Health Technol. (2017) 7:453–467
DOI 10.1007/s12553-017-0185-3

ORIGINAL PAPER

Selling your soul while negotiating the conditions: from notice and consent to data control by design

Luca Belli[1] · **Molly Schwartz**[2] · **Luiza Louzada**[3]

Received: 4 October 2016 / Accepted: 20 February 2017 / Published online: 18 March 2017

Abstract This article claims that the Notice and Consent (N&C) approach is not efficient to protect the privacy of personal data. On the contrary, N&C could be seen as a license to freely exploit the individual's personal data. For this reason, legislators and regulators around the world have been advocating for different and more efficient safeguards, notably through the implementation of the Privacy by Design (PbD) concept, which is predicated on the assumption that privacy cannot be assured solely by compliance with regulatory frameworks. In this sense, PbD affirms that privacy should become a key concern for developers and organisations alike, thus permeating new products and services as well as the organisational modi operandi. Through this paper, we aim at uncovering evidences of the inefficiency of the N&C approach, as well as the possibility to further enhance PbD, in order to provide the individual with increased control on her personal data. The paper aims at shifting the focus of the discussion from "take it or leave it" contracts to concrete solutions aimed at empowering individuals. As such, we are putting forth the Data Control by Design (DCD) concept, which we see as an essential complement to N&C and PbD approaches advocated by data-protection regulators. The technical mechanisms that would enable DCD are currently available (for example, User Managed Access (UMA) v1.0.1 Core Protocol). We, therefore, argue that data protection frameworks should foster the adoption of DCD mechanisms in conjunction with PbD approaches, and privacy protections should be designed in a way that allows every individual to utilise interoperable DCD tools to efficiently manage the privacy of her personal data. After having scrutinised the N&C, PbD and DCD approaches we discuss the specificities of health and genetic data, and the role of DCD in this context, stressing that the sensitivity of genetic and health data requires special scrutiny from regulators and developers alike. In conclusion, we argue that concrete solutions allowing for DCD already exist and that policy makers should join efforts together with other stakeholders to foster the concrete adoption of the DCD approach.

Keywords Notice and consent · Privacy by design · Data control by design · Data protection · Health data

This article is part of the Topical Collection on *Privacy and Security of Medical Information*

✉ Luca Belli
luca.belli@fgv.br

Molly Schwartz
molly.schwartz@iki.fi

Luiza Louzada
arquivoluiza@gmail.com

[1] Center for Technology & Society, Fundação Getulio Vargas (FGV), Rio de Janeiro, Brazil

[2] University of Malmö, Malmö, Sweden

[3] Universidade do Estado do Rio de Janeiro, Rio de Janeiro, Brazil

Until 1983, Canon law foresaw that a lawyer defined as *Advocatus Diaboli* (i.e. the Devil's Advocate) had the task of uncovering any evidence or misrepresentation impeding and potentially jeopardising the canonisation of a given candidate to sainthood. A more renown and picturesque version of the Devil's Advocate is offered by the homonymous movie, where Keanu Reeves, a young and ambitious attorney, sells his soul to the Devil, Al Pacino. Not so late after such decision, Reeves starts realising and suffering the negative consequences of his decision. If an individual's soul were to be

materialised, it would be fragmented in data describing one's character, feelings, ideas and so on. Although personal data[1]may not be so precise as to describe one's soul, they may reveal a considerable amount of very precise information regarding almost every aspects of one's life. Public bodies as well as private entities may collect such information for a variety of purposes and the data collection and processing may produce an ample spectrum of (un)intended consequences on the individual to which the data refer.

Starting with the 1948 Universal Declaration of Human Rights, the respect for private and family life has been recognised as a fundamental human right, whose protection has been laid down by a number of binding documents at the international level. Since the 1970s,[2] the progress with regard to the capability to collect and process data has shown the need for the definition of legal safeguards, protecting the individuals from the risks of undue processing of personal data. Notably, the privacy of personal data has been closely related to informational self-determination, arguing that individuals should be able to independently determine what kind of information about themselves can be collected and processed as well as the circumstances and conditions of such collection and processing. In this perspective, data protection frameworks have aimed at ensuring individuals' self-determination through the possibility to take an informed decision and choose to accept or refuse the data collection and processing conditions, by freely expressing – or denying – an informed consent.

This article claims that the aforementioned Notice and Consent (N&C) approach is not efficient to protect the privacy of personal data. On the contrary, if data where to be considered individuals' soul, the N&C configuration could be seen as a license to freely exploit it. For this reason, legislators and regulators around the world have been advocating for different and more efficient safeguards, notably through the implementation of the Privacy by Design (PbD) concept, which is predicated on the assumption that privacy cannot be assured solely by compliance with regulatory frameworks. [7]. In this sense, PbD affirms that privacy should become a key concern for developers and organisations alike, thus permeating new products and services as well as the organisational *modi operandi*.

Through this paper, we act as diligent *Advocati Diaboli*, aiming at uncovering evidences of the inefficiency of the N&C approach, as well as the possibility to further enhance PbD, in order to provide the individual with increased control on her personal data. The paper aims at taking a step further, shifting the focus of the discussion from "take it or leave contracts" to concrete solutions aimed at empowering individuals. As such, we put forth the Data Control by Design (DCD) concept, which we see as an essential complement to N&C and PbD approaches advocated by data-protection regulators. In the same perspective of the PbD approach, DCD predicates proactivity rather than reactivity, thus empowering the individual with the tools necessary for avoiding abusive data collection and processing ab initio. The technical mechanisms that would enable DCD are currently available (for example, User Managed Access (UMA) v1.0.1 Core Protocol [52]). We, therefore, argue that data protection frameworks should foster the adoption of DCD mechanisms, which we see as an evolution of the PbD approaches. As such, privacy protections should be designed in a way that allows every individual to utilise interoperable DCD tools to efficiently manage the privacy of her personal data.

The methodology of this paper is based on both a literature review and an analysis of concrete implementations of technical tools designed to allow users to assert control over their personal data management, with a particular focus on the MyData initiative. [40] The first section of this paper will provide an overview of the "traditional" N&C mechanism, used to protect individuals' data privacy online and will emphasise the failures of such mechanism. Particularly, we will stress that, in the online environment, individuals are presented with complex and legalistic privacy notices to which they can either consent, in order to enjoy a given service, or refuse, thereby forfeiting the option to use the desired service. This all-or-nothing scenario highlights that the current N&C model is impractical and illusory, turning a tool that is supposed to empower individuals to make informed choices into a tool for submerging users in unread contractual terms, accepted as the de facto price of online services.

In Section 2, we briefly analyse the concept of PbD, underscoring that it represents an advancement in terms of

[1] According to EU legislation, "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Furthermore, "data concerning health" is defined as "personal data related to the physical or mental health of a natural person, including the pro vision of health care services, which reveal information about his or her health status," while "genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question." See art. 4.1, 15, and 13. Regulation (EU) 2016/679, better known as General Data Protection Regulation. Due to its comprehensive nature, the EU approach is usually considered as a data protection benchmark. The U.S. approach, as an instance, has been criticised for being less coherent and consistent, offers multiple competing definitions of personal information. See e.g. Schwartz and Solove [50].

[2] In the 1970s, growing use of automated systems aimed at collecting and processing data about individuals stimulated the elaboration various national efforts gave birth to the first privacy frameworks - e.g. in the 1974 US Fair Information Practice Principles or the French 1978 *Loi Informatique et libertés* (Law n°78–17) – and stimulated the first international frameworks on data protection. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were adopted by the Council of the OECD and became applicable on 23 September 1980. In January 1981, the Council of Europe adopted a Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

data privacy protection, compared to an inefficient N&C approach. To cope with such inefficiency, PbD proposes a proactive approach that embeds the protection of privacy into technologies, procedures, and architectures. This evolutionary step is particularly meaningful, for it represents a shift from a legal approach to privacy to a "design-thinking" approach. This approach translates legal concepts into the technical architecture of the Internet environment, and ICT-environments in general, as well as into the organisational architecture of the various entities operating in such an environment. PbD is grounded in the integration of the protection of privacy into the modus operandi, priorities, objectives, and design processes of any organisation.

In Section 3, we examine the emergence of DCD models and initiatives that we consider a step forward in the direction of data privacy debate, enhancing both N&C and PbD. PbD usefully requires designers and operators to fashion procedures, products, and services with the privacy of their users in mind and ideally offering privacy protections by default. However, PbD still does not fully empower users to take control over their privacy because, as in the N&C context, individuals are only given the option to choose whether or not their data will be collected and processed rather than being able to exert full control over how their personal data are used and by whom. Indeed, both N&C and PbD schemes fail to consider the nuances that exist between strong data privacy protection and no data privacy protection. Particularly, N&C and PbD do not seem to consider the possibility that individuals might be interested in allowing the collection and use of their data, or some categories of their personal data, when it is necessary for specific purposes and data are processed by trusted agents.

PbD aims at providing individuals with concrete solutions for the effective exercise of their fundamental right to privacy, rather than choosing between blanket data collection and no data collection. However, we contend that the concrete implementation of this approach is delegated to the provider, thus leaving to the individual the burden of controlling and modifying the privacy settings of each service. Although this may seem an advance, it can be argued that PbD still fails to reduce the complexity for the user, potentially transposing the difficulties that the user may face in deciphering the contractual condition of each service to the complexity of defining technical features that vary from service to service. Moreover, PbD requirements and implementations may differ from one legal system to another, thus raising costs for developers and organisations alike, while potentially fostering further fragmentation and complexity. By suggesting the concept of DCD, we aim at achieving two purposes. First, we hope to shift the focus to the empowerment of individuals with the possibility to actively control, in a simple and effective fashion, the modalities of their personal data collection and use. Secondly, we stress that, in order to be effective, DCD has to be grounded on interoperability, so that users' choices can be understood and directly implemented by the systems defined according to a PbD approach.

Lastly, in Section 4, we discuss the specificities of health and genetic data, and we apply the DCD rationale to this context. The possibilities of collecting and processing genetic and health data is rapidly expanding and policymakers are starting to address the responsibilities of the new medical intermediaries. However, we stress that the sensitivity of genetic and health data requires special scrutiny from regulators and developers alike, in order to avoid jeopardising the individuals' rights. In conclusion, we argue that concrete solutions allowing for DCD already exist and that policy makers should join efforts together with other stakeholders to foster the concrete adoption of such approach.

1 Notice and consent: good intentions with questionable outcomes

Beginning in the late 1970s a number of privacy principles emerged from various national legal systems and were subsequently distilled into the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[3] developed by the Organisation for Economic Cooperation and Development (OECD), as well as in the Privacy Framework[4] developed by the Asia-Pacific Economic Cooperation (APEC).

The fundamental concern leading to the elaboration of privacy principles and legislation was to foster an appropriate balance between individuals' privacy and the free flow of information. In this perspective, personal data should be collected and processed only when necessary and proportionate to the achievement of a legitimate aim or when the individual whose personal data are being processed has freely expressed her informed consent. Notably, the individual's capacity to determine what personal data may be disclosed to third party was prominently articulated in the landmark Census decision[5] of the German Federal Constitutional Court (Bundesver fassungsgericht). According to the Court's reasoning, privacy safeguards allow individuals to preserve the separation of societal sub-systems, thus preventing the propagation of sensitive information from one area of life – such as one's family life, professional environment, or health-care – into another. Hence, when individuals cannot fully exercise their informational self-determination, overseeing and controlling what personal information about them is accessible and how it can be used, they may not be able to fully enjoy their freedom to act without external compulsion.

[3] See OECD [38].
[4] See http://publications.apec.org/publication-detail.php?pub_id=390
[5] See Bundesverfassungsgericht, Decision of 15 December 1983 (1BvR 209, 269, 362, 420, 440, 484/83), decisions. Vol. 65, 1–71.

In this regard, UN Special Rapporteur on Privacy, Joe Cannataci, has recently reiterated the importance of protecting data privacy to allow individuals to develop their personality "in the freest of manners" [5] as they discover themselves throughout their lifetime. Indeed, privacy protections aim at guaranteeing individuals' freedom to construct the persons they wish to become, having autonomy of action and thought.[6] Based on these considerations, the "privacy self-management" approach has been developed to provide individuals with control over their personal data. Conspicuously, the approach assumed that those who are properly notified of the reason, context, and purpose of their personal data collection, processing, or disclosure will be able decide freely whether to consent or not to such activities. Furthermore, to implement privacy self-management in an appropriate fashion, the N&C approach has been traditionally matched to a bundle of rights[7] attributed to the individual in her quality of "data-subject" in order to manage the privacy of her personal data.

Although, in principle, such an approach seems to help individuals exert control over their personal data, the convergence of our offline activities – such as commerce, social interactions or entertainment – into the online world has shown the inadequacy of N&C mechanisms. Indeed, rather than allowing individuals to manage their personal-data privacy, the N&C approach has increasingly become an instrument for individuals to pay for online services with the consent to access, process, and disclose their personal data. When facing the binary choice between enjoying a service or being excluded from its use, based on a willingness to hand over personal data, users rarely choose the latter option. This leads to a sort of "privacy paradox"[8] according to which individuals affirm that they value their fundamental right to privacy but regularly trade over their personal information in exchange for access to applications.

Furthermore, it has been proven that the very assumption upon which such choices should be made – i.e. fact that the individual is duly informed in order to express consent – is not only fallacious but de facto extremely challenging to put into practice. Indeed, empirical investigations have demonstrated that assuming individuals are adequately informed based on their acceptance of online services' contracts turns out to be "the biggest lie on the Internet."[9] Besides dedicating scarce or no time to the consultation of Privacy Policies (PPs) and Terms of Service (ToS), users frequently consider these documents as a nuisance [34], due to their length and complexity[10] as well as their overwhelming number. Indeed, every Internet intermediary regulates its service via specific contractual provisions, [2], thus multiplying the contractual agreements that individuals are supposed to analyse in order to utilise the services.

The N&C mechanism is grounded on the assumption that the expression of consent by ticking a case signifies user knowledge and conscious acceptance of the contractual clauses of every service she utilises. Such assumption seems more than questionable. Indeed, studies have demonstrated that individuals should spend 8 h a day for 76 days every year to read the ToS and PPs of the websites they visited on average. [31] In addition, as shown by research conducted by Center for Technology & Society at Fundação Getulio Vargas, a wide range of online service providers do not commit to notifying users about changes in their ToS and PPs – or they commit to notification only when changes are deemed as "significant" according to unspecified criteria – and do not specify who are the "third parties" with whom personal data will be shared. [56] Such elements make it virtually impossible to express consent in an informed fashion.

Therefore, it may be argued that the N&C scheme is grounded on a series of dubious claims. Firstly, it assumes that individuals expressing their consent to PP and ToS behave as rational economic subjects, having the time and knowledge to analyse carefully the content of every contractual agreement. Secondly, it postulates that individuals hold the bargaining power necessary to freely accept the provisions included in contractual agreements unilaterally defined by the providers. Such assumptions clearly overestimate both the bargaining power and the degree, quality and intelligibility of the information at the disposal of individuals who are weighing the costs and benefits of providing their consent. In this sense, it should also be considered that, according to the OECD Programme for International Assessment of Adult Competencies, in several developed countries less than 30% of the population between 16 and 65 year-old enjoys the literacy and information processing skills[11] that seem essential to comprehend and agree with contractual provisions. Such

[6] See the keynote delivered by Joe Canatacci at the Health Privacy Summit 2016 https://www.youtube.com/watch?v=XuBWs3PBDMk

[7] Notably, Article 8 of the Council of Europe Convention 108 and Article 12 of the EU Data Protection Directive 46/95/EC ascribe to data subjects the right to: access their personal data; to have their data deleted or blocked; and to object the use of their data for direct marketing purposes, to take automated decisions, or to be processed producing disproportionate results. The updated OECD Privacy Guidelines as well as the new EU General Data Protection Regulation further clarify that individuals enjoy also the right to have their data erased, rectified, completed or amended [37].

[8] See Blank et al. [4].

[9] See e.g. Obar and Oeldorf-Hirsch [34]. See also http://www.biggestlie.com/

[10] Such criticalities are well-known to policymakers since the mid-2000s. For instance, based on empirical research [58], Federal Trade Commissioner Jon Leibowitz famously stated: "Initially, privacy policies seemed like a good idea. But in practice, they often leave a lot to be desired. In many cases, consumers don't notice, read, or understand the privacy policies. They are often posted inconspicuously via a link at the very bottom of the site's homepage – and filled with fine-print legalese and techno talk."

[11] The situation does not look rosier, in countries traditionally considered as having a highly educated population, like Japan, The Netherlands or Finland, where the percentage of illiteracy within the adult population is close to 40%, or in countries considered as highly developed, such as the U.S., France or Germany, where the percentage of illiteracy exceeds 50% of the adult population. See OECD [36].

percentage is very unlikely to be more encouraging in developing counties, where illiteracy rates are generally higher.

In light of the aforementioned considerations, as well as of those expressed in the previous paragraph, it seems that trusting the N&C aptitude to protect individuals' data-privacy may be at best naïve or, more realistically, fallacious. Moreover, it is important to acknowledge that, despite the stated intention to attribute informational self-determination to individuals, the N&C mechanism has de facto evolved into a payment model, consisting in trading consent to personal-data exploitation for the possibility to access online services. Indeed, in the context of a data-driven economy,[12] the very purpose of online services' ToS and PPs is to create a contractual regime allowing service providers to collect and exploit individuals' personal data, which subsequently become a new class of asset [57] owned[13] by the provider.

As such, it seems quite evident that, rather than protecting individuals' privacy, the N&C approach has demonstrated to be much more effective at creating the conditions to transform the privacy of users' data into a commodity that can be decoupled and traded for services. The download of any "free" mobile application turns out to be a very telling experience with regard to what is the real price of online services. Indeed, virtually every mobile application can be used only under the previous acceptance of the ToS, which typically foresee the application provider right to collect and process a wide range of personal information spanning form the user telephone number and IP address to geo-localisation data, list of contacts, etc. In this regard, it has been argued that the N&C failure to protect privacy and simultaneous success in easing the exploitation of personal data may be the fruit of specific ideological choices. Conspicuously, Hull [20] has emphasised that the N&C model consecrates "the belief that privacy can only be treated in terms of individual economic choices to disclose information; the occlusion of the fact that these choices are demonstrably impossible to make in the manner imagined; and the occlusion of the ways that privacy has social value outside whatever benefits or losses may accrue to individuals."

The acknowledgement of the inefficiency of N&C to protect privacy has therefore led to the quest for further mechanisms allowing individuals to regain control over their personal data. In this regard, the PbD approach seems a positive step forward.

[12] See e.g. [1, 6]. For a reading list on data-driven economy literature, see https://www.uschamberfoundation.org/reading-list-data-driven-economy

[13] Although not all providers make this element explicit in their PPs or ToS, some services such as the PockémonGO application openly state that "Information that we collect from our users, including [personal data], is considered to be a business asset. Thus, if we are acquired by a third party as a result of a transaction such as a merger, acquisition, or asset sale or if our assets are acquired by a third party in the event we go out of business or enter bankruptcy, some or all of our assets, including your (or your authorized child's) [personal data], may be disclosed or transferred to a third party acquirer in connection with the transaction." See https://www.nianticlabs.com/privacy/pokemongo/en

In the following section, we briefly analyse PbD, arguing that, although representing an improvement from the mere N&C, PbD can and should be complemented with DCD strategies to grant users the effective control over their data privacy via interoperable tools rather than perpetuating a model in which privacy conditions and parameters vary confusingly between services.

2 Designing privacy into architectures

As argued above, the N&C approach has been more effective at facilitating the collection, processing, and subsequent monetisation of personal data than providing individuals with control over their data privacy. Particularly, in the N&C context, the expression of consent represents the moment in which the data-subject loses control over her personal data rather than acquiring informational self-determination. Once consent is given, the contractual party who drafted the PP will be in charge of managing the personal data for purposes than can be very vaguely defined, such as "improving the service," including the possibility of sharing them with undefined third parties. [56] The individual, on the other hand, will be only marginally involved in the data life-cycle, with scarce or no recourse aside from seeking remedies for privacy breaches retroactively after the breach has taken place.

Since the mid-1990s, the popularisation of ICTs and the emergence of the data-driven economy have exposed the deficiencies of the N&C approach and stimulated the need for a complementary strategy allowing individuals to actively manage their data privacy. In 1995, the Dutch and Canadian Data Protection Authorities jointly published a seminal report, arguing that technology can be used to protect individuals' privacy and concretely proving that so-called Privacy-Enhancing Technologies (PETs) could be used to allow data-subjects to actively control the processing of their personal data [55]. In this sense, Van Blarkom et al. [54] highlighted that "PETs are based on the development of a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system".

The reflection on PETs has been essential to nurture the development of the PbD concept, stressing the need for a diversification of data-protection strategies and widening the focus of the privacy discussion into the design of technologies and organisational practices. Notably, while PETs aim at providing individuals with specific tools to protect their privacy, PbD is a wider conceptual framework, based on the recognition that the technical architecture of the products and services or the organisational structure of processes and programmes have a direct impact on the user capability to protect his privacy. On the one hand, PbD aims at embedding privacy into

technical and organisational architectures, allowing individuals to prevent the social, financial, and physical harms that may be caused by the misuse of their personal data within such architectures. On the other hand, PbD aims at fostering accountability of both public and private organisations collecting and processing personal data [7]. Therefore, the aim of both PETs and PbD is to prompt a proactive approach to data privacy, in which the user can play an active role thanks to the privacy protections that are embedded *ab origine* into the services, processes, networks, etc. The goal of PbD is to lead engineers, providers and administrators to consider carefully the interests of the individuals, including privacy protections, when they design or redesign[14]specific information systems. As such, PbD aims at utilising both technical and governance strategies, considering privacy within organisations' risk management and establishing user-friendly features that allow individuals to manage the privacy of their data.

The PbD approach represents a positive step forward, by implicitly acknowledging the deficiency of the N&C approach and recognising that sound privacy protections should actively involve both system designers and users. However, it would be overconfident to assume that the existence and promotion of PbD approaches equal to their effectiveness. Indeed, as pointed out by ENISA [12], "privacy and data protection features are generally ignored by traditional engineering approaches when implementing the desired functionality. This ignorance is caused and supported by limitations of awareness and understanding of developers and data controllers as well as lacking tools to realise privacy by design." Besides the lack of clear guidelines on how to properly engineering privacy protections into processes, systems, and services, one of the main challenges to the effective implementation of PbD is the prevalence of business concerns over privacy concerns. Indeed, as noted above, data collection and processing for advertising purposes are at the core of the Internet economy. In this respect, the OECD [35] has emphasised that retailers, public administrations, financial institutions, healthcare providers, together with specialised data analysts and data brokers are only some of the main stakeholders whose business models increasingly rely on personal data as an essential input. Indeed, the current trend toward the Internet of Things[15] is going to transform potentially any producer of every "thing" into a data collector and processor whose business will be affected by data analysis.

A situation where individuals have the possibility to define privacy settings for each service and each thing they use may be considered as an improvement. However, it seems highly unlikely that all players in the Internet ecosystem will conceive and implement privacy settings in the exact same way. Moreover, it seems likely that, when faced with the option to define privacy setting of each and every service and thing they use, individuals will likely start considering such options as a "nuisance" as they currently do with regard to the consultation of privacy conditions. [34] The fragmentation of different PbD implementations by service providers and "things" producers may indeed turn out to be e substantive obstacle to the effectiveness and usefulness of PbD strategies. Hence, although the implementation of appropriate technical and organisational measures can improve individuals' capacity to protect their data privacy, it would be overconfident to argue that PbD guarantees individuals' full control over how their data are utilised. Indeed, the abovementioned phenomenon of discrepancy and multiplication of PbD settings is not the only type of fragmentation that can jeopardise the benefits of PbD. Notably, despite the general commitment of Data Protection and Privacy Commissioners to PbD,[16] such approach remains subject to juridical fragmentation, being based on obligations defined by domestic legal frameworks and monitored by national regulators. The very concept of privacy is subject to multiple interpretations and, even in a situation where national regulators elaborate clear PbD guidelines, it is unreasonable to assume that privacy guidelines elaborated by different regulators would be both compatible and consistently implemented. Hence, it seems reasonable to assume that, when dealing with privacy settings in a PbD context, individuals would face a similar hurdle to the one they currently face with deciphering ToS and PPs.

Indeed, PbD will be implemented differently depending, firstly, on the domestic legal requirements and, secondly, on the specific technical features that every business actors may choose to adopt. To promote a legally interoperable[17] PbD approach on how to assess the privacy implications of technical protocols, the Internet Engineering Task Force (IETF) has designed an Internet standard, the RFC 6973, providing guidance " to make designers, implementers, and users of Internet protocols aware of privacy-related design choices." [11] This approach, which is only limited to Internet standards, still presupposes that operators and providers assess and implement privacy protections independently and, although it offers useful guidelines, the utilisation of such guidelines remains optional. As noted above, when conducting (potentially onerous) Privacy Impact Assessments (PIA) in order to put in place appropriate governance and technical privacy

[14] Cavoukian and Prosch [8] also highlight that privacy can be redesigned using a transformative "Privacy by ReDesign" process which offers a framework for undertaking a proactive assessment of existing gaps in how an organization manages personal information and addresses those gaps systematically.

[15] See e.g. Ziegeldorf et al. [60]; KPMG [25].

[16] See 32nd International Conference of Data Protection and Privacy Commissioners. Jerusalem, Israel 27–29 October, 2010 Resolution on Privacy by Design. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/1 0–10-27_Jerusalem_Resolutionon_PrivacybyDesign_EN.pdf

[17] For a discussion of the concept of legal interoperability and its applications, see Santosuosso and Malerba [46]; Weber [59]; Belli & Foditsch [3].

protections, intermediaries may be tempted to prioritise business considerations over protecting their users' privacy. As such, PbD implementations may find a further element of fragmentation in the cost that their implementation may determine.

To make PbD effective, the EU General Data Protection Regulation (GDPR) gives specific recognition to PbD and, for the first time, establishes legal obligations allowing its enforcement. Notably, the GDPR makes explicit reference to the data minimisation principle,[18] introduces data protection by default, stipulates the protection of personal data as a default property of systems and services, and promotes the possibility to use data pseudonymisation. The GDPR requirements usefully deal with the juridical fragmentation problem, harmonising PbD at the European level, obliging intermediaries established or willing to operate in the European Economic Area to consider privacy when designing policies, procedures, and systems. However, despite easing the suppression of data and creating data-portability obligations, the European PbD framework does not guarantee that individuals have full control over how their data are used nor that they can easily define privacy settings in the dozens or hundreds of services and things they intend to utilise.

To be effective, PbD should be complemented by DCD, ascribing to individuals the possibility to define how their personal data could be utilised and consecrating their choice into interoperable technical tools, allowing intermediaries to easily understand user choice and abide. Current PbD obligations do not achieve such goals and leave individuals dealing with a number of diverging legal and technical PbD-configurations. Hence, the existing approach allows individuals to manage some aspects of their data privacy but it does not grant them the ability to fully and esaily control how their personal data will be exploited. To foster a DCD approach able to thrive and fill the gaps of PbD, a multistakeholder approach seems necessary. Individuals should actively define their data-exploitation permissions and preferences via user-friendly and interoperable tools; business players design information systems in order to be compatible with such tools and respect user preferences; and policymakers should fashion in a legally interoperable framework, promoting user engagement and incentivising the adoption of DCD by the private sector.

In the next section, we describe a selection of initiatives, as examples of approaches that foster DCD. Furthermore, we point out that the existence of various DCD initiatives demonstrates an active interest within civil society and technical communities in the effective development of DCD.

[18] Data minimisation posits the collection, processing and disclosure of the minimal data necessary to perform a task, in order to reduce the chances that personal data be misused or leaked.

3 Data control by design

Over the past decade, the ways in which personal data are collected, shared, and processed have become a major cause for individual concern. The 2015 Data Protection Eurobarometer showed that, while 71% of respondents saw providing personal information online as a necessity of modern life, yet 85% of respondents felt they do not have complete control over the information they provide online [13]. Likewise, Pew Research surveys on the state of privacy in the United States show that 91% of Americans agree that they have lost control over how their data is collected or used by companies [41]. These numbers illustrate that in countries with some of the most sophisticated data-protection frameworks, ordinary individuals do not feel in control of their personal data online. Furthermore, data privacy and security issues are only becoming more exacerbated as the management sensitive data, like health data, moves increasingly onto less secure platforms, like mobile applications. In this perspective, the increasing "appification" of health data poses snowballing threats to data privacy and security, as demonstrated by the widespread sharing of sensitive data with third-party services without notifying or receiving prior consent from data subjects. [30].

Any attempts to alter the current paradigm of personal data brokering in favour of systems that are more transparent, secure, and user-centred must work against the dominant funding models for online services, based on data collection for targeting advertising purposes. [16] Targeted advertising funding models rely on the massive collection, aggregation, and analysis of personal data, facilitated by companies known as data brokers, for the purpose of delivering highly personalised advertising content [43]. Due to the combined lack of consumer knowledge about personal data collection and lack of viable alternatives to data collection under the current N&C regime, consumer demand has been an insufficient driver to reform the current model triggering an alternative ecosystem of digital services, operating according to the DCD approach that we outline in this paper. As emphasises by Mitchell [32], the concept of individuals acting as their own personal data managers is completely novel under the current paradigm: "Up to now, the disciplines of direct, digital and database marketing have based themselves on a single common assumption: that the organization is the data manager; that direct marketing is driven by the organization that collects, analyses and uses data in pursuit of its own purposes."

The question of how to advance the development of digital services, particularly considering the rise of the Internet of Things and of Big Data analytics, without compromising individual freedoms, privacy, and autonomy has spurred a movement toward a new kind of data control that empowers individuals. As argued in the previous sections, the

development of services based on N&C has been very useful to favour data-monetisation but has also shown that ordinary users are not equipped with the information, knowledge and skills, necessary to understand and control the fate of their personal data. In order to give people the power to control the collection, sharing, and usage of their data in a practical way, it seems necessary to rethink the way ICT and services are developed by "baking" data control features into the ICT design. This is the premise of the PbD approach but, as we have argued, such approach may have relevant limits. Therefore, we suggest to expand and strengthen the PbD concept, embracing a DCD approach offering users interoperable data control tools conveying the individual data privacy settings in an interoperable and machine readable fashion. In the next sections, we will outline the basic principles of the DCD approach and highlight some of the initiatives that put it in practice, before moving on to discuss the specific challenges and opportunities when it comes to reforming data control around health data.

3.1 User empowerment

One notable attempt at envisioning and outlining DCD through a new schema of personal data management, in which humans are at the centre and in control of their own personal data ecosystems, is called MyData. Developed openly and collaboratively, the concept originated with the Open Knowledge Finland working group and was expanded in a white paper written primarily by researchers at the Helsinki Institute for Information Technology and the Tampere University of Technology and sponsored by the Finnish Ministry of Transport and Communications [40]. MyData is unique in that it is not one specific data management tool or digital service. Rather, it is a set of principles defining what "humancentric" data management looks like and how it could be enacted with the technological solutions at hand. The MyData principles include:

- **Human centric control over data**: people have a right to access their personal data and control their privacy settings, as well as the means necessary to enact these rights;
- **Usable data:** People can get access to their personal data held by companies, governments, or other third parties in a format that is machine-readable, open, and accessible via application programming interfaces (APIs) and open standards;
- **Open business environment**: by complying to a common set of personal data standards, business and services make it possible for people to exercise freedom of choice between interoperable services, preventing the current scenario where people get "locked" into silos of services owned by a single company because they cannot export their data and take it elsewhere. [40]

These principles have been iterated and manifested in many initiatives around the world by researchers, technologists, entrepreneurs, and activists who are trying to rethink and reform the current personal data management paradigm.[19] In this perspective, Searls [47] argues that the shift towards a different data-management paradigm will prompt a new age of consumer empowerment fuelled by new tools and standards that will facilitate an unprecedentedly demand-driven market. In such context, individuals will have personal power in their relationships with providers and producers and vendors thanks to the utilisation of tools allowing them to:

a) "*Manage relationships with organizations;*
b) *Make individuals the collection centers for their own data, so that transaction histories, health records, membership details, service contracts, and other forms of personal data are no longer scattered throughout a forest of silos;*
c) *Give individuals the ability to share data selectively, without disclosing more personal information than the individual allows;*
d) *Give individuals the ability to control how their data is used by others and for how long. At the individual's discretion, this may include agreements requiring others to delete the individual's data when the relationship ends;*
e) *Give individuals the ability to assert their own terms of service, reducing or eliminating the need for organization-written terms of service that nobody reads and everybody has to "accept" anyway;*
f) *Give individuals means for expressing demand in the open market, outside any organizational silo, without disclosing any unnecessary personal information;*

[19] In addition to the projects discussed in further detail later in this paper, some cursory examples of initiatives that are intended to shift the personal data management paradigm include: 1) the QIY Foundation, which is a consortium of private and public organisations based out of the Netherlands. The QIY Foundation has developed a technology protocol and scheme of principles that are designed to help members of the consortium cooperate in a way that gives people who use their services control over their data. 2) The midata vision, which was published under the United Kingdom's 2010 to 2015 coalition government to announce a voluntary partnership between 26 public and private organizations. The midata vision was created for the purpose of giving individuals access to their personal data on request, in machine-readable format, and in a safe way. [28, 51] 3) The Meeco digital service, built by a private company based out of Australia to help individuals add, organise, edit, and share their personal information on one secure platform. 4) The Midata.coop initiative, which is led by researchers experimenting the creation of regional cooperatives that allow people to store, manage, and control access to their health-related personal data through a combination of open source software and government regulations. [18] 5) The Custumer Commons project, aiming to develop a suite of legal terms and visual icons for individual people to set the terms for how their data can be shared and used by second and third parties, in the model of how Creative Commons terms work for copyright law. [48, 49] 6) Datamixers, an online start-up company based out of Belgium, which provides a platform for customers to access their personal data from different sources.

g) *Base relationship-managing tools on open standards, open APIs (application program interfaces), and open code;*
h) *Make relationships work both ways.*"

Such elements are also in the process of concrete implementation through initiatives such as ProjectVRM of the Berkman Klein Center for Internet and Society, where "Vendor Relationship Management" systems are being developed to give customers increased control over their commercial relationships by using protocols like JLINC. This protocol provides an automated schema for data to be shared according to terms established by the customer. [48, 49] In the same perspective, Sir Tim Berners-Lee, also known as the father of the World Wide Web, has also turned his focus to the question of personal data ownership with a project called Solid, which he is leading at MIT and the Qatar Computing Research Institute. The purpose of project Solid is to use W3C standards and protocols to give users control over who can access their data as well as where their data reside, thereby allowing users to decouple their data from a specific digital services or platform, preventing data lock-ins and facilitating the secondary use of data. [10] It is important to stress that the work of Doc Searls, Tim Berners-Lee, and other initiatives are all chipping away from different angles at the same issue. The shared concern is indeed how to create a future in which the increased presence of data-based digital platforms in people's everyday lives gives people, even those with limited digital literacy, more power over their lives, thus allowing them to regain informational self-determination.

In a networked environment saturated in overlapping software platforms, it becomes increasingly difficult to monitor who has access to one's personal data and to manage the porous boundaries between the public and the private spheres. In this regard, it is interesting to note Siva Vaidhyanathan's [53] new conceptualisation of privacy for the digitally networked world. Building upon Julie Cohen's "social value of privacy" [9], Vaidhyanathan asserts that an accurate definition of privacy is not the ability to exercise autonomous control over information about our lives. Rather, "it more accurately comprises the ways we manage our various reputations within and among various contexts," keeping in mind that these contexts are intersecting and overlapping in a digital world. While the prospect of individual people successfully managing their reputations within fluid digital contexts seems challenging, technology and standards experts have been working to create novel approaches that give users simple, centralised control over the dissemination of their data, such as the Kantara Initiative's User-Managed Access (UMA) protocol. [29] By basing data control around standardised, user-driven protocols that give users the ability to explicitly consent to how personal data is disseminated and accessed, the UMA protocol has provided the technological standard to facilitate a new model of data control.

The sophistication and proliferation of solutions to the quandaries of providing user-managed data control in a networked environment show that it is possible to implement data control by design if such approach is established as a priority for private and public organisations that manage personal data. There are numerous technology start-ups trying to create digital solutions that may successfully help people implement "data sovereignty"[20] by aggregating, securing, and even monetising their personal data across different platforms. While privacy is a major feature for such personal data management tools, monetisation of personal data is perhaps an aspect of these services that is attracting more interest and attention. One of the main purposes of services like Datacoup[21] and Meeco[22] is indeed to provide secure APIs for users to aggregate disparate personal data streams and monetise them. Such projects are based on the consideration that companies are currently paying intermediaries, known as "data brokers," for data profiles about potential consumers, hence consumers could potentially become their own data brokers and be paid directly for letting companies access data about themselves and their habits. In accordance with this perspective, a start-up called DataWallet[23] has proposed to remunerate individuals for the data profiles that they provide through social media, and it reached a queue of over 20,000 people waiting to test the beta version after it launched in 2016. [23]. It seems also important to stress that diverging views exist on this matter and it has been frequently argued that monetising data implies the monetisation of the human right to privacy. [21] In this sense, data monetisation may lead to different levels human rights protection depending on the economic conditions of an individual, in light of the fact that less financially-capable individuals may be more inclined – or have no option other than – to sell their personal data to have access to services.

In any respect, it is essential to note the abundance of ideas, products, and services being generated around a new understanding of data control, driven by Internet users in a bottom-up fashion. Such proliferation of DCD implementations certainly indicates that the future can bring changes to the power and cost structures of the current personal-data marketplace. Furthermore, the emergence of DCD approaches, indicates the increasing consolidation towards a multistakeholder approach to data privacy, in which users undertake a fundamental role both in the design and implementation of data protection tools and strategies. This

[20] The term "data sovereignty" has been employed to mean different things. Katryna Dow, the CEO and Founder of the personal data management start-up Meeco, has publicly adopted the term as a tagline for the mission of the company, defining it as the concept that an individual's personal data and information should belong to them. See https://meeco.me/why-meeco.html

[21] Co-founder and CEO of Datacoup Matt Hogan describes Datacoup as a personal data marketplace where users can aggregate and sell their data See PSFK Labs [42].

[22] Meeco is a service intended to help users organise, edit, share, encrypt, and search their personal information across devices. See https://meeco.me/

[23] Founded with angel funding from Tim Draper and Marc Benioff, DataWallet is a free application that launched with a closed beta version in June 2016.

evolution evokes a fundamental change in the way data privacy is or should be framed,ascribing an active role to users. In this perspective, users – and start-up innovators – proactively design tools allowing individuals to regain control on their personal data. Such tools should be both man-readable, i.e. being easily utilisabled by non-expert users, and machine readable, i.e. being compatible and understandable for any service or device in an interoperable fashion. The collaboration of different stakeholders is therefore essential to allow DCD solutions to function. Indeed, public policies should incentivise the development and use of such tools both by individuals and business actors.

However, it is also relevant to stress that certain domains, notably the health-data management, deserve special consideration due to the existence of particularly sensitive issues around privacy and data management. Such considerations will be analysed in the following subsection and further expanded in Section 4.

3.2 Health data

The prospect of using big data analytics, wearable devices and embedded technologies to revolutionise healthcare has engendered both great hopes and great fears. Respondents to a recent Pew Research Center study expressed their concern that new technologies facilitating biomedical developments would become available before they have been sufficiently tested to understand their impact, reflecting a lack of faith in the marketplace to regulate the advancement of sensitive biomedical technologies in a positive direction [14]. In this regard, it can be argued that moves to computerise and centralise the collection of health data may further exacerbate the monitoring of individuals, increasing the chances of potential abuses. Despite concerns, however, there are many movements across the public and private sectors to use sophisticated big data analyses as a tool to improve the quality and the reach of healthcare services.

A cursory survey of cutting-edge health data initiatives shows some notable trends. Firstly, the healthcare systems are going to be increasingly centralised in a way that lets people be informed and receive quality healthcare across geographic borders i.e. allowing individuals to access their up-to-date health records regardless of whether they are seeking care outside of their local or national healthcare provider.[24] Secondly, big data analytics, combined with genetic and biometric data mapping[25] are going to be progressively used to spot trends and patterns across vast troves of medical data in a way that improves diagnoses and treatments and gives people the option to crowdsource the diagnose of their symptoms and find the appropriate cure.[26] Thirdly, life-style tracking devices analysing personal data are going to be matched with incentive programmes promoting healthier lifestyles, and utilised by insurance companies.[27] All of these trends present their own challenges and opportunities and one of the chief challenges is how to control the access and sharing of sensitive health data after they have been collected. This concern is especially intensified by the power asymmetries between data subjects and the companies that collect their data and subsequently share them with third parties. [44].

With the goal of putting forward concrete solutions to the aforementioned concerns, the Digital Health Revolution project was launched in Finland to further human-centric control over health data according to the MyData principles in a way that facilitates innovations around health data without compromising data control.[28] Likewise, in Switzerland, HealthBank was launched as a cooperative start-up that aggregates and analyses health data, while also guaranteeing data security and giving the user the ability to manage who can access their health data. Although, it is too early to assess whether these types of initiatives will successfully empower individuals and mitigate the risks linked to the automated collection and processing of health data, the proliferation of such initiatives seems to indicate growing interest from developers, users and market. However, it should be noted that a major not only from country to country but also within different parts of the same country.[29] [45] Therefore, legal fragmentation remains a key impediment to borderless health technologies, due to localised, diverse, and complex legislation.

[24] For example, services like NemID, that provides a centralised single interface for e-government services in Denmark (including healthcare), HealthBank, which is a private company whose service consolidates healthcare data management for Swiss citizens, and eIDAS, which is a web protocol designed to provide interoperable identity services, all take different approaches to allowing people to access a dynamic, up-to-date, machine readable version of their health data rather than requesting particular records from past healthcare providers every time they use a new healthcare provider.

[25] 23andMe is a privately owned, direct-to-consumer commercial online genetic testing service and Promethease is program that reanalyses genetic testing results from companies like 23andMe based on public genetic data [44].

[26] For example, HealthTap is a mobile health start-up that allows people to consult remotely an interactive community of physicians; WebMD is a service that provides access to medical information and research through one online access portal; The Figures Janascript Library generates graphical representations of health data [26]; and OneDrop offers a mobile diabetes management tool.

[27] Programmes like Castlight health, the Chevron Wellness Program, Apple HealthKit, CipherHealth, and the John Hancock Vitality program all utilise automated data collection methods, like smartphone-based step trackers, sleep tracking applications, and food diaries to incentivise people to track and quantify their everyday activities for the purpose of altering behaviour in a way that optimises their personal health. The incentive mechanisms of these services range from the simple appeal of gamification to monetary rewards.

[28] Digital Health Revolution is a partnership between universities and research centres across Finland that are actively researching and prototyping new healthcare data systems and services that operate in accordance with the MyData principles of data security, interoperability, and usability.

[29] In an American Medical Informatics Association white paper advocating the creation of a national framework for the secondary use of health data in the United Sates, Safran et al. explain that, while there would be many benefits to the secondary use of health data, "secondary use of health data poses technical, strategic, policy, process, and economic concerns related to the ability to collect, store, aggregate, link, and transmit health data broadly and repeatedly for legitimate purposes. Thus, lack of coherent policies and standard "good practices" for secondary use of health data impedes efforts to transform the U.S. health care system." [45]

Baking data control into health technologies by design and providing interoperable data-control tools to users seems therefore key to implementing health services that ethically take advantage of the potential of current and future data-driven technologies without creating situations in which users' highly sensitive medical data is compromised or people are discriminated against based on their health profiles. Hence, it is important to reiterate that DCD and PbD are not mutually exclusive but, on the contrary, they mutually reinforce reach other. Indeed, DCD allows to properly implementing PbD, promoting user-driven data control through transparency as to how personal data can be accessed and used; allowing individuals to explicitly consent to data access, use, and share and affording the possibility to move data from one service to another without data lock-ins.

In the following section, we will try to analyse the considerations developed above from the perspective of health-data and genetic-data protection. These fields deserve special attention not only for the particular sensitivity of health and genetic data but also, and mainly, because the collection and processing of such data may have both ground-breaking effect in terms of medical discoveries as well as nefarious social and ethical consequences.

4 Specificities on consent for health and genetic data

Individuals are increasingly organising their lives based on supposed "health information" found online or with the assistance of mobile applications that track their routines. If in the past only health professionals examined patients, building and honouring trust relationship in accordance with deontological codes, nowadays, more and more data systems can process vast amounts of data from each person to recognise potential diseases and provide results that an individual may not even be looking for. In such a context, the expression of an informed consent becomes increasingly challenging because, frequently, the meaning of the collected medical data and the purpose for which they could be used may only be established after the collection. Health-data mining is therefore considerably contributing to highlight the fragility of the N&C approach, due to the difficulty of predetermining the purpose for which the data could be used, thus making it extremely ambitious to express informed consent.

However, it must be noted that health-data mining is opening important business opportunities, prompting substantial innovation in healthcare. Particularly, a data-mining process known as "precision medicine" is considered as a cutting-edge technique in health-data analytics and countries such as the U.S.[30] and UK[31] are investing heavily in research aimed at facilitating its development. Precision medicine is based on mining datasets encompassing the individual's genetic, health and lifestyle data, with the aim of recognising specific patterns of illness and nurturing research in prevention techniques. Such inference can be revealed through big data analytics, while simultaneously allowing to precisely defining how each person reacts to medication and treatment according to their specific profile [33]. The hope is that the synchronisation of these datasets through data-science methodologies will allow the provision of more personalised and effective health-care.

As in other areas of study, the way in which medical understanding is constructed lends itself well to be enhanced by big data analytics, which make the identification of individual and collective patterns increasingly possible and effective. More and more information about an wider number of people is available and can be processed and analysed using observable patterns, based on, for example, Google searches of symptoms and diagnoses,[32] hospital notes and health plans, and even genetic diagnoses provided by companies such as 23andMe,[33] pointing to new ways of producing knowledge in the area of medical science. Hence, the possibilities of collecting and processing genetic and health data, besides data on individuals' lifestyle is increasingly "total." [34] This trend has been identified as "the best problem"[35] to be studied by specialists in the fields of data processing and profiling.

Precision medicine promises to overcome important limitations in medical science and offers truly significant advances, but this technique, together with many other health-data management solutions, presents data-misuse risks that should not be underestimated. Policymakers are starting to address the responsibilities of the new medical intermediaries, elaborating specific guidelines such as the Council of Europe Recommendation on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests, adopted in October 2016.[36] However, in cases where the informed consent is necessary, the problems addressed in the first part of this article with regard to the N&C approach still demand the elaboration of more

[30] See https://www.nih.gov/precision-medicine-initiative-cohort-program

[31] See https://www.genomicsengland.co.uk/

[32] In Brazil, for instance, Google queries for health-related information are the second most popular searches. See http://cetic.br/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nosdomicilios-brasileiros/

[33] The Direct-to-Consumer tests are available on https://www.23andme.com/

[34] In this context, it becomes useful to utilise the concept of "total control" as proposed by Michel Foucault in his idea of Society of Control in "Discipline and Punishment".

[35] The practice of individual profiling, collecting and automatically processing data to build hypotheses regarding personality and interests, is of great importance to businesses, as personalised advertising at an opportune moment is highly successful in conquering new customers. [27]. Notably, the "dataman" Jeffrey Hammerbache, developer of the software Cloudera, stated that, in his search for "following the smartest people to find the best problem," healthcare is "the best problem by far." See http://bits.blogs.nytimes.com/2013/06/19/sizing-up-big-data-broadening-beyond-the-internet/?_r=0

[36] https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016806b2c5f.

convincing solutions. Notably, the processing of health and genetic data may reveal highly sensitive information for which traditional N&C schemes and many existing PbD approaches may fail to provide appropriate guarantees.

First, health data are intimately linked with the very way persons perceive themselves and structure their sense of identity. [19] The manner some genetic mutations are presented during Direct-to-Consumer genetic testing,[37] for example, will affect how individuals see themselves and the course of a chosen treatment. The discourse itself may create expectations of disease prevention or even of "human improvement." This situation is particularly serious in light of the fact that Direct-to-Consumer genetic testing is not guaranteed to be reliable, because is frequently not backed up with proven scientific conclusions[38] and the approval of regulatory bodies.[39]

Second, institutional decisions could be made to the detriment of individuals, given the propensity for discrimination based on current and potential states of health that may lead to socially unacceptable behaviours. Among the risks of misuse of health data, genetic discrimination is a real concern. In this regard, [15] points out the existence of several cases of actual genetic discrimination including:

a) employers, who do not intend to hire (or even dismiss) professionals who are vulnerable in terms of health, or even those who are at risk of disease;
b) health plans which use the argument of a pre-existing condition to deny assistance;
c) adoption agencies, that, in some cases, make a medical examination, attesting parents' longevity and good health, as a condition of approving adoption[40];
d) schools, taking decision affecting students based on genetic considerations, as recently noted by the U.S. media[41];
e) sport teams, excluding members on genetic grounds, as in the case of the rejection of players from the Brazilian national volleyball team due to the presence of the sickle cell trait. [17]

Furthermore, it seems likely that high impact information[42] may emerge from genetic sequencing or from big data processing of health information.[43] With this in mind, it seems essential to regulate data protection, promoting PbD and privacy by default for data holders and, simultaneously, increase individuals' capacity to express consent through the possibility of controlling how data can be used. The need to go beyond the N&C approach, towards a DCD approach and towards further data-protection education, seems to be corroborated by the behavioural studies arguing that people are merely "boundedly rational" when making decisions [24] and that the expression of consent is particularly problematic in the medical context. [39] As highlighted by O'Neil [39], "consent is particularly problematical in medical practice, because it is commonplace even for patients who are in the maturity of their faculties to find themselves at a time of weakness and distress surrounded by others who seem (and may be) more knowledgeable, whose influence and power are considerable, who they very much don't want to offend. If consent is to be a governing principle in medical ethics, we seemingly need to be ideal rational patients but when we are patients we are often furthest from being ideally rational."

All necessary measures should be taken to ensure that people fully understand the implications that their health data could determine and, when such implications are not predictable, the data subject must be asked to express specific consent. In this sense, it seems essential that data subjects have authentic autonomy in the management of their health data, in addition to be asked to enter N&C schemes or use PbD features. As such, the active involvement in the data subject into the definition and implementation of DCD tools capable of guaranteeing:

a) standardisation of consent mechanisms so that an individual would be able to express consent and define the conditions of the exploitation of certain categories of data, rather than giving consent and manage privacy features every time they are interacting with a different intermediary;
b) that people are informed and educated about how their data may be used and, besides consenting when they feel comfortable, they might also define they preferences of how their data might be used, thus regaining some bargaining power;

[37] Direct-to-consumer genetic testing refers to genetic tests that are marketed directly to consumers via television, print advertisements, or the Internet.
[38] Between 2013 and 2015, the US Food and Drug Administration (FDA) ordered 23andMe to discontinue marketing its personal genome service (PGS), concerned about the potential consequences of customers receiving inaccurate health results. See http://www.nytimes.com/2015/10/21/business/23andme-will-resumegiving-users-health-data.html?_r=0.
[39] In this sense, Genewatch Executive Directore Helen Wallace has stressed that when genetic tests "are not regulated and the science is still poorly understood - so there is a real danger people could be misled about their health" and that her "main concern is that the human genome is set to become a massive marketing scam." See https://www.theguardian.com/science/2008/jan/22/genetics.health
[40] In this hypothesis, a person who has a genetic mutation which presents a threat and who is strongly advised by doctors not to have children would be unable to experience parenthood.
[41] See http://www.wired.com/2016/02/schools-kicked-boy-based-dna/.
[42] High impact information are those which reveal high propensity to certain serious illnesses, such as the presence of the mutation BRCA, which is correlated with breast cancer instances, or the genetic mutation that points to Huntingdon's disease in the future.
[43] This is particularly sensitive in countries where the health system holds employers responsible for providing health assistance to their employees.

c) that the consent and conditions "travel with the data" so that they are adhered to by every entity who gains access to the data.

Lastly, the complexity of the assessments to be made in order to express consent and define preferences with regard to health and genetic data collection and processing brings to attention the growing need for trust in both the data processor and the health professional that should accompany the data subject in her choices. As noted by Hanen (2009), the importance of trust is raising to the detriment of the individual autonomy, given that "a considerable portion of most patients' knowledge of medical matters derives from what they are told by their physicians, and people not medically trained may have difficulty understanding some of what they are told." In this sense, the lower the patient's capacity to understand, the great the need for trust in the health professional. This situation becomes more complicated when it involves people who need to provide consent concerning their health or genetic data for research, as they are generally unable to identify the nature of the information that may emerge. In addition, given the capacity of technological advancements to reveal unpredictable discoveries, it is particularly difficult to explain to the patient the type of information that may emerge from the sequencing of their genetic data and from further research in precision medicine. For these reasons, some initiatives, such as Genomics England, make it clear that the patient must state in advance whether she wishes to know of possible high impact information in her genetic sequencing so that the individual's right not to know is respected.[44]

5 Conclusion

Over the four sections of this paper, we have tried to emphasise the inadequacy of a mere N&C approach in order to guarantee the protection of individuals personal data, we have commended the positive steps determined by PbD but also argued that more could and should be done to empower individuals providing them with greater control on their personal data. Such considerations seem to be corroborated by the current proliferation of initiatives, such as MyData or Solid, aimed at conferring not only greater control but also grater bargaining power to individuals in the definition of how their data can be exploited. The need for an innovative and more user-centric approach to data privacy is further exemplified by the complexity of the current scenario of Big Data in the medical field, where patients risk to be reduced to mere data-producers for health-data mining purposes. As a patient, the person is cared for by a health professional who has a duty to meet specific information standards when obtaining consent and to keep a pact of confidentiality with the patient, in line with deontological codes, imposed by the ethics of medical practice or even by bioethics [22], as well as legal provisions of privacy and data protection. When the patient turns to be a simple consumer of health applications, the bond of trust between the patient and the health professional no longer exists and the duty to care for the patient is lost. Although, it is not yet possible to reasonably foresee how medical care could be transformed with the use of *data driven decisions*, it is important to bear in mind that individuals should always retain control on how their health and genetic data are exploited.

The health and genetic areas tellingly exemplify the insufficiency of N&C due to the quantity and complexity of the information that needs to be analysed and understood in order to express an informed consent regarding data collection and processing. Furthermore, in such contexts, the element of trust becomes increasingly important to construct responsible mechanism and institutions that "only earn their designations as trustworthy if there are feasible procedures by which an individual can check on what is done." (Hanen, 2009) Building trust through a user-centric DCD approach, implemented by initiatives such as MyData, plays a key role in allowing individuals to exert control over their personal data and take autonomous decisions about their lives, thus and freely developing their personalities.

The availability of intelligible information is necessary to carefully consider and to reflect on the pros and cons of giving consent to the collection and processing one's personal data – and, even more importantly, one's health and genetic data – but does not guarantee per se individuals' control on personal data. The proposed DCD approach aims at guaranteeing individuals' privacy, autonomy, dignity and sense of who they are, in an empowering, user-friendly and interoperable fashion. To be workable, a DCD approach requires a multistakeholder effort, involving both technical communities, users and business innovators, developing concrete implementations and promoting the adoption of the approach, but also public and private players developing policies and their – technical and organisational – architectures in a DCD-compatible fashion. The current evolution of privacy frameworks seems to have already acknowledged the limits of N&C, tending towards a more realistic protection of privacy through PbD. DCD has the potential to complement and enhance PbD. The question seems to be, therefore, what stakeholder will be the driving force of the DCD approach.

[44] The guarantee of the right not to know does not resolve the complexity of the question in that. Even if a person states that he/she does not want to know, in cases where a possible genetic mutation has to be or probably will be shared with blood relatives, they may demand the right to be informed, particularly in cases where treatment is available. For this reasons, in some contexts, the familial consent is discussed. "However, familial versions of informed consent could not be instituted without obstructing individuals who for medical or other reasons seek information about their own genetic status, yet lack familial consent to do so" [39].

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

Funding There is no funding source.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent Informed consent was obtained from all individual participants included in the study.

References

1. Acquisti A. (2010). The Economics of Personal Data and the Economics of Privacy. Joint WPISP-WPIE Roundtable. Background Paper #3. OECD Conference Centre. https://www.oecd.org/sti/ieconomy/46968784.pdf.
2. Belli, L. & Venturini, J. (2016). Private ordering and the rise of terms of service as cyber- regulation. Internet Policy Review, 5(4). https://policyreview.info/node/441/pdf.
3. Belli, L. and Foditsch, N. (2016) "Network Neutrality: An Empirical Approach to Legal Interoperability", in Belli, L. and De Filippi, P. (Eds.) Net neutrality compendium: human rights, free competition and the future of the internet. Springer.
4. Blank G, Bolsover G, Dubois E. New privacy paradox: young people and privacy on social network sites. Global Cyber Security Capacity Centre: Draft Working Paper; 2014.
5. Cannataci, J. (2016). Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci. A/HRC/31/64.
6. Cattaneo G. et al. (2015). European Data Market SMART 2013/0063. D6 — First Interim Report.https://idc-emea.app.box.com/s/k7xv0u3gl6xfvq1rl667xqmw69pzk790.
7. Cavoukian A. Privacy by design: the 7 foundational principles. Ontario: Office of the Information and Privacy Commissioner; 2009. Retrieved May 30, 2016 from https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf
8. Cavoukian A. and Prosch, M. (2011). Privacy by ReDesign: Building a Better Legacy. http://privacybydesign.ca/content/uploads/2010/11/ PbRD.pdf.
9. Cohen JE. Configuring the networked self: law, code, and the play of everyday practice. New Haven, CT: Yale University Press; 2012.
10. Conner-Simons A. Web Inventor Tim Berners-Lee's Next Project: A Platform that gives users control of their data. 2015; In MIT CSAIL. http://www.csail.mit.edu/solid_mastercard_gift
11. Cooper, et al. Privacy considerations for internet protocols. RFC. 2013;6973 https://tools.ietf.org/html/rfc6973#ref-PbD
12. ENISA (2014). Privacy and data protection by design. From policy to engineering. https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.
13. European Commission (2015). Special Eurobarometer 431 "Data Protection." http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf.
14. Funk, C., Kennedy, B., & Podrebarac Sciupac, E. (2016). U.S. Public Wary of Biomedical Technologies to 'Enhance' Human Abilities. Pew Research Center. http://www.pewinternet.org/2016/07/26/u-s-public-wary-of-biomedical-technologies-to-enhance-human-abilities/.
15. Geller, L. et al. Individual, family, and societal dimensions of genetic discrimination: a case study analysis. In: ALPER, J. et al. (Eds.). The doubleedged helix: social implications of genetics in a diverse society. Baltimore: The Johns Hopkins University Press, 2002. p. 247-266.
16. Gjorgievska, A. (2016). Google and Facebook lead digital ad industry to revenue record. Bloomberg Technology. https://www.bloomberg.com/news/articles/2016-04-22/google-and-facebook-lead-digital-ad-industry-to-revenue-record.
17. Guedes, Cristiano & Diniz, D. (2007). Um caso de discriminação genética: o traço falciforme no Brasil. PHYSIS: Rev. Saúde Coletiva, Rio de Janeiro, 17(3):501-520, 2007 Available at http://www.scielo.br/pdf/physis/v17n3/v17n3a06.pdf.
18. Hafen E, Kossmann D, Brand A. Health data cooperatives - citizen empowerment. Methods Inf Med. 2014;53(2):82–6. doi:10.3414/ME13-02-0051.
19. Hanen, Marsha. (2009). Genetic Technologies and Medicine: Privacy, Identity, and Informed Consent. Lessons from the identity trial: Anonymity, Privacy and Identity in a Networked Society. Available on http://idtrail.org/content/view/799.html.
20. Hull G. (2015). Successful failure: what Foucault can teach us about privacy self-Management in a World of Facebook and big data. In Ethics and Information Technology 17(2).doi:10.1007/s10676-015-9363-z.
21. Jerome, J. (2013). Buying and Selling Privacy: Big Data's Different Burdens and Benefits Available on http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=1513383.
22. Junges, José Roque. Recktenwald, Micheli. Hebert, Noéli Daiãm Raymundo. Moretti, Andressa Wagner. Pereira, Bárbara Nicole Karlinski. (2015) Sigilo e provacidade das informações sobre usuário nas equipes de atenção básica à saúde: revisão. Revista Bioética: 2015–23 (1). Available on http://revistabioetica.cfm.org.br/index.php/revista_bioetica/article/view/1000.
23. Kellogg, B. (2016). DataWallet Launches to Empower Consumers to Claim the Profits Made with Their Data. prweb. http://www.prweb.com/releases/2016/06/prweb13479668.htm.
24. Kerr I. et al. (2009). Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent. Lessons from the identity trial: Anonymity, Privacy and Identity in a Networked Society. Available on http://idtrail.org/content/view/799.html.
25. KPMG. The internet of things: should We embrace its full potential? Cyber Insights Magazine: Edition. 2015;3 https://assets.kpmg.com/content/dam/kpmg/pdf/2016/04/ch-the-internet-of-things-en.pdf
26. Ledesma A, Al-Musawi M, Nieminen H. Health figures: an open source JavaScript library for health data visualization. BMC Medial Informatics and Decision Making. 2016; doi:10.1186/s12911-016-0275-6.
27. Louzada, L. (2015). Bancos de Perfis Genéticos para fins de investigação criminal: reflexões sobre a regulamentação no Brasil. Dissertação de Mestrado. Programa de Pós-Graduação em Ciências Sociais e Jurídicas da Universidade Federal Fluminense (PPGSD/UFF).
28. The midata vision of consumer empowerment. From the Department for Busniess, Innovation & Skills and The Rt Hon Edward Davey. 2011; https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment
29. Machulak, M. P., Maler, E. L., Catalano, D., & Van Moorsel, A. (2010). User-managed access to web resources. In Proceedings of the 6th ACM workshop on Digital identity management (pp. 35–44). ACM.
30. Mantovani E, Quinn P, Guihen B, Habbig A, De Hert P. eHealth to mHealth – a journey precariously dependent upon apps? European Journal of ePractice. 2013;20:48–66. http://www.vub.ac.be/LSTS/pub/Dehert/461.pdf

31. McDonald A.M. and Cranor L.F. (2008). The Cost of Reading Privacy Policies. In I/S: A Journal of Law and Policy for the Information Society. 2008 Privacy Year in Review issue.
32. Mitchell A. From data hoarding to data sharing. Journal of Direct, Data and Digital Marketing Practice. 2012;13(4):325–34. doi:10.1057/dddmp.2012.3.
33. Nebert D, Bingham E. Pharmacogenomics: out of the lab and into the community. Trends Biotechnol. 2001;19(12)
34. Obar J. A. and Oeldorf-Hirsch A. (2016). The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services http://ssrn.com/abstract=2757465.
35. OECD. (2013a). Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value. OECD Digital Economy Papers, No. 220. OECD Publishing. Paris. doi:10.1787/5k486qtxldmq-en.
36. OECD. OECD skills outlook 2013: first results from the survey of adult skills. OECD Publishing. 2013b; doi:10.1787/9789264204256-en.
37. OECD. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. 2013c; http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
38. OECD. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. 1980; http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
39. O'Neil O. Informed consent and genetic information. Studies in History Philosophy of Biology and Biomedical Sciences. 2001;32(4)
40. Poikola, A., Kuikkaniemi, K. and Honko, H. (2015). "MyData: A Nordic Model for human-centered personal data management and processing." Finnish Ministry of Transport and Communications. http://www.lvm.fi/documents/20181/859937/MyData-nordic-model/2e9b4eb0-68d7-463b- 9460-821493449a63?version=1.0.
41. Rainie, L. (2016). The state of privacy in America: what we learned. Pew Research Center. http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/.
42. PSFK Labs. Creating a Transparent Marketplace for Personal Data. 2015; http://www.psfk.com/2015/08/personal-data-datacoup-personal-information-marketplace-matt-hogan.html
43. Ramirez, A., Brill, J., Ohlhausen, M., Wright, J. and McSweeney, T. (2014). Data brokers: a call for transparency and accountability. Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
44. Ruckenstein M. Keeping data alive: talking DTC genetic testing. Information, Communication & Society. 2016:1–16. doi:10.1080/1369118X.2016.1203975.
45. Safran, C., Bloomrosen, M., Hammond, W.E., Labkoff, S., Markel-Fox, S., Tang, P., & Detmer, D. (2007). Toward a National Framework for the secondary use of health data: an American medical informatics association white paper.
46. Santosuosso A. and Malerba A. (2014). Legal interoperability as a comprehensive concept in transnational law. Law, Innovation and Technology 6(1) http://www.tandfonline.com/doi/abs/10.5235/17579961.6.1.51.
47. Searls D. The intention economy: when customers take charge. Cambridge: Harvard Business Review Press; 2012.
48. Searls, D. (2016a). Time for THEM to agree to OUR terms. Customer Commons Blog. http://customercommons.org/blog/.
49. Searls, D. (2016b). At last, a protocol to connect VRM and CRM. ProjectVRM Blog. http://blogs.harvard.edu/vrm/2016/08/18/at-last-a-protocol-to-connect-vrm-and-crm/.
50. Schwartz P.M. & Solove D.J. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. N.Y.U. L. Rev. 86.
51. Shadbolt N. Midata: towards a personal information revolution. Digital Enlightenment Yearbook. 2013:202–24.
52. "User-Managed Access (UMA) Profile of OAuth 2.0". Retrieved on 30 September 2016 from https://docs.kantarainitiative.org/uma/rec-uma-core.html.
53. Vaidhyanathan, S. (2015). The rise of the Cryptopticon. The Hedgehog Review 17(1). http://www.iasc-culture.org/THR/THR_article_2015_Spring_Vaidhyanathan.php.
54. Van Blarkom G.W., Borking J.J. and Olk J.G.E. (2003). Handbook of privacy and privacy-enhancing technologies the case of intelligent software agents. PISA Consortium.
55. Van Rossum H, et al. Privacy-enhancing technologies: the path to anonymity. In: Registratiekamer, the Netherlands, and information and privacy commissioner. Ontario: Canada; 1995.
56. Venturini, J. et al. (2016). Terms of service and human rights: an analysis of online platform contractual agreements. Revan Editor. http://internet-governance.fgv.br/sites/internet-governance.fgv.br/files/publicacoes/tos_0.pdf.
57. World Economic Forum. Personal Data: The Emergence of a New Asset Class. 2011; http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf
58. Williams F. (2006). Internet privacy policies: a composite index for measuring compliance to the fair information principles.
59. Weber, R. (2014). Legal interoperability as a tool for combatting fragmentation. GlobalCommission on Internet Governance, Paper Series n°4. https://www.cigionline.org/sites/default/files/gcig_paper_no4.pdf.
60. Ziegeldorf JH, Garcia Morchon O, Wehrle K. Privacy in the internet of things: threats and challenges. Security and Communication Networks. 2014;7:12. doi:10.1002/sec.795.