] See Kingsfund, The Future is now. Available at https://www.kingsfund.org.uk/reports/thefutureisnow/ (accessed 3rd December 2016).

state of mind, activity and context to be easily collected and used to generate valuable insights (FTC 2015). Smart devices such as Jawbone Up 2, Fitbit Charge HR, Garmin Vivosmart are now equipped with processing functionalities that provide individuals with control over their personal information and extend opportunities for managing personal goals and lifestyles (Hilts, Parsons, and Knockel 2016, 19–20). Katz's description of wearables as evolving into cultural 'accoutrements to our self-creation and symbolic interpersonal communication' is a commonly held view of modulated spaces of information flows which are transforming the health and fitness landscape (2003, 315–318). To better articulate why platforms raise data protection challenges, an account is needed of how individual's understandings and expectations of agency become institutionalised as a condition for participation in these communication spaces.

B. The Platform Economy for Health and Fitness.

The platform economy for health and fitness cannot be meaningfully segregated from the data economy or offline platforms, which is estimated to have contributed €430bn to the EU economy in 2012 (Copenhagen Economics 2013). The European Commission announced that the platform economy, which includes services mediated by apps, would generate more than €63bn and very likely provide a boost to the European economy.[2] This is a conservative estimate of the value of markets for personal data for two reasons. First, the value of the EU data economy was estimated at 1.85% of EU GDP in 2014 and growth forecasts of 5.6% per annum are anticipated for subsequent periods. Second, one objective of the GDPR is to facilitate free flows of information and mobilise data subjects as economic actors in the digital economy. These developments will not only generate multiple streams of information flows for personal data markets, but also provide an important resource for innovation and development (COM (2017), 9 final 3–4). The next generation of health and fitness platforms and devices, with over 30 billion sensors becoming integrated into the Internet of Things, will have tangible societal and economic ramifications (COM (2016), 180). The National Data Guardian has identified sharing of data and communication platforms as being central to the delivery of an efficient and high-quality connected health care in the public health sector (NDG 2016). Three trends in the health and fitness domain should be noted. The work undertaken by MindTech Healthcare

[2] See generally European Union Committee Online Platforms and the Digital Single Market http://www.publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/12902.htm (accessed 3rd December 2016).

Technology Co-operative serves as a useful barometer of the future of data-driven operations in the connected health terrain. A feature of data-driven operations is the integration of multiple stakeholders into the spaces of information flows so that each is able to access and extract value from personal data. The Co-operative, for example, comprises an assemblage of manufacturers, patients, clinicians, retailers and suppliers who are part of the mental healthcare and dementia infrastructure providing timely therapeutic interventions as well as providing networked services and support across the data value creation chain. Google DeepMind and Moorfield's Eye Hospital's well-publicised collaboration in analysing digital eye scans illustrates another important trend of the logic driving information flows – before value can be extracted, data have to be collected and subsequently transformed by algorithms into information and knowledge to further the objectives of infrastructure providers.[3] Finally, the growing influence of corporate power in these domains in harnessing value from personal data should not be overlooked. Start-up investments from Silicon Valley are now being channelled through investment and funding activities, acquisitions of content and communication service providers and emergence of collaborative partnerships (Casper 2013).

Since data protection laws have long elevated individual's autonomy, agency and choice, two vignettes will be used to illustrate how data-driven operations redefine individuals' agency (Cohen 2016, 62–63). First, John uses Strava, the popular cycling and running fitness app and wearables. He purchased the wearable after reading reviews about Strava on blogs, was impressed by marketing advertisements extolling the benefits of improved personal fitness and was keen to interact with other users on social media. John regularly tracks his bike rides and runs via his iPhone or GPS device. He also posts information regarding the distances covered and activities completed on the website and regularly compares these with performances of other users. John receives push notifications on his laptop and smartphone. Second, Colin suffers from serious bouts of forgetfulness and is recovering from a triple heart bypass surgery. He uses an activity-monitoring device, which alerts him to any prolonged period of inactivity or failure to take his medications. Colin is an enthusiastic user of social media and frequently tweets information relating to his health condition. He regularly updates his profile on the national patient portal and participates in discussions on the secure site made available for users of the activity-monitoring device.

[3] See http://www.moorfields.nhs.uk/news/moorfields-announces-research-partnership (accessed 3rd December 2016).

Three observations can be made regarding the mediated construction of participation and communication. First, interactions between platforms and individuals are determined by information collected in these constructed spaces. Tools and affordances are made available to individuals so that control can be exercised over which information becomes visible and shared within the networked environment via social media. Privacy settings and customisation tools and affordances provide individuals with control to allay concerns about privacy. There is another perspective. From a commercial or goal-oriented strategy, participation in this environment is conditional on cultural acceptance of rules relating to the collection of personal information. This ordering of relations has significant consequences for individuals' expectations of how they exercise and experience their autonomy and agency (Langlois and Elmer 2013, 14). Acceptance of the rules triggers a chain of data processing operations. Monitoring of individuals' activities is maintained through emails, web surveys, promotional communications and feedback portals. Platforms and wearables also enable information to be collected automatically. The reasons how and why this is important will be developed later but it can be observed that the automatic collection of information during registration and visits to the website and resources accessed are presented as measures to enhance customer experience and provide high-quality services. Second, platforms subject volunteered and automatically collected data to processes that continuously extend the life cycle of personal information through automated decision-making and creation of user profiles (LIBE 2015, 19). Apart from the use of accessible interfaces and other functional affordances as conduits for collecting personal information, push notifications ensure that individuals' daily activities are synchronised with the goal of the platform, which is to sustain information flows. Push notifications, such as alerts, emails and real-time updates on the actions of others are haptic instants intended to orient or nudge the user towards embracing norms of visibility, sharing and participation (Gilmore 2015). Patients such as Colin experience haptic instants differently. Real-time monitoring and alerts enable technologies to bridge time and space and erode boundaries between 'human' and 'algorithmic' agency in decision-making. Both accounts of haptic instants highlight what Langlois and Elmer describe as the act of redefining communication, through data mining processes which 'seek to enhance, format, encode and diagnose communication' (2013, 14). The flows of bodies of information from users to companies or organisations providing infrastructure services are vividly reflected by Helmond's metaphor of platforms as 'pouring data systems that set up data channels to enable data flows with third parties' (Helmond 2015). Crucially, users remain oblivious

to these back-end operations. Business models of leading global companies such as Apple, Microsoft, Fitbit, Atheer Labs and Nymi use back-end systems to process digital footprints and link these with data purchased from information brokers, and information stored in data sets to optimise data (Hilts, Parsons, and Knockel 2016). To be able to monetise data, platform providers enframe communication which is akin to the creation of *sui generis* proprietorial-type rights over personal information. It is the next insight which is particularly helpful to understanding the significance of the relationship between algorithmic processes of decision-making and platforms.

Much of the recent focus on the platform economy resembles familiar debates which revolve around the economic logic of rationality, efficiency and innovation (Evans and Gawer 2016). There is a deeper issue other than the fact that platforms are now regarded as knowledge-generating structures that transcend the biopolitical (Boyd and Crawford 2012, 663). Health and fitness platforms are not simply infrastructures of economic logic and social utility but in the context of the platform economy, also one of computational grammar. Algorithms analyse input data as 'digital objects' at three intersecting levels: the textual or semantic elements, affordances used and an algorithmic lexicon that generates insights, information and knowledge from bodies of information so that value can be extracted (Langlois and Elmer 2013, 11–13). What we are concerned with here is not just the construction of meaning from textual or semantic information but the 'nontrivial extraction of implicit, previously unknown, and potentially useful information from data' to generate new knowledge, hypothesis and patterns based on design choices that convert behaviour, identity and preferences of individuals into digital code (Frawley, Piatetsky-Shapiro, and Matheus 1992, 58). Agre's account of algorithmic logic is particularly helpful in drawing attention to how and why algorithmic conversion of bodies of information into computer code needs to be taken seriously by policy-makers notwithstanding the benefits for enhancing public health and innovation (1994, 105–112). The process of data capture, aggregation and value extraction, he observes, is structured by a 'grammar of action' which is contingent on questions identified by the processor and goals to be attained (Agre 1994, 116). The transformation of information into software code leads to the construction of what Esposti describes as the digital self, whereby the life cycle of personal data is gradually layered by feedback loops and continuously aggregated with data from multiple sources in the value chain (2014, 212–213). The important consequences for human agency will be elaborated in the next section.

C. Conclusion.

Imperceptibly, the everyday practice of life, whether by visits to the hospital, recording of blood and glucose results, interactions on social media or achieving personal targets in sporting activity end up with reality being constructed autonomously, with little or no effective regulatory or individual oversight (Turow, McGuigan, and Maris 2015, 475– 476). Data protection rules could arguably be seen as a framework that anticipates such problems by appealing to data controllers to exercise restraint, on the one hand, and data subjects urged to exercise their agency and information rights, on the other. Its genealogy may shed some light on why corporate actors tend to view the law's ordering of information relations and broad information processing principles as business as usual.

III. The General Data Protection Regulation and Mediated Construction of Bodies of Information: Framing the Data Protection Challenge.

'In the face of this dramatic revolution taking place in our societies, Silicon Valley tells us that everything will be fine…They dictate their rules to us…The hard currency of the digital age is, as it were, being filched from our pockets without our even noticing. This process has been going on so surreptitiously and for all practical purposes without regulation that these businesses are now the biggest undertakings in the world.' (Albrecht 2016, 473-474)

Albrecht's concerns could be dismissed as mere rhetoric, but it does not detract, however, from the unease felt by many that data protection rules are being increasingly used by data controllers towards realising economic and commercial goals and leave individuals exposed to the erosion of their privacy and information rights (Acquisti 2009, Solove 2013). An examination of the paradigmatic series of questions – *what* type of data, by *whom*, for *what* purposes and for *how* long – that informs the balancing of interests between individuals and organisations may provide us with the beginnings of an under- standing of the challenges posed by data mining practices and platforms (Fuster 2014; Lynskey 2016). However, to fully understand Albrecht's concerns and the issues raised by the metaphor used at the outset in the article, a shift in perspective may help broaden the narrative frequently encountered in data protection discourse. We can rephrase the inquiry which frames the article simply: what obligations do data protection law impose on data

controllers in their use of algorithms for analytical and predictive purposes in the platform economy? This question now takes on particular significance under current GDPR rules should data controllers assert: (i) no personal data is being processed; (ii) personal data has been manifestly made public by the data subject; (iii) explicit consent by the data subject has been obtained or that (iv) measures to safeguard the data subject's rights and legitimate interests such as privacy by design, de-identification and anonymisation are in place, particularly where automated decisions including profiling have taken place. The following discussion will not rehearse long-standing debates in data protection law of its normative foundations or the predatory data mining practices of corporate actors but will proceed instead to indicate those aspects of data governance easily overlooked and which now needs to be re-assessed in the context of the platform economy. Owing to limitations of space, the impact of the GDPR on public health and biomedical research will not be examined, but this will not detract from the line of reasoning advocated, which is to assess the significance of platform logic for three areas: personal data, rules defining data controllers' obligations and profiling.

A. The Rationale of Dual Objectives.

Article 1 sets out two objectives of data protection law, which is to provide rules for the free movement of personal data and the protection of individuals' fundamental rights including the right to the protection of their personal data. Since data protection rules define how personal information is accessed and used, the balance to be maintained between the dual objectives in the communication spaces mediated by technologies has become an important policy consideration when accommodating the interests of data controllers and data subjects (EDPS Opinion 4/2015, 9). The Article 29 Working Party ('Article 29 WP') in its joint statement has no doubt as to the scale of the challenges technological infrastructures pose for the operation of information rights and obligations in the networked environment (WP227 2014, 2–4). Data protection rules operate in an environment ultimately constructed by private actors with clearly defined expectations about the role and value of personal data. Data protection rules not only enable personal information to be commodified, but also more significantly, structure expectations regarding parties understanding of their information rights, responsibilities and duties. Processing of personal information, for example, is permitted if an activity meets one of six grounds set out in Article 6. The rules also formulate a set of fair information collection and processing principles which urge restraint by data controllers, requiring them, for

example, to access and use only minimal information necessary for the purposes for which they were collected and retained for a period no longer than required (Article 5). Explicit consent is needed when sensitive and health data are processed together with some procedural and technical requirements that must be met as a precaution to minimise risks to data sub- jects (Article 9, *Bodil Lindqvist*). To minimise risks to data subjects, data controllers are encouraged to adopt technical solutions such as encryption, anonymisation and pseudonyms. Within this framework, individuals are provided with a set of information rights which enable them to exercise some control over how their personal information is used, such as mechanisms for access, disclosure, objection and rectification (Articles 12– 19). The GDPR also provides data subjects with exit rights in the form of a right to portability (Article 20). Processing activity which involves anonymised data or data that is not personal is not covered by the GDPR. Data protection law also provides mechanisms for redress in respect of the collection, processing or use of personal data (*Google Spain*, *Digital Rights Ireland*, and *Schrems*).

The brief account serves to illustrate how data protection rules map onto the dual objectives and should bring to the surface the complex policy challenges and tensions that underpin Albrecht's concerns. It also makes clear the policy presumption of reducing barriers to the free flow of information and exceptionally, economic interests will be displaced if erosion of a user's personal information is seen to be of a nature warranting intervention, as the Court's observation in *Google Spain* makes plain:

> in light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing. (para. 81)

Finally, it may be useful to recall that historically, the importance attached to the complementary role of dual objectives in data protection law represented a policy innovation designed to reflect the emergence of an information society. The public and private sector assumed important roles as repositories for collecting, aggregating and processing large amounts of information (Hustinx 2014). Directive 95/46/EC, the predecessor to the GDPR, mirrored a regulatory culture focused not only on minimising constitutional threats to citizens but also on the need to create a flexible regulatory framework that would enable Internet intermediaries and businesses to help realise economic and social objectives (OECD 1980, Commission 2003). However, the platform

economy we are concerned with poses some unique challenges not previously encountered. The networked society today by all account bears very little semblance to the way economic and social activities were conducted during the early period of the 'read-write' web (Hustinx 2014). Every sphere of economic, political and cultural activity now revolves around the collection, linking, sharing and use of personal data within a value creation chain (COM (2015), 192 final para. 5). Increasingly, individuals are having to accept stringent terms regarding the processing of their personal data (EDPS, Opinion 8/2016, 11– 13). Data-driven systems are enabled by infrastructure architectures which are interoperable and enable personal data to be accessed and used by different actors for a wide range of purposes. Advances in technologies for collecting and repurposing of personal information have now accelerated efforts to develop regulatory solutions in response to the impact of data collection practices on individual's fundamental rights (Article 29 WP, Opinion 6/2014, 17, Opinion 8/2014, 6–8, Opinion 3/2016, 5–6). Public perception seems to be that the scale of collection and reuse of personal information is driven very much by economic and commercial imperatives (LIBE 2015, 14–16). Notwithstanding these developments, the ruling in Google Spain probably serves as a reminder that even though there is consensus on the value of pursuing the dual objectives, there is, however, less agreement on the measures and mechanisms for bridging data protection theory and practice, on the one hand, and articulating a vision of a digital economy that does not marginalise the fundamental rights of individuals, on the other (EDPS Opinion 4/ 2015, 14).

B. Personal Data, (Meta) Data and the Digital Self.

The GDPR rules apply to designated activities which involve the processing of personal data of natural persons unless one of the stated derogations apply (Recitals 18–20 and Article 2). The protection of personal data is regarded as a fundamental right (Recital 1, *Promusicae*). However, it is not an absolute right and 'must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality' (Recital 4, *Schecke* para. 86–88). The question whether personal data is processed is crucial to triggering the rules under the GDPR. Personal data is described as 'any information relating to an identified or identifiable natural person' (Article 4(1)). Personal information that has been anonymised, in the sense that the data subject is no longer identifiable, will not be covered by data protection rules. Furthermore, data protection rules do not apply to the processing of anonymised information

undertaken for statistical or research purposes. The GDPR now clarifies the scope of 'personal data', which extend beyond physical, physiological, mental, economic, cultural or social identifiers and imposes obligations on data controllers to ensure that they introduce design solutions safeguarding individuals' personal information (Article 38, Article 29 WP Opinion 3/2016). This is particularly relevant to the context of growing dominance of corporate actors in the health and fitness domain, as a wide array of personal information can now be accessed and distributed by actors in the platform's value chain (e.g. location data, online identifiers and mobile device identifiers) (Article 4(1)).[4] Information collected from Jack *via* an app, the wearable device or uploaded onto the platform would be regarded as personal data. Raw sensor data which enable conclusions to be drawn about Colin's health status or health risks would similarly be regarded as coming within the scope of sensitive health data. It is arguable that lifestyle apps that enhance an individual's fitness could be regarded as health enhancing and data collected from users' devices would be covered by data protection rules (Article 29 WP, Opinion 2/2013).

One type of data that merits closer scrutiny is the status of unstructured bits of data collated from upstream and downstream data operations, which may or may not be combined with 'personal data which are manifestly made public by the data subject' to generate new insights on aspects of an individual's behavioural, health or cognitive conditions (Article 9(2)(e)). Much of the contemporary discussions, inspired in part by Westin's argument that individuals have a right to self-determination regarding their accessibility to the public, have been aligned with understandings of theorising the relationship between technologies and information in terms of ownership, confidentiality, informational privacy or the 'right to be left alone'. Additionally, the nature of personal data has become an area for claims and counterclaims about the effectiveness of privacy by design, de-identification, encryption, pseudonyms and anonymity measures (Article 29 WP, Opinion 2/2013, 5–6, Article 29 WP, Opinion 4/2007). At the root of these debates is an etymological one – is data the same as information? Bygrave, for example, regards this as a relevant question, since many of the protections available to data subjects and obligations imposed on data controllers are unlikely to be available when information processed is not regarded as personal data (2010). The etymological conundrum also raises a technical issue, namely whether personal information which renders an individual directly

[4] See Guidance issued by Article 29 Working Party for DPO's http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

or indirectly identifiable can be de-linked to enable data to be processed. The implication here is that data, information and knowledge can be viewed sequentially as beginning from a state of namelessness to one where identification or identifiability becomes possible (Zins 2007, 486–489). The state of namelessness is an attractive idea if we recall Nissenbaum's suggestion that this sets limits to the reachability of individuals (1999, 142– 143). To take a simple example, 1325001 would seem to achieve the status of namelessness and data coupled with the identifier would be regarded simply as data rather than information that identifies an individual. What if extraneous anonymised and unrelated data is introduced which links 1325001 to Jack, the fitness enthusiast? The Strasbourg Court's ruling in *S and Marper v UK* (2009), may provide some clues on how the question could be answered. The question before the Court was whether DNA samples of persons suspected of breaching the criminal law, collected and retained by police in a database was 'personal data' rather than data that identified an individual. The case was decided in favour of the complainants under Article 8 of the ECHR. One argument made before the Court was that unstructured bits of code such as DNA samples were themselves not personal data, since individuals only became identifiable if material collected from a crime scene was introduced and a match produced. This argument was rejected. Bygrave is perhaps right to question the line of reasoning that regards data and information as synonymous, even though the *travaux préparatoires* does not provide any clear guidance in this regard (para. 68 and 76). That said, when the case was previously heard in the House of Lords, Baroness Hale's observation may give us a sense of the reason why data protection law discourse appears to treat data and information as interchangeable. It was observed that an argument that relied on distinguishing 'raw' data from information derived from data was questionable, as the primary consideration for collecting the sample data in the first instance was 'for the information which they contain' ((2004) UKHL 39 para. 70). Though scholars in informatics may question this view, if this observation is correct, the idea of reachability may be relied upon to extend the obligations of data controllers to data subjects in the age of Big Data (Mittelstadt 2016). The reachability argument could also be used to support Borgesius's analysis of the rationale of the GDPR's innovative intervention, which ensures that individuals singled out by information systems will now continue to be protected (2016). The idea of reachability may be particularly relevant when we turn to the role of algorithms in creating profiles based on structured and unstructured data even though the real-world identity of individuals remains hidden or unknown (Recital 26). More significantly, the ruling in *Marper* reminds us of how knowledge structures that have

underpinned our approach to issues of identification and identifiably may now need to accommodate the fact that digital technologies are now transforming the way machines enable individuals to be easily reached and digital selves created by algorithmic knowledge-generating structures (Berry 2011, 5).

C. Interaction between Fair, Lawful and Consent Principles.

Bygraves describes data protection law as being founded on core principles that are coherent and whose instrumental value lies in the provision of 'guiding standards during interest-balancing processes' (Bygrave, 2002, 57). Data protection rules derive their legitimacy from the social contract tradition and its internal coherence and rationality creates a principled basis for binding data subjects and data controllers to the authority of law. At first glance, the fair information collection and use principles can be said to entrench default positions that enable personal information to be processed without compromising the information rights and expectations of individuals (Article 29 WP Opinion 03/2013). Article 5, for example, provides a cluster of values intended to serve as a guide to the standard setting role for information processing activities by defining in advance the discretion available to data controllers. The GDPR also provides data subjects with the right to withdraw their consent, access personal information held by data controllers and even object to retention, distribution and subsequent use (*Google Spain* and *Schrems*). Proportionality, purpose limitation and transparency continue to be regarded as an important part of the regulatory toolkit for restraining predatory data mining practices (Article 29 WP Opinion 03/2013, 11–14). Any expectation that fair information collecting principles would promote consumer trust or that a market for privacy would emerge in tandem with the personal data economy may have been dampened by a grim reality (Article 29 WP Opinion 8/2014, 4).[5] The default positions which safeguard data subjects' interests have been shifted by data controllers to reduce barriers to extracting value from personal data (Article 29 WP Opinion 03/2013, 35). Pattern recognition algorithms which subject vast amounts of personal data to analysis also highlight the growing lack of transparency in data-driven operations. These practices also raise questions about the legitimacy of the type of algorithms being deployed, the predictions being made and the impact of bias, inaccuracies and errors on individuals (Kotthoff 2014, 57). Given that consumers of

[5] See for example privacy concerns with NHS Health's free apps library http://bmcmedicine.biomedcentral.com/articles/10.1186/s12916-015-0444-y and data sharing concerns raised by mobile apps http://techscience.org/a/2015103001/. Accessed 3rd December 2016.

platform services and wearable devices have considerable knowledge and resource constraints, data protection rules are particularly wanting in curbing information pathologies *ex ante*. This shortcoming furthermore obscures a more significant consequence for individual's expectations of how their personal information is processed and used. Article 6(f) together with contractual arrangements between data controllers and data subjects, grounds fundamental rights claims within market-oriented mechanisms (Raab 1999, 75–76; Article 29 WP, Opinion 6/2014, 23–43).

Finally, the continued role and value of consent in technologically mediated environments have been placed under immense strain in the networked environment (Hildebrandt 2008). A combination of apathy, difficulty in grasping information practices in privacy policies, assumptions regarding data controllers' compliance and lack of enforcement have contributed to considerable consumer anxiety and mistrust (Sweeney 2013). There is another issue. Treating explicit consent as separate from obligations of fair and legitimate processing places the onus on data controllers to supervise their behaviour and avoid 'gaming' data protection law. The accountability gap is also exacerbated by the fact that it is burdensome, if not impossible, for individuals to continually manage and monitor their interactions and digital footprints. It is true that while consent from individuals can be obtained either expressed or implied, Article 9 implements additional prescriptive requirements where personal sensitive data is processed. However, not dissimilar problems of choice, lack of understanding and imbalance in bargaining power continue to be encountered. Consent, for the purposes of the health and fitness domain, is one of the grounds for legitimate processing under Article 6(f) and Article 9. Data protection rules, well intentioned though they may be, too readily assume that data controllers are incentivised to act in a manner that aligns their expectations with the interests of data subjects. Manufacturers of wearable devices such as Fitbit now join the list of platform and service providers that:

> alter practice and sometimes pull norms and standards along with them ... and reconfigure ontologies ... [and] define ethical and political precepts. (Nissenbaum 2015, 160)

The emerging conception of agency in technology-mediated environments suggests that the right to self-determination is far from being an effective mechanism for curbing corporate actors overreaching their processing activities (EDPS Opinion 4/2015, 11–13).

If any headway is to be made in this area of policy-making, three assumptions that underpin the liberal view of consent as a benchmark of agency and autonomy must be confronted. First, that users of wearables and health platforms can define *a priori* what type of information can be accessed and by whom. Second, related to the first is the logistical and technical challenge for users to discover if fair processing principles have been breached. Third, the right to self-determination assumes that individuals can make assessments about inferences that can be drawn either from individual tweets, posts or when these are linked with information to their data trails. Taken together, any sense that information is relational and expectations are justiciable are winnowed by *ex post* remedial sanctions and unmonitored back-end data-driven operations. As Cohen observes, the governance dilemma encountered in the platform economy is not Orwellian but that of overcoming an entrenched vision of an information society being sustained by 'an atmosphere of regulatory lenity' (2016, 62).

D. Data without Bodies, Automated Decision Making and Profiling.

"Chat Bot Message: Hi Aisha. If your thoughts turn to a Romantic Weekend, don't forget we can provide you with some really nice champagne. We also have some decadent chocolates and cakes. Before I forget – congratulations on your engagement!"

The vignette provides a relatively simple view of interactions in spaces constructed by communication infrastructures (Bowers and Rodden 1993). Algorithms, platforms and communication spaces have become so much a natural part of our daily lives that we cease to notice them and underestimate their far-reaching influences on our expectations and choices (*cf.* Weiser 1991). A recurring sub-theme of this article is that the materiality of conditions now makes it difficult to ascertain the boundaries between machine and human agency. Albrecht's desire to reshape the normative contours of corporate dominance within a constitutional domain should also be understood in terms of how data protection rules sustain and internalise 'algorithmically rendered materiality' (Papacharissi 2015, 119). Boundary management is important, as it enables individuals to define and control access to the self. To contextualise key provisions in the GDPR that address automated decision-making and profiling, we need, however, to look beyond the interactions between human and computing technologies. Focus should instead be directed towards the role of algorithms in structuring and defining how individuals now interact with information and experience their environment. Significantly, it is through interactions with information that

experiences are framed and amplified. These thoughts will inform the subsequent analysis of Articles 21 and 22 of the GDPR.

Profiling, which comprises the output of the automated algorithmic process, involves pattern recognition and n-gram modelling for predictive or assessment purposes based on volunteered, observed and cloud sourced data. Individuals such as Jack, Colin and Aisha, as subjects of information rights are, for example, provided with mechanisms under the GDPR to object to processing of personal information should profiles of their behaviour and preferences be created (Article 21) but only when data controllers' lawful authority is dependent on the argument that such form of processing is necessary in attaining the legitimate commercial interests of the controller or third party (Article 7 (f)). To be entitled to a successful claim under this provision, when data subjects are made aware of this practice taking place, they must show, however, that the profiling has seriously undermined their fundamental rights (*Digital Rights Ireland*). Data controllers can, of course, provide evidence of an audit of the algorithm to show why the legitimate interests or the fundamental rights of the data subject have not been overridden. Data subjects, it should be said, still retain the right to object to any direct marketing which may be based on their purchasing activities, behaviour and interests (Article 21(2)). Unlike Article 21, Article 22(1) prohibits automated processing, including profiling which produce legal effects or is likely to produce a significant outcome for data subjects. Article 22(2) provides some limited exemptions to the prohibition. Explicit consent or automated decision-making necessary to facilitate the contractual performance between the data controller and data subject are two such examples. In such cases, Article 22(3) imposes obligations on data controllers to implement suitable measures which safeguard the rights of data subjects (i.e. privacy by design, principles of minimisation and proportionality and limited retention). Finally, article 22(4) stipulates that automated decision-making, including profiling involving sensitive categories of information such as those relating to aspects of an individual's health, political, religious beliefs and race are prohibited unless explicit consent has been obtained or public interest warrants the adoption of the measure (Article 9(2)(a)(g)), in addition to suitable safeguards protecting the legitimate interests and rights of the data subject being provided. Apart from the measures to safeguard data subjects indicated above, data controllers could, for example, satisfy this requirement by providing data subjects with a redress mechanism such as the opportunity to express their views to an authorised person. To ensure that data subjects are made aware of automated decision-

making practices, data controllers must provide data subjects with meaningful information about the logic as well as any significant consequences resulting from the profiling and automated decision-making process (Article 13(2)(f)).

Scrutiny of algorithms and their central role in data-driven operations will continue to gain increased attention from policy-makers. It seems bizarre that whereas democratic power structures in society, such as property, institutions and law, are not impervious to scrutiny and oversight, algorithms operating as technological rules of making up people from data seem to have been accorded the 'immense privilege of invisibility' (Ackerman 1980, 4). Algorithms have been problematised in terms of the 'opacity' of back-end processing activities (Burrell 2016), agents for automated veridiction (Fourcade and Healy 2016, 16), mathematical constructs of mirror worlds (O'Neill 2016) and personalisation agents (Turow, McGuigan, and Maris 2015). Article 22(1) can also be regarded as a regulatory intervention aimed at encouraging data controllers to introduce greater transparency by explaining the logic and consequences resulting from their data-driven operations (Article 13(2)(f)). This is a significant regulatory innovation, which means that data controllers are potentially accountable for new knowledge about data subjects created by correlating computational and personal data (Hildebrandt 2008, 41). The discriminatory consequences resulting from the opacity of these forms of data-driven practices have been well-covered in the literature, with particular focus on advertising, marketing, health and civil liberty concerns (Hildebrandt 2015, 97–102 Schermer, Custers, and Van Der Hof 2014). The observations made by the Article 29 WP on the risks of marginalising the 'human in the loop' continue to be relevant and these can be summed up as follows: automated decision-making and profiling create an imbalance in the relations between data controllers and data subjects; distortions, errors and bias can be amplified; surveillance trends remain unnoticed and compromises trust; and the scale and impact of harm to individuals difficult to quantify (2013). In limited instances, if it can be shown that contravention of data protection rules contributed to distress and anxiety, there is scope for relief *ex post* (*Google v Gore-Vidal*).
How an algorithm 'sees' individuals is important from a data protection perspective for two reasons. First, since corporate actors and health organisations now have at their disposal software tools which autonomously seek to gain insights into individuals' behaviour, preferences and values, there is no established standard of review to minimise or eradicate predictive harms to individuals (Tufecki 2015, 207). Second, merely focusing on the content of the communications or interactions in these communication spaces is

problematic since platform logics create material conditions that create a 'two-way mirror' with little or no regulatory oversight of the processes for constructing the algorithmic model of decision-making (Balkin 2012, 95). Some of the problems with the predecessor to Article 22 which are present have been extensively covered elsewhere (Savirimuthu 2016). At present, data subjects have arguably no locus standi with regard to predictive harms that may result from algorithmic profiling *ex ante*. Some clarification is needed as to how much information or level of detail data controllers now need to make available to data subjects – assuming that *contra* 'Cookie' law – the volume of linked data is likely to be enormous or may involve disclosing commercial secrets. However, explaining to the individual the 'logic' may not be a real problem, if automated decision-making is of an administrative nature, or involves purchasing or news recommendations based on the individual's profile. Algorithms already assist us on a wide range of matters – manage our health and fitness, choice of holiday destinations, restaurants, books and purchases. Human decision making is not always rational and technologies may have a particular role in society (Nagel, *et al*, 2016). In this respect, algorithms raise a broader issue – can or should individuals' exercise of agency now be subjected to paternalistic interventions? This is not a question that can be readily answered. Any policy response must however consider three interrelated ideas which inform Article 22. First, new forms of sociality are being constructed by greater interconnectivity and sensor capabilities of devices and technological infrastructures and consequently, safeguards need to be implemented by data controllers. Second, transparency and awareness are regarded as necessary to raise data subjects' awareness of how personal data and digital footprints create feedback loops for algorithms. Third, policy recognition that the knowledge generating and predictive capabilities of algorithms should be made meaningful to data subjects, particularly in respect of actual and possible outcomes (Article 29 WP Opinion 8/2014 p. 8, Barocas and Selbt, 2016). Platform infrastructures are repositories for petabytes of data, with machine learning algorithms emerging as the digital equivalent to actuarial science, creating calculated publics using nothing more than code to identify, select and classify. As artificial intelligence and automated decision making become interlinked with health and fitness activities of individuals, these "thinking machines" now create echo chambers and filter bubbles with the consequence that digital persona end up being 'endowed with a life of their own' (Fourcade and Healy, 2016 p.11). Rouvroy, building on Foucault's vision of governmentality and Althusser's ideology of technology, spells out the way technological infrastructures pose challenges for individuals' agency, dignity and privacy.

Notwithstanding the considerable opportunities provided by the advent of new technologies, Rouvroy regards the threats posed by computer processes as linked to the focal point of these algorithms, not the embodied individual, [but] which "has as sole 'subject', a 'statistical body', that is, a constantly evolving 'data-body' or network of localizations in actuarial tables" (2012, 11). These are not mere philosophical musings. It will be recalled that the Facebook emotional contagion study and disquiet engendered by 'Fake News', suggest that curated information can be processed by algorithms to structure news feeds and influence individual's agency and autonomy (Kramer *et al*, 2014, Tufecki, 2015). The policy challenge is whether data protection law's transparency rules extend to what Parisi describes as, adaptive algorithmic processes which exclude certain opportunities and choices from consumers (2013, 13).

E. Of Semantic Discontinuity and the End(s) of Law.

The European Data Protection Supervisor's recent observations regarding the opportunities and challenges posed by new technologies and big data has called for a public debate about the role of ethics in data mining practices and expressed concerns about false trade-offs (EDPS Opinion 4/2015, 9). In two recent interventions, Cohen and Hildebrandt have lent their voices to this debate by introducing narrative frames to pierce the veil of the seeming inscrutability of technological infrastructures and called for the mirror worlds of digital identities to be subjected to due process and the rule of law. Hildebrandt's account of the transition from print to digital, engages with a theme pursued in this article, which is that as sociotechnical technologies render invisible patterns visible only to data controllers, their goals and priorities may not be easily reconciled with human rights norms such as respect for human dignity and agency (2016, 217). Cohen's concept of semantic discontinuity, by contrast, is not framed through the lens of a phenomenological account of technology (2012, 234). Semantic discontinuity, Cohen suggests, is an 'interstitial flexibility within the system of legal rights, institutional arrangements, and associated technical controls' (2012, 234). While we may encounter gaps and inconsistencies in technological, institutional and social structures, Cohen deploys the semantic discontinuity concept to illustrate the way algorithmic proxies dispatch frictions defining much of the practice of everyday life with its technical infrastructures now erecting rules of veridiction, whose legitimacy is teleological (Cohen 2017). Both contributions emphasise the challenge facing data protection law by highlighting threats to its doctrinal armory from personal data-dependent business models. This article provides

another way through which we can approach such debates.

In summary, some reasons can be offered to explain why data protection rules will continue to struggle with the pressures imposed by data-driven business models in the plat- form economy for data subjects' information rights. Most of these have been highlighted above: the misalignment of incentives, the interaction between the right to self-determination and autonomy, and problems in identifying and articulating future harms which are 'significant'. With the emergence of the Internet of Things, the innovations introduced by the GDPR in the form of privacy by design requirements, penalties for non-compliance with data processing obligations and greater emphasis placed on transparency, portability, access and objection remedies are important policy interventions. Auditing algorithms may provide some respite should software codes anticipate what John likes to listen to when running, assist Colin in his rehabilitation or define Aisha's new lifestyle expectations and values (Mittelstadt 2016). Whether this will serve any practical use or resonate with their needs or concerns when data controllers' interests prevail is an important policy issue. The lexicon of standardisation, classification and reification casts doubts on whether data protection law can effectively mediate the space of information flows which bring into motion two different logics – the space of places where individuals assert their autonomy and information rights in an environment embedded with sensor technologies and the space of flows which continue to be tilted in favour of economic and political arrangements. The absence of boundaries between personal and non-personal data, and strains placed on free and informed consent in negotiating algorithmic decision-making may continue to defy the ability of policy-makers to enforce these soft norms into the networked environment of information flows (Elmer 2004). The alignment between the ideal of autonomy, rights of self-determination and data protection continues to be a problematic one as:

> consent is a liberty-based construct, but effective data protection is first and foremost a matter of design. (Cohen 2017, 17)

IV. Conclusion: Interregnum.

The analysis undertaken in this article points to an alternative approach to framing understandings of health platforms and wearables, and situates our understanding of the GDPR within the communication spaces mediated by context-aware sensors and automated decision-making processes. The implications of the interplay between platform

logic and its algorithmic processes for flows of information seem to follow a type of Newtonian law of information flows, where institutional, regulatory arrangements and social practices combine to create a market-oriented technology of justice with corporate actors as its primary beneficiaries (*cf.* Ackerman 1980, 235). Platform logic and algorithms now present policy-makers with a social imaginary where both humans and affordances are co-evolving in ways that blur the boundaries, on the one hand, between personal and non-personal data and human and algorithmic cognition and decision-making, on the other (Parisi 2009). If data protection discourse is to be better calibrated with algorithmic divination and platform logics, how the GDPR renders justiciable, claims for regulatory rather than individual intervention when boundaries between an individual's information rights, autonomy and algorithmic predictive capabilities eventually disappear, will be one of the defining moments in data protection jurisprudence. Data protection rules at its best can maximise the opportunities algorithms and the platform economy make possible in transforming health care and well-being of individuals in society. We may, however, need to temper our optimism. If the health and fitness space can be likened to a new chapter being inscribed into the algorithmic Book of Revelations, the worry is whether as each page is turned 'we shall ever tell two identical stories of two different instances of making up people' (Hacking 1986, 236).

Selected Bibliography

Ackerman, B. 1980. Social Justice in the Liberal State. Yale: Yale University Press.

Acquisti, A. 2009. "Nudging Privacy: The Behavioral Economics of Personal Information." IEEE Security and Privacy 7 (6): 82–85.

Agre, P. 1994. "Surveillance and Capture: Two Models of Privacy." The Information Society 10 (2): 101–127.

Albrecht, J. P. 2016. "Regaining Control and Sovereignty in the Digital Age." In Enforcing Privacy: Regulatory, Legal and Technological Approaches, edited by D. Wright and P. De Hert, 473–488. Dordrecht: Springer.

Article 29 Working Party. Opinion 4/2007 Opinion 4/2007 on the Concept of Personal Data.

Article 29 Working Party. Opinion 02/2013 on Apps on Smart Devices.

Article 29 Working Party. Opinion 03/2013 on Purpose Limitation.

Article 29 Working Party. Advice Paper on Essential Elements of a Definition and a Provision on Profiling within the EU General Data Protection Regulation.

Article 29 Working Party. Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party, WP227 2014.

Article 29 Working Party. Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC.

Article 29 Working Party. Opinion 8/2014 on the Recent Developments on the Internet of Things. Article 29 Working Party. Opinion 03/2016 on the Evaluation and Review of the e-Privacy Directive (2002/58/EC).

Balkin, J. 2012. "Room for Maneuver: Julie Cohen's Theory of Freedom in the Information State." Jerusalem Review of Legal Studies 6: 84–85.

Barocas, S., and A. Selbst. 2016. "Big Data's Disparate Impact." California Law Review 104 (3): 671–732. Berry, D. 2011. "The Computational Turn: Thinking About the Digital Humanities." Culture Machine 12: 1–22.

Borgesius, F. 2016. "Singling Out People Without Knowing their Names-behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation." Computer Law & Security Review 32 (2): 256–271.

Bowers, J., and Rodden, T. 1993. Exploding the Interface: Experiences of a CSCW

Network. In Proceedings of the INTERACT '93 and CHI '93 Conference on Human Factors in Computing Systems (CHI '93). ACM, New York, NY, USA, 255–262.

Boyd, D., and K. Crawford. 2012. "Critical Questions for Big Data." Information, Communication & Society 15 (5): 662–679.

Burrell, J. 2016. "How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms." Big Data & Society January–June 2016: 1–12.

Bygrave, L. 2002. Data Protection Law: Approaching its Rationale, Logic and Limits. Hague: Kluwer. Bygrave, L. 2010. "The Body as Data? Biobank Regulation via the 'Back Door' of Data Protection Law." Law, Innovation and Technology 2 (1): 1–25.

Casper, S. 2013. "New-technology Clusters and Public Policy: Three Perspectives." Social Science Information 52 (4): 628–652.

Cohen, J. 2012. Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. New Haven, CT: YUP.

Cohen, J. 2016. "Between Truth and Power." In Freedom and Property of Information: The Philosophy of Law Meets the Philosophy of Technology, edited by M. Hildebrandt and B. van den Berg. Abingdon: Routledge.

Cohen, J. 2017. "Affording Fundamental Rights: A Provocation Inspired by Mireille Hildebrandt." Critical Analysis of Law 4 (1): 1–22.

Commission. 2003. Report from the Commission – First Report on the Implementation of the Data Protection Directive (95/46/EC) COM (2003) 265 final.

Commission. 2015. A Digital Single Market Strategy for Europe. COM (2015) 0192 final.

Commission. 2016. Digitising European Industry: Reaping the full benefits of a Digital Single Market. COM (2016) 180 final.

Commission. 2017. Building A European Data Economy. COM (2017).

Copenhagen Economics. 2013. The Impact of Online Intermediaries on the EU Economy. Copenhagen. Couldry, N., and A. Hepp. 2016. The Mediated Construction of Reality. Cambridge: Polity.

Elmer, G. 2004. Profiling Machines: Mapping the Personal Information Economy. Cambridge, MA: MIT.

EDPS. 2015. Opinion 4/2015 Towards a New Digital Ethics: Data, Dignity and Technology.

EDPS. 2016. Opinion 8/2016 EDPS Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data.

Esposti, S. 2014. "When Big Data Meets Dataveillance: The Hidden Side of Analytics."

Surveillance & Society 12 (2): 209–225.
Evans, P., and A. Gawer. 2016. The Rise of the Platform Enterprise: A Global Survey. New York: Center for Global Enterprise. January.
Fourcade, M., and K. Healy. 2016. "Seeing Like a Market." Socio-Economic Review 1–21.
Frawley, W., G. Piatetsky-Shapiro, and C. Matheus. 1992. "Knowledge Discovery in Databases: An Overview." AI Magazine 13 (2): 57–70.
FTC Staff Report. 2015. Internet of Things: Privacy & Security in a Connected World. Washington: FTC.
Fuster, G. 2014. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Berlin: Springer.
Gilmore, J. 2015. "Everywear: The Quantified Self and Wearable Fitness Technologies." New Media & Society 18 (11): 2524–2539.
Hacking, I. 1986. "Making Up People." In Reconstructing Individualism: Autonomy, Individuality, and the Self in Western Thought, edited by T. C. Heller, M. Sosna, and D. E. Wellbery. Redwood City, CA: Stanford UP.
Helmond, A. 2015. "The Platformization of the Web: Making Web Data Platform Ready." Social Media + Society 1 (2): 1–11.
Hildebrandt, M. 2008. "Profiling and the Rule of Law." Identity in the Information Society 1 (1): 55–70.
Hildebrandt, M. 2015. Smart Technologies and the End of Law: Novel Entanglements of Law and Technology. Cheltenham: Edward Elgar.
Hilts, A., C. Parsons, and J. Knockel. 2016. Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security. https://openeffect.ca/reports/Every_Step_You_Fake.pdf.
Hustinx, P. 2014. EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf.
Katz, J. 2003. "Bodies, Machines and Communication Contexts: What is to Become of Us?" In Machines that Become Us: The Social Context of Personal Communication Technology, edited by J. Katz, 311–319. New Brunswick, NJ: Transaction.
Kotthoff, L. 2014. "Algorithm Selection for Combinatorial Search Problems: A Survey." AI Magazine 35 (3): 48–60.
Kramer, A., J. Guillory, and J. Hancock. 2014. "Experimental Evidence of Massive Scale

Emotional Contagion Through Social Networks." Proceedings of the National Academy of Sciences 111 (24): 8788–8790.

Langlois, G., and G. Elmer. 2013. "The Research Politics of Social Media Platforms." Culture Machine 14: 1–17.

LIBE. 2015. Big Data and Smart Devices and their Impact on Privacy. Brussels: European Union. http://www.europarl.europa.eu/studies.

Lynskey, O. 2016. The Foundations of EU Data Protection Law. Oxford: OUP.

Mittelstadt, B. 2016. "Auditing for Transparency in Content Personalization Systems." International Journal of Communication 10: 4991–5002.

Nagel, S., V. Hrincu, and P. Reiner. 2016. "Algorithm Anxiety – Do Decision-making Algorithms Pose a Threat to Autonomy?" In 2016 IEEE international symposium on ethics in engineering, science and technology. IEEE Ethics 1-7.

NDG (National Data Guardian). 2016. "Review of Data Security, Consent and Opt-Outs." https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF.

Nissenbaum, H. 1999. "The Meaning of Anonymity in an Information Age." The Information Society 15 (2): 141–144.

Nissenbaum, H. 2015. "'Respect for Context': Fulfilling the Promise of the White House Report." In Privacy in the Modern Age: The Search for Solutions, edited by M. Rotenberg, J. Scott, J, and J. Horwitz, 152–164. New York: The New Press.

OECD. 1980. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. France: Paris.

O'Neill, C. 2016. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York: Crown Pub.

Papacharissi, Z. 2015. Affective Publics: Sentiment, Technology, and Politics. Oxford: Oxford UP. Parisi, L. 2009. "Symbiotic Architecture: Prehending Digitality." Theory, Culture and Society 26 (2–3): 346–374.

Parisi, L. 2013. Contagious Architecture: Computation, Aesthetics, and Space. Cambridge, MA: MIT.

Raab, C. 1999. "From Balancing to Steering: New Directions for Data Protection." In Visions of Privacy: Policy Choices for the Digital Age, edited by C. J. Bennett and R. Grant, 68–96. Toronto: University of Toronto Press.

Rouvroy, A. 2012. "The End(s) of Critique: Data-behaviourism vs. Due-process." In Privacy, Due Process and the Computational Turn. Philosophers of Law Meet

Philosophers of Technology, edited by M. Hildebrandt and E. De Vries, 143–168. Abingdon: Routledge.

Savirimuthu, J. 2016. "Networked Children, Commercial Profiling and The EU Data Protection Reform Agenda: In the Child's Best Interests?" In The EU as a Children's Rights Actor: Law, Policy and Structural Dimensions, edited by Iusmen and H. Stalford, 221–257. Opladen: Barbara Budrich.

Schermer, B. W., B. H. M. Custers, S. Van Der Hof. 2014. "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection." Ethics and Information Technology 16 (2): 171–182.

Solove, D. 2013. "Privacy Self-Management and the Consent Dilemma." Harvard Law Review 126 (7): 1880–1903.

Sweeney, L. 2013. "Discrimination in Online Ad Delivery." Communications of the ACM 56 (5): 44–54.

Tempini, N. 2015. "Governing Patientslikeme: Information Production and Research Through an Open, Distributed, and Data-based Social Media Network." The Information Society 31 (2): 193–211.

Tufecki, Z. 2015. "Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency." Journal on Telecommunications and High Technology Law 13: 203–218.

Turow, J., L. McGuigan, and E. Maris. 2015. "Making Data Mining a Natural Part of Life: Physical Retailing, Customer Surveillance and the 21st Century Social Imaginary." European Journal of Cultural Studies 18 (4–5): 464–478.

Van Dijk, J. 2013. Culture of Connectivity: A Critical History of Social Media. Oxford: Oxford University Press.

Weiser, M. 1991. "The Computer of the 21st Century." Scientific American 265: 94–104.

Zins, C. 2007. "Conceptual Approaches for Defining Data, Information and Knowledge." Journal of the American Society for Information Science and Technology 58 (4): 479–493.

Cases

Bodil Lindqvist C-101/01 [2003] ECR I-12971

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources C-293/12 Google v Vidal-Hall [2015] 3 WLR 409

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González C-131/12 ECLI: 2014:317

Maximillian Schrems v Data Protection Commissioner C-362/14 ECLI: 2015:650

Promusicae C-275/06 ECLI: 2008:54

Regina v. Chief Constable of South Yorkshire Police (Respondent) ex parte Marper (FC)(Appellant) Consolidated Appeals [2004] UKHL 39

S and Marper v UK [2008] ECHR 1581

Volker und Markus Schecke and Eifert C-92/09 ECLI: 2010:662