Consent and the illusion of autonomy in EU data protection: the necessary utopia

Gaia Manganello (s2180308)
Media Technology MSc program, Leiden University
August 2020
Thesis advisor 1: Peter van der Putten
Thesis advisor 2: Maarten Lamers

EU data protection laws are premised on a view of users as competent and rational agents, who are able to autonomously oversee the processing of their personal data; accordingly, the consent of the data subject has consistently played a major role in determining the lawfulness of the processing. The increasing sophistication of the environment repeatedly lead policymakers to amend conditions for consent, in order to ensure that its giving resulted from an actually informed and conscious decision; however, research shows that choices made by users are typically far from being autonomous, in that they are usually neither informed nor rational. This problem becomes even more significant if one considers that the right to data protection is recognised as fundamental in the EU, and that for this reason, consent to data processing represents the functional expression of the data subject's freedom and dignity. The present research is divided in two parts: in part 1, a review of the scientific literature is carried out, and the obstacles to meaningful consent are pinpointed and clustered; in part 2, the significance of the detachment of consent theory and practice is explored, and alternative approaches to consent are evaluated through scenario planning. The emerging implications provide the basis for a general discussion on the challenges of data protection as a fundamental right.

Keywords*: European Union, public policy, fundamental rights, data protection, data processing, ePrivacy, GDPR, privacy policies, consent, problems, individual autonomy, informational self-determination, privacy paradox, cognitive biases, bounded rationality, compliance*

Part 1

Data protection in practice: Recurrent problems in the evolution of consent to data processing

Abstract: *In the progressive development of European data protection laws, the consent of the data subject was consistently designated as a valid legitimating ground for the processing of personal data. However, due to a variety of reasons, research has frequently called into question the meaningfulness of consent given in digital environments, which is particularly concerning in light of the fact that the right to data protection is recognised as fundamental in the EU. Drawing from legal and academic documents, the present review analyses the development of the notion of consent over time, referring to existing literature to pinpoint the main models, on the basis of which persistent problems are then identified, clustered and discussed. What emerges from this inquiry is that, although the EU framework theoretically sees consent as an act of autonomy and as the functional expression of freedom and dignitaries values, this view is not reflected in common practice: empirical data show in fact that users are often compelled to make choices upon which they are not able or willing to deliberate, and for this reason typically end up giving their consent without even reading notices. The appreciation that certain problems have maintained constant relevance over time casts doubts on the strategic choices underlying the EU approach to consent; possible implications and future directions are discussed.*

1. Introduction

Advances in data processing and increasing degrees of media convergence made it possible for companies to easily extract personal information from Internet users and analyse it with the aim of improving advertising techniques, so as to provide their customers with targeted services and products better tailored to their behaviours. While, on one hand, this enables users to find meaningful offers faster and with greater ease, as well as allowing companies to reduce wastage, a number of concerns were raised over time by the scientific community and international organisations with regard to possible privacy violations (Jensen & Potts, 2004[1]; Acquisti et al., 2015[2]; Carolan, 2016[3]). In the context of European legislation, the protection of personal data is recognised as a fundamental right, in accordance with article 8 of the Charter of Fundamental Rights of the European Union[4], and is today mainly safeguarded by the junction of Directive 2002/58/EC (hereafter ePrivacy Directive)[5] and Regulation (EU) 2016/679 (better known as the General Data Protection Regulation - hereafter GDPR)[6]. In conformity with these documents, provided that the data subject has consented to the use of his/her data, the processing can be deemed lawful; yet, especially in online environments, it seems rather hard to establish whether the giving of consent results from an actually meaningful choice. In fact, the reported behaviour of users towards their privacy preferences is often incongruous with their stated intentions, and understanding the causes of this phenomenon appears crucial to the adequate appraisal of potential privacy risks.

Earlier notions of consent to data processing contemplated user passivity as a satisfactory indicator of consent, and ended up legitimating instances of processing that were later recognised as wrongful or unethical (e.g. the opt-out approach). Overall, the relevance of the legal conception of consent was often compromised by the ambiguity of provisions in digital environments and by the rapid emergence of new fields of application, and for this reason, conditions for consent validity were gradually made more specific over time[3].

According to the most recent definition laid down in the GDPR, consent is "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*"[6]. With this more detailed framing, European policymakers attempted to ensure that consent may not be inferred from passive behaviour, but rather results from an active and informed choice made by the data subject. As it turns out, however, even if the GDPR imposed stricter criteria for transparency on data controllers and gave users more control over their privacy preferences, like previous laws it is based on the assumption that users are competent, rational agents; though consent in this regulation is

theoretically rooted on a much greater framework of protection and consent is only one of the possible legitimating bases of the processing, it is still grounded on the supposition that users are able to oversee the processing of their personal data, which was often disputed by the scientific community.
The purpose of this literature review is to analyse the grounds upon which each model of consent was put forward and to assess the empirical relevance of newly-introduced provisions with respect to scientific research on user behaviour and web heuristics; based on these premises, the main weaknesses of each approach will be pinpointed and discussed in the search of persistent problems and eventual research gaps.
The rest of this paper is structured as follows: in section 2, the problem is articulated and the relative research questions are developed. Section 3 and 4 illustrate which design choices and methodological steps were taken, with respect to the research questions, to conduct the investigation. In section 5, the theoretical background is described and the evolution of the notion of consent is put in perspective with existing scientific research; emerging problems are identified, and those which remain significant are then summarised and clustered in section 6. Section 7 highlights the societal relevance of the matter and exposes potential risks. In section 8, considerations are formulated and possible policy and research directions are discussed. Section 9 sums up matters discussed and draws conclusions.

2. Problem statement & research questions

As stated in the GDPR, in order for data controllers to carry out lawful data processing, at least one of six reported conditions must apply. One of the proxies that can be used to legitimate the processing is the consent of the data subject, meaning that as long as individuals who produce the information agree to the terms proposed to them and controllers can demonstrate the effectiveness of the measures adopted, the processing of personal data can be considered licit (Rec. 42, 74, Art. 6(1a))[6]. In online environments, agreements between data controllers and data subjects usually take the form of privacy policies, terms of service (TOS) or end-user license agreements (EULAs), but there is ample evidence that, despite claiming to care about privacy, most users blindly consent to the processing of their data without even reading policies, and therefore often appear willing to give up more than they could reasonably be expected to. Obar & Oeldorf-Hirsch (2018)[7] conducted an experimental investigation on privacy policy and TOS reading behavior, demonstrating not only that when presented with consent materials, the majority of users doesn't read them, but most notably that consent is generally given even if the terms of the agreement are blatantly invasive; as indicated, 93% of participants agreed to give away their first-born child to a fictitious service provider.
Plenty of studies have sought to identify the various factors leading to the reported passive behaviour at the origin of this phenomenon (sometimes referred to as p*rivacy paradox*) and as a result, a variety of influences were, over time, successfully pinpointed as potential hindrances to the meaningfulness of consent given by data subjects in digital environments.
Behavioural inconsistencies are certainly not the only challenging factors for policymakers who are entrusted with the task of setting out adequate requirements for the validity of consent. With the emergence of novel tools and services, in fact, new unforeseen risks keep originating, which is particularly alarming in light of the fact that data protection is a fundamental right, and that consequently, the digital industry shouldn't be allowed to self-regulate, but clear provisions should instead be laid down by institutions with respect to all the possible fields of application of the consent rule. Unsurprisingly, this duty has proven increasingly complex: in late 2016, on the basis of the issues exposed by a REFIT evaluation, the European Commission started drafting a new regulation (Regulation on Privacy and Electronic Communications, hereafter ePrivacy Regulation)(European Commission, 2017)[8] to better tackle a number of emerging problems related to the protection of personal data and confidentiality of communications and to some unnecessary burdens being placed on the Digital Single Market. Among others, the evaluation found that the most recent model of consent is both over-inclusive and under-inclusive, in such a way that it covers non-privacy intrusive practices while, at the same time, disregarding certain intrusive ones (e.g. device fingerprinting). As subsequently highlighted, the ePrivacy Directive has not fully met its objectives and end-users are not sufficiently empowered by the current provisions; however, more than three years after these results were brought forward, the final draft of the new regulation has yet to be approved by the Council of the European Union.

In line with the current provisions and with official proposals of future ones, the overarching questions of the present review are:

- What problems affected the EU notion of consent over time?
- Was consent practice aligned to theory?

3. Research design

In order to investigate the research questions, this review will adopt a case study design so as to better isolate each different notion of consent and narrow down the main problems carried along by each model respectively. This will be achieved by examining a limited selection of legal acts, each of which represents a distinct approach: the choice of the appropriate documents was operated in relation to existing academic literature (as will be shown) and to the Multiple Stream Framework (MSF) by John Kingdon (1984)[9].
As argued by Kingdon, three streams must meet to allow for new ideas to be included in the political agenda: the problem stream (in which issues are identified), the policy stream (where alternative solutions are proposed by different policy entrepreneurs) and the political stream (through which policymakers acknowledge the challenge and endorse particular decisions); if these streams meet, a policy window opens[9]. Within the sphere of privacy and data protection, since early EU laws started to regard user consent as one of the conditions for lawful data processing, various social and political entrepreneurs managed to draw the attention of policymakers on the issues entailed by such a model, sparking synergy among these streams and triggering the emergence of revised definitions of consent. With this in mind, the opening of three core policy windows was identified: first the model of *presumed consent*, then *informed consent* and finally *active consent*. In accordance with the provisions laid down in the proposal for the new ePrivacy Regulation[8], it will be argued that a fourth model seems to be making its way into the agenda, namely *selective consent*. This process is summarised in Table 1. In line with Kingdon's MSF, this study also contends that, having acknowledged that a number of prominent issues can be pinpointed and that there is evidence of political will to intervene, the flaws responsible for the reported low effectiveness of this model can be inferentially located in the policy stream; solutions proposed and implemented in the agenda so far have built upon each other, which makes it reasonable to suppose that certain problems underlying the earlier notions of consent might still affect current measures.

4. Methodology

Pertinent information was gathered through mixed search and retrieval methods, as different kinds of literary objects were brought together.
As a starting point, the most recent version of the Handbook on European data protection law (2018)[10] was purposively retrieved from the official website of the European Union Agency for Fundamental Rights; the text was navigated in the search for acts and notions related to the word "consent"; useful insights were then isolated and scrutinised more in depth in order to identify key concepts and words (e.g. *privacy, data protection, personal data, data processing, consent, online, cookies, European Union, directive, regulation, policies, notices, informed*). The latter were subsequently randomly combined and used as queries in the search for meaningful academic papers on the Google Scholar online database; to enhance relevance, in some cases publications were filtered in relation to precise time ranges. Literature produced within specific research domains (such as academic papers strictly related to privacy in health care or working environments) was excluded from the analysis.
Inter alia, this exploration led to the recovery of a 2016 review by Eoin Carolan, "*The continuing problems with online consent under the EU's emerging data protection principles*"[3], that dissects the matter with a satisfactory level of detail and facilitates comprehension by breaking up the development of the notion of consent put forward over time in three main models (*presumed*, *informed* and *active*) and tracing each of them to the respective legal acts. Although Carolan's study doesn't make explicit reference to Kingdon's MSF, it illustrates well the main changes undergone by the conception of consent to data processing in the EU and the circumstances that led policymakers to make the relative amendments; however, it was completed just before the GDPR was adopted, and therefore

proposes a limited overview of the current state of the art. The present investigation can be considered, in some respects, a continuation of his analysis.
Additional insights rest on literary materials retrieved as previously indicated on Google Scholar or through snowball sampling.

5. Consent in European privacy policy

The significance of the notion of consent in European data protection laws can be traced back to long-standing philosophical discussions related to the concepts of human dignity and autonomy. Manson & O'Neill (2007)[11] ascribe the origins of the debate on informed consent to the Age of Enlightenment and to the emergence of the theory of social contract, whose core was the belief that freely given consent legitimates actions that would otherwise be unacceptable. The notion of autonomy, in particular, is generally seen as the cornerstone of the conceptual foundation of consent (Kosta, 2013)[12]; in the well-known Kantian sense, autonomy represents an individual's entitlement to choose for themselves and to do so in accordance with their conception of good (Carolan, 2016)[3]. When, in the 19th century, the right to self-determination started to emerge, principles such as individual sovereignty and freedom of choice began to play major roles in legal contexts (Feinberg, 1982)[13]; it is with the Charter of Fundamental Rights (European Parliament, 2000)[4] and the Treaty of Lisbon (European Union, 2007)[14], however, that the right to the protection of personal data gained an independent legal basis in the EU, and consent to data processing was ultimately enshrined within the framework of the ius cogens as the functional expression of fundamental human rights.
In 2011, in response to a request of the European Commission, the Article 29 Working Party issued an Opinion on the definition of consent that aimed to clarify on the requirements for consent to be valid under applicable law. According to this document, the autonomy of the data subject is both a pre-condition and a consequence of consent; however, this principle has limits, and the relevance of consent as an enabler of individual autonomy and self-determination relies on its use in the right context and with the necessary elements. As a matter of fact, consent is not a means for data controllers to transfer liability on individuals, and a fully valid consent does not relieve controllers of their obligations[15].
While it was clear from the very beginning that the notion of consent put forward by institutions was firmly grounded on virtuous principles, it was less clear how these tenets should be respected in practice. The fast and unprecedented development of new technological devices and the growing range of application urged policymakers to set specific requirements for the validity of consent, but the job of setting clear rules on a domain that keeps changing turned out to be a Sisyphean task: shortly after new conditions were adopted, novel IT tools were developed, and legal concepts soon became inadequate or ambiguous.
The evolution of the notion of consent in EU data protection laws is hereby broken down in four main models, each of which was (/will likely be) introduced to supposedly amend particular shortcomings of its predecessor. Hence, we distinguish between *presumed consent* emerging with the Data Protection Directive, *informed consent* with the ePrivacy Directive, *active consent* with the GDPR and finally *selective consent* with the ePrivacy Regulation. Table 1 illustrates the envisioned framework, where each model of consent is categorized on the base of the legal act with which it appeared, the problems expressly addressed and the revised conditions consequently laid out. From a MSF perspective, every emerging notion is paired to the relative decision agenda (i.e., which problems were up for active decision) and its legislative enactment.

5.1 Presumed consent

When *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (European Parliament and Council, 1995)[16] was adopted, the growing degree of public concern around the risks posed to informational privacy by technology-driven changes was given an official voice; recital 4 clearly states that "increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity" and that "the progress made in information technology is making the processing and exchange of such data considerably easier"[16].

	Legal act:	Problems addressed:	Notion of consent:
Presumed consent	Data Protection Directive (1995)	• Increasingly frequent recourse to processing of personal data in social and economic spheres. • Considerably easier processing and exchange. Rec. 4.	**Definition**: Freely given, specific and informed indication of wishes. **Conditions**: • Must be given unambiguously. • Must be explicit for special categories of data. Art 2(h), 7(a), 8(a).
Informed consent	↑ ePrivacy Directive (2002)	• New risks for personal data and privacy posed by publicly available electronic communications services. • Need for specific legal, regulatory and technical provisions in the case of public communications networks (increasing capacity for automated storage and processing). Rec. 6, 7.	**Definition**: See above. **Conditions**: • In the case of electronic communications or value added services, users must be informed of the processing prior to giving consent. • Use of tools such as spyware, web bugs, hidden identifiers is allowed only for legitimate purposes, on condition that users are provided with clear and precise information given through user-friendly methods. • Access to specific content may still be made conditional on the well-informed acceptance of legitimate devices. Art 2(f), 6(3/4); Rec. 17, 24, 25.
Active consent	GDPR (2016)	• Substantial increase in cross-border flows of personal data and exchanges between public and private actors. • Unprecedented increase in the scale of collection and sharing of personal data. • Silence, pre-ticked boxes or inactivity should not constitute consent. Rec. 5, 6, 32.	**Definition**: Freely given, specific, informed and unambiguous indication of wishes given by a statement or by a clear affirmative action. **Conditions**: • Controllers shall be able to demonstrate that the data subject has consented. • If the performance of a contract is conditional on consent to the processing of unnecessary data, consent may not be considered freely given. • Must be explicit for special categories of data and automated individual decision-making. Art 4(11), 7(1/4), 9(2a), 22(2c).
Selective consent	↑ ePrivacy Regulation Proposal (2017)	• ePD failed to keep pace with technological developments (e.g. OTTs). • Harmonisation jeopardised by unclear drafting of provisions and ambiguity in legal concepts. • Users don't understand requests to accept cookies and are sometimes exposed to tracking without their consent. • The consent rule is both under and over-inclusive. Memorandum (Par 1.1, 3.1).	**Definition**: See above. **Conditions**: • Consent may legitimise, inter alia: processing of electronic communications data, use and collection of information from terminal equipment and unsolicited marketing communications. • Consent can be centralised in software such as browsers, but operators can still maintain their current business model. Art. 6(2c/3a), 8(b), 9(1), 16(1); Memorandum (Par 3.4).

↑ = Particularises and complements the above. Table 1.

According to article 2(h) of Directive 95/46/EC, consent is "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"; to further accentuate requirements for this indication, article 7(a) goes on to clarify that consent must be given unambiguously. As stated in article 8(a), in the case of processing of special categories of data, consent must also be explicit.
Furthermore, data subjects are entitled to inquire about the use of their data and to object to it[16].
As pointed out after the directive took effect, even though policymakers made a seemingly valid effort to encourage the voluntariness of consent, the effectiveness of the text was crippled by a fundamental weakness: in fact, the demarcation implied in article 8 suggested that the indication of user consent didn't need to be explicit in order to be lawful, which ended up legitimating passive and non-expressive forms of consent such as user acquiescence (Carolan, 2016)[3]. As a result, although the data subject's consent under the Data Protection Directive was pinpointed just as one of the possible conditions to make data processing licit, it quickly became the most popular proxy used by data controllers to corroborate their compliance. This led to the widespread adoption of questionably permissive opt-out privacy policies, whereby, in the absence of objections, it was by default assumed that users had read and consented to agreements. Unfortunately, the practical effort demanded to average users to exercise their rights turned out to be too high, especially in light of the growing technological sophistication and the complexity of the technical and legalistic language usually featured in privacy policies.
As later reported, insofar as the Data Protection Directive sought to give data subjects the right to autonomous choice, policymakers had clearly overlooked the overarching question as to whether users were actually able to make that decision. Besides, objection to the use of personal data could result in denial of access to a service, undermining altogether the existence of real options[3].

5.2 Informed consent

Right after Directive 95/46/EC was adopted, it became evident that users had such a limited understanding of the online environment (and thus of the possible uses of their data) that it was unrealistic to expect them to resort to the recently set out provisions. In order to redress these issues, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector* (European Parliament and Council, 2002)[5] was later introduced, with the purpose of implementing the Data Protection Directive and repealing other existing legislation; in the wake of Directive 95/46/EC, this new legal text expressly stated the urge to overcome the new range of risks posed to data protection by the development of new digital technologies (Rec. 5, 6)[5]. Whereas the definition of consent remained essentially the same, the 2002 ePrivacy Directive aimed to make sure that the use of emerging technologies such as spyware, web bugs, hidden identifiers, cookies and similar devices may only be allowed if data subjects are appropriately informed on their use, and that the provision of such information is as user-friendly as possible. Furthermore, the new model stressed the importance of an informed choice by requiring data controllers to accurately provide users with the details of the processing of their data prior to obtaining their consent.
The emphasis put on transparency by these new stipulations was coherent with the general view of users as rational and competent agents; however, given that the Data Protection Directive already fell victim to problems stemming from low user pro-activity, it could have been anticipated that the provision of additional information wouldn't necessarily have translated to increased engagement. As maintained by Carolan (2016)[3], it may be argued that the same behavioural insights that inspired this directive also challenge its efficiency: in fact, with the development of new Internet services, even engaged users struggled to understand the potential uses of their data, and policies were still often written with complex language and questionable accessibility standards. As later explained by the Article 29 Working Party (2009)[17], the "complexity of data collection practices, business models, vendor relationships and technological applications in many cases outstrips the individual's ability or willingness to make decisions to control the use and sharing of information through active choice."
To make matters worse, the ePD proposed another risky specification: according to recital 40, unsolicited communications for direct marketing purposes require prior explicit consent, which implicitly validates lower standards for consent in the case of data processed with different purposes. Moreover, recital 25[5] recognises cookies and similar technologies as legitimate tools and authorises their use as long as users are provided with clear and precise information

and have the opportunity to refuse: not only does this still allow for an opt-out-approach in the case of behavioural targeting, but it also justifies the future uses of these devices. Additionally, the same recital goes on to state that website access can be made conditional to the acceptance of these identifiers, suggesting that service providers can resort to the so-called *take-it-or-leave-it* consent requests, whereby service access is denied unless users consent to the precessing of their personal data.
As later acknowledged by a number of European organisations, the ePD overlooked some major issues (e.g. coercive tick-boxes, unnecessary data processing, conditional service access) which impaired the existence of a meaningful choice as well as the voluntariness and value of user consent (Article 29 Working Party, 2009[17]; European Commission, 2010[18]; European Data Protection Supervisor, 2015[19]).
Lastly, the ambiguity of certain legal concepts produced different interpretations of the conditions for consent in the various Member States (requirements varied from written to implicit consent), revealing a strong need for clarification (European Commission, 2010)[18].

5.3 Active consent

Having acknowledged that, in some cases, user consent could be used to legitimise data processing in the absence of the elements constituting its validity and that, in certain cases, even data controllers couldn't be sure whether user silence actually signified acceptance, once again it was evident that some long-known issues were fuelling a persistent problem stream. In the interest of encouraging active user engagement and counteracting the passivity permitted by the two previous consent notions, the model of active consent started to emerge. In an attempt to enhance both data protection rights and digital businesses opportunities, in May 2016 the General Data Protection Regulation[6] was adopted, repealing the Data Protection Directive and particularising and complementing the ePrivacy Directive (European Data Protection Board, 2019)[20].
With the introduction of the GDPR, the right to data protection hit an important milestone: this document, in fact, doesn't just discern between rightful and wrongful instances of data processing, but can be seen more as a data governance framework, and holds at its core the principle of "data protection by design and by default" (Art. 25)[6]. This means that for all those who develop, design, select and use systems that process personal information, data protection can never be a secondary consideration, but shall rather be a forethought. For this reason, consent in the GDPR should be regarded as resting on a layer of protection measures and principles such as fairness and transparency: among others, personal data shall always be processed lawfully, fairly and in a transparent manner, as well as collected for specified, explicit and legitimate purposes (Art. 5)[6].
As in the case of Directive 95/46/EC, user consent under the GDPR must be freely given, specific, informed and must express an unambiguous indication of the data subject's wishes; however, the GDPR specifies that consent is just one of the six bases for lawful data processing (article 6) ergo, as stressed by the Article 29 Working Party (2018)[21], controllers should always take time to determine whether it is the most appropriate lawful ground in relation to each particular instance of data processing. Yet, of all the six lawful bases laid down in the GDPR, consent is the only one that can be used to legitimise processing that is not considered strictly necessary, and while the others only apply if certain preconditions are met, consent can be used a bit as a "Jolly Joker" (Karácsony, 2019)[22].
In keeping with recitals 11 and 32, consent can't be inferred from default browser settings anymore, but it should be obtained at the outset through "a clear affirmative act" such as ticking a box[6]. The GDPR also declares unequivocally the rights of the data subject: according to what stipulated, users have the right to be informed on the processing of their data (prior to it) and eventually object or temporarily restrict it, as well as the right to access data, rectify them, erase them, and where feasible, to have them directly transmitted to other controllers[6]. As per articles 9 and 22, explicit consent is required with respect to processing of special categories of personal data and to automated individual decision-making (e.g. profiling); although consent can't be tacit anymore, it can still be implicit for broader types of data and technologies.
In principle, in view of what already discussed, the shift from a passive model to an active one that calls for user participation stands for a more empirically-sensitive and therefore more effective approach to data protection. Nonetheless, as will be more thoroughly debated in the next sections, it can be argued that, due to certain inherent properties of online environments, active engagement can't be deemed a satisfactory indicator of users' autonomous choices, and much less of their wishes: as has long been recognized, in fact, stronger legal requirements for

consent can result in an overload of consent requests, thus intruding upon service use and burdening users with overwhelming amounts of information (Jesus & Mustare, 2019[23]; Schermer et al., 2014[24]). It is not surprising that information overload was identified as a negative predictor of policy reading behaviour, and that consent materials are commonly perceived as too long, too numerous and taking up too much time (Acquisti et al., 2015[2]; Steinfeld, 2016[25]; Obar & Oeldorf-Hirsch, 2018[7]).
Furthermore, the GDPR provides little if any technical guidance to the entities who are supposed to implement it: Politou et al. (2018)[26] refer to this approach as being "technology agnostic" and claim that because of this ambiguity, few organisations are actually able to demonstrate compliance.
Even conceding that users have the adequate psychological resources to understand consent materials, a number of cognitive biases and heuristics often allegedly impel them to take irrational and privacy-intrusive choices; the act of ticking a checkbox, for example, can itself become a gateway for passive behaviour by starting to be accepted as the default option (Kahneman & Tversky, 1984[27]; Acquisti & Grossklags, 2005[28]; Carolan, 2016[3]; Steinfeld, 2016[25]; Van Ooijen & Vrabec, 2019[29]).
As it turns out, under current data protection laws, most consent notices are usually still quite complex, intrusive and provide either too few or too many options, leading users to perceive them as a nuisance as well as giving them the impression that their choice is not meaningful, for which reason they usually give their consent without reading the terms included (Obar & Oeldorf-Hirsch, 2018[7]; Pardo & Métayer, 2019[30]; Utz et al., 2019[31]).
The problem is further exacerbated by the fact that, though the GDPR doesn't regard as freely given a consent that is made conditional on the acceptance of unnecessary processing (Art. 7), it still allows for consent request techniques that leave users in the absence of a real choice and are therefore commonly regarded as misleading or unacceptable (e.g. clickwrap prompts and tracking walls)(Zuiderveen Borgesius et al., 2017 [32]; Obar & Oeldorf-Hirsch, 2018[7]).
Thankfully, last May the European Data Protection Board (EDPB) released a new set of guidelines on consent that complete and expand upon earlier Opinions issued by the Article 29 Working Party; not only does this new document provide essential clarifications on the validity of consent collected through tracking walls, but it also elucidates on what constitutes unambiguous consent (European Data Protection Board, 2020)[33]. Indeed, as stated by the EDPB, consent can only be an appropriate lawful basis for the processing of personal information if data subjects are offered control and a genuine choice with regard to accepting or declining the terms offered; if, for instance, users are unable to refuse or withdraw consent without detriment, or if consent is bundled up as a non-negotiable part of terms and conditions, consent cannot be deemed freely given. When cookie walls are used, data subjects are not presented with a genuine choice, for which reason the resulting consent can't be considered valid. Besides, although the mere continued use of a service is occasionally considered a demonstration of consent by controllers, the EDPB makes it clear that actions such as scrolling or swiping through a webpage are not distinguishable enough from other user activity, and hence do not, under any circumstances, satisfy the requirement of a clear and affirmative action[33].
That being said, the model of active consent brought forward by GDPR is not exempt from certain remarkable deficiencies; in some respects, as we have seen, it could even be argued that this regulation worsened some of the existing problems, since under current provisions not only do users ignore privacy policies, but they make the active effort to dismiss them.
Finally, despite the fact that consent in the GDPR is envisioned as being part of a greater framework of protection and the entities who process personal data should abide by the tenet of data protection by design and by default, this clearly doesn't ensure that there is compliance. A report called "Out of control" issued in January by the Norwegian Consumer Council (Forbrukerrådet, 2020)[34] analysed the transmission of customer data between ten popular apps running on Google's Android operating system (the largest mobile operating system worldwide) and third party actors, showing the vast extent to which users are illegally tracked and profiled by the adtech industry. As shown in the report, none of these apps provide in fact any meaningful ways of giving or refusing consent to the sharing of personal data with third parties, which were estimated to be at least 135 altogether; considering that all of these actors might have their own purposes of processing, this poses the question as to whether it is even practically possible for such apps to ask for consent in any meaningful way[34].

5.4 Selective consent

As mentioned earlier, in 2016 the European Commission's regulatory fitness and performance programme (REFIT) ran an evaluation that illustrated how the consent rule under the ePD and the GDPR is at the same time under-inclusive and over-inclusive, demonstrating how, due to the fast pace of technology, laws protecting personal data and the confidentiality of communications do not capture the entire range of privacy-intrusive tracking technologies and limit excessively some non-intrusive ones (e.g. first party web-analytics). On top of that, as reported, end-users face requests to accept tracking cookies without understanding their meaning and are even occasionally exposed to cookies being set without their consent (European Commission, 2016)[35].

In light of the issues exposed by the evaluation, soon afterwards the Commission started working on the new ePrivacy Regulation (European Commission, 2017)[8], aimed at particularising and complementing the GDPR and repealing the ePrivacy Directive. After the initial proposal of this regulation was accepted, however, all of the drafts advanced by the Commission have been rejected by the Council, and even though the text was expected to be officially adopted in May 2018, that proved an unrealistic target; to this day, as a matter of fact, the ePrivacy Regulation is still merely a proposal, and it seems like the more time passes, the more controversial this regulation becomes (European Digital Rights, 2019)[36].

Although there is clearly nothing definitive, the preliminary document identifies the main general objectives and explains the rationale driving the drafting of the new provisions. To begin with, the instrument chosen by the Commission is a regulation instead of a directive, for the sake of ensuring consistency with the GDPR and avoiding divergent interpretation in the Member States[8].

Indeed, important technological and economical developments have occurred since the ePrivacy Directive was last amended in 2009 (European Parliament and Council, 2009)[37]; having acknowledged the new risks posed to personal data and confidentiality of communications, as well as the fact that the ambiguity of certain legal definitions has jeopardised the harmony of the market, EU ambassadors now seek to increase trust in the Digital Market by enhancing the security of its services.

To do so, the scope of the ePD will supposedly be extended, meaning it will not only cover traditional communication services, but also Over-The-Top ones (OTTs) like instant messaging apps, Voice over Internet Protocol (VoIP) platforms and machine-to-machine communications such as the Internet of Things (IoT)[8]. Moreover, according to the explanatory memorandum, in order to allegedly empower end-users and simplify the regulatory environment, businesses may centralise consent in software such as browsers and send data subjects occasional prompts about their privacy settings. However, in conformity with the preferred policy option (Option 3), this “does not deprive website operators from the possibility to obtain consent by means of individual requests to end-users and thus maintain their current business model”[8].

As per article 10, when installing electronic communications software, data subjects shall be informed about privacy settings and clearly offered the option to prevent third-parties from accessing and storing information on their terminal equipment. Particular emphasis is put on the broadening of exceptions to cookie consent rules: browsers are encouraged to provide easy ways for users to change privacy settings and to allow them to white/blacklist certain websites, while consent shouldn’t be requested for cookies that actually enable the use of the service requested by the data subject and that involve no, or only very limited, intrusion of privacy (Rec. 21, 24)[8].

The aforementioned arrangements reflect a need to give users better tools to protect their privacy without placing excessive restrictions on the legitimate interests of the digital industry, but it seems as if once again, the strategical problems posed by user passivity remain relevant; regardless whether the rule of consent is extended to new technological domains, we know that if request techniques remain the same, the meaningfulness of consent will still be considerably hampered by the same issues affecting the GDPR. Besides, even if consent management is delegated to browsers or similar software, a whole range of problems could still be overlooked. The centralisation of consent would surely result in a lighter intrusion upon service use, but by the same token, it would call for increased participation from data subjects, as they would have to actively look for the browser’s privacy settings; with user passivity being one of the main weaknesses of consent, this seems like an optimistic expectation. At the same time, even if requirements for transparency are strengthened (e.g. information provided by controllers should not dissuade users from selecting higher privacy settings and should include relevant

insights about the risks associated to accepting third party cookies)[8], it is unclear how this would encourage data subjects to engage in the reading of policies.
As research shows, when it comes to privacy preferences, users often just can't be bothered, and frequently rely on browser extensions like "I don't care about cookies" to get rid of consent requests, explicitly authorising any eventual instance of data processing (Utz et al., 2019)[31]. For this reason, as later highlighted by the European Data Protection Supervisor (2017)[38], the Article 29 Working Party (2017)[39] and the European Economic and Social Committee (2017)[40], it is extremely important, if not crucial, that default settings are privacy-protective (requiring opt-in rather than opt-out). Furthermore, according to these authoritative bodies, given that consent should be freely given and specific, consumers shouldn't be forced to agree to data processing in exchange for service access, and it's necessary that the new provisions explicitly prohibit take-it-or-leave-it choices and tracking walls; additionally, technical settings should be sufficiently granular to allow users to choose particular purposes and providers[38][39][40].
On 1 October 2019, following Case C – 673/17 (the "Planet49" case), the European Court of Justice ruled that pre-ticked checkboxes in consent requests involving cookies are not sufficient indicators of valid consent (European Court of Justice, 2019)[41], which leads us to believe that, in the event that consent is centralised, defaults will presumably require opt-in and will hence be privacy-protective; it remains to be seen, however, how this ruling will affect future proposals.
It is worth noting that, though consent requests should present unequivocal distinctions between first and third-party storage and access, the specificity of consent given to first-parties could be hindered by existent and emerging analytical tools: as soon as some browsers started offering the option to block third-party cookies, in fact, digital services providers began devising new ways of tracking and retargeting user activity. Facebook and Google, for example, already developed new types of beacons and cookies that allow companies to bypass the establishment of a direct first-party relationship with the user (Marvin, 2017[42]; Flynn, 2018[43]).
Moreover, as shown in Fig. 1, many service providers rely on third-parties for basic functionalities such as storing opt-out requests, and users are paradoxically required to allow tracking to not be tracked.

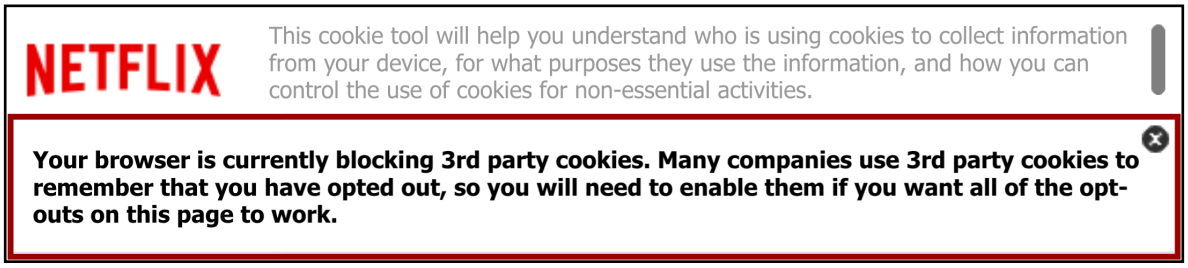

Figure 1.

In view of the matters discussed, the effectiveness of the model of selective consent evidently relies on some pivotal decisions that are yet to be taken by institutions; nonetheless, even in the optimistic scenario that consent is centralised and defaults are made privacy-protective, certain requirements appear still ambiguous and potentially harmful.
The fact that consent is not required for storage and access that are "strictly necessary and proportionate for the legitimate purpose"[8], for instance, casts doubt on what, in practice, makes processing legitimate. In a progress report shared by the European Council in May, it is stated clearly that the legitimate interests pursued by providers are overridden where the fundamental rights and freedoms of the end-users are at stake; for instance, the legitimate purpose ground cannot be used if data are analysed to derive characteristics of end-users and build their profile (Council of the European Union, 2020)[44]. However, as often maintained by Rodotà (2007)[45], the purpose specification principle is being slowly eroded, and data are collected and made available for different purposes that are considered just as important.
As a matter of fact, this principle is rarely honoured in practice: Fouad et al. (2020)[46] performed a large-scale crawling, collecting third-party cookies from 84,658 high-traffic

websites, and found that 95% of the devices examined did not have an explicitly declared purpose and were thus impossible to audit for compliance.
The challenge of ensuring not only the balance of the market, but also the effective protection of fundamental rights becomes ever more sophisticated, but it is yet unsure how exactly all of these issues will be addressed in the future by EU institutions.
The next section presents a comprehensive summary of the problems attributed over time to the consent rule that could potentially remain relevant when the ePrivacy Regulation is enforced, therefore undermining the practical meaningfulness of the EU consent strategy.

6. The enduring problems of consent

We can see how, even though the notion of consent brought forward by institutions was systematically envisioned as the materialisation of individual self-determination and autonomy, its practical application didn't always end up representing these values. Conditions for consent were always intended to grant data subjects the right to a free, informed and specific choice, an indication of wishes made in accordance with one's conception of good; yet, not only did legal requirements legitimate unnecessary or even coercive instances of processing, but they entirely overlooked the possibility that individuals were actually not able to deliberate upon the potential impact of their choice. As already mentioned, academic literature abounds with research that reveals how, although users claim to care about the protection of their personal data, most of them see privacy notices as an obstacle and consent to them without even reading them (Acquisti & Grossklags, 2005[28]; Meinert et al., 2006[47]; Marotta-Wurgler, 2012[48]; Obar & Oeldorf-Hirsch, 2018[7]). This phenomenon is usually called the privacy paradox, and although a variety of theories were proposed as potential explanations, it is still matter of extensive research (Acquisti et al., 2015[2]; Carolan, 2016[3]; Kokolakis, 2017[49]; Gerber et al., 2018[50]; Jesus & Mustare, 2019[23]). Especially in the behavioural sciences domain, there is no shortage of studies that draw attention to the risks associated with certain mistaken assumptions, and the scientific community frequently pointed out that, by reason of the burden that is put on the user side, approaches to online data protection relying primarily on transparency and user control are fallacious, as due to common practices, privacy policies are often unusable decision-making aids (Jensen & Potts, 2004[1]; Nissenbaum, 2011[51]; Acquisti et al., 2013[52]). Although the ePrivacy Directive, the GDPR and the ePrivacy Regulation proposal explicitly call for transparency and user-friendly provision of information, the average user faces multiple challenges when trying to establish who owns his/her data, what kind of information it is and for what purposes it's being stored and processed (Carolan, 2016)[3].
The nature of the problems identified while examining the literature varies, and for the sake of clarity, possibly persistent issues were clustered in three independently relevant macro-categories: according to what reviewed, their character can be considered legal (i.e. depending mostly on policy), practical (i.e. due to factors inherent to the technical environment) and behavioural (i.e. originating from the cognitive biases of data subjects).

6.1 Legal problems

Legal problems essentially depend on the instruments chosen by policymakers and legislators to safeguard the right to data protection, and can be seen as gaps in the relationship between authorities and data controllers; these deficiencies result in ambiguous obligations placed on liable entities and in widespread, unsupervised misconduct.

- *Ambiguity of legal provisions.* EU data protection laws are deliberately technology-neutral in order to enhance their adaptability and prevent the risk of legal obsolescence; said neutrality, however, often results in ambiguous provisions that don't take into account technical feasibility and whose interpretation is left to the data controller (Curren & Kaye, 2010[53]; Hildebrandt & Tielemans, 2013[54]; Kamara, 2017[55]; Politou et al., 2018[26]; Ataei et al., 2018[56]).
  As a case in point, in line with what implied by current laws, both data subjects and data controllers should, at any time, be able to produce evidence of the particular terms for which consent was given; research shows however that, due to how easily certain tools can be manipulated, current practices don't always guarantee indisputable proofs, but strong cryptographic properties are instead needed (Jesus & Mustare, 2019)[23]. A further example is that, according to article 13(e) of the GDPR[6], when data are shared with third parties,

controllers are allowed to only report categories of recipients and not names, so even if data subjects have the right to obtain confirmation as to whether or not their data is being processed (Art. 15), it's often not clear who they should ask that question (Madge, 2017)[57].
Many of the questions emerging from this technology-agnostic stance, such as the validity of consent collected through tracking walls, were over time addressed and answered by the competent authorities (e.g. the Article 29 Working Party or the EDPB), but this sort of corrective approach allows for privacy violations to occur until each particular matter is cleared up (admitting it is). Especially in light of the growing sophistication of the environment, this doesn't seem like an ideal strategy to safeguard a fundamental right; though it might sound counterintuitive, in fact, it is argued that technology-neutral laws may need to be paired with technology-specific legislation in order to retain the substance of the right that they support (Hildebrandt & Tielemans, 2013)[54].

- *Non-compliance*. Although the GDPR theoretically requires those who develop, design, select and use privacy-invasive systems to abide by the principle of data protection by design and by default, it is unclear how compliance ought to be corroborated; a report issued last April (Ryan & Toner, 2020)[58] shows that European governments do not provide their national Data Protection Authorities (DPAs) with sufficient budgets and technical staff to enforce their power, and that for this reason, DPAs hesitate to take action against tech firms even when wrongdoing is evident.
  The problem is not limited to the blatant abuses of major companies, but it materialises in extensive and pervasive violations carried out by all kinds of digital service providers: Sanchez-Rola et al. (2019)[59], for instance, found that around 92% of the websites evaluated (2,000 high-traffic websites, hosted both inside and outside of the EU) violate legal requirements by setting at least one long-lasting identifier directly on page load, even before displaying cookie banners, and even if users choose to opt-out from tracking; moreover, the websites in which users have a clear reject option or are presented right away with a cookie settings dialog amount to less than 4% of the total[59]. In a similar vein, Nouwens et al. (2020)[60] scraped the designs of the five most popular Consent Management Platforms on the top 10,000 websites in the UK and demonstrated that only 11.8% of them meet the minimal requirements set by the GDPR. As reported, dark patterns and implied consent are ubiquitous; sadly, not only do vendors of these platforms turn a blind eye to illegal configurations, but they occasionally even incentive them[60].
  The problem of non-compliance gets particularly thorny when it comes to data produced by individuals who lack the legal capacity to give their consent: Vlajic et al. (2018)[61], for instance, recently presented overwhelming evidence of illegal, highly covert tracking in children-oriented websites, operated by third party companies and without parental consent.
  Given the absence of wide-reaching and flexible tools that can assist in ensuring that all the actors who are liable for the processing and the effectiveness of the relative measures actually comply to their obligations, the technology-agnostic approach appears yet more ill-advised.

6.2 Practical problems

For the average user, understanding the possible repercussions of typical processing practices is a quite challenging task: this is due largely to the complexity of the technical environment, which keeps increasing and manifests itself with both a technological and a legal dimension. Even if data subjects devote themselves to the supervision of their privacy preferences, however, the amount of time required to make meaningful consent choices is often ridiculously high (e.g. see Forbrukerrådet, 2020)[34]. On top of it, technological developments could carry along new privacy risks of which no one is currently aware.

- *Time required to read consent materials*. Even admitting that users were willing to read notices, the effort demanded to them was proven unrealistic in terms of both time and attention: in 2008 it was estimated that if American users were to fully read all the policies they encountered online, the task would have required approximately 40 minutes per day (which would have produced an annual loss of $781 billion in terms of national opportunity cost)(McDonald & Cranor)[62]. If one considers that nowadays data subjects might be asked for their consent from hundreds of actors all at once (as third parties may share data with their own third party partners, and so on)(Forbrukerrådet, 2020)[34], the idea of informed consent becomes almost preposterous.

In light of these matters, it is not surprising that Obar & Oeldorf-Hirsch (2018)[7] found that, when presented with a privacy policy, 74% of participants chose the quick-join clickwrap option, which allowed them to evade reading altogether. Their results also show that, whereas reading time was estimated to be 29-32 minutes for an educated adult, individuals who did read the policy spent on average 73 seconds on it. Yet, 97% of participants accepted the agreement.

- *Complex and legalistic language*. It can't be assumed that users have the appropriate level of education to understand legal agreements: as has long been recognised, the language featured in policies is often complex and legalistic, and therefore beyond the grasp of many users (Jensen & Potts, 2014[1]; Carolan, 2016[3]; Steinfeld, 2016[25]). In fact, the academic community refers to it as "legalese", and sometimes corporate policies reportedly manipulate language to obfuscate unethical data handling practices and use persuasive techniques to increase the company's trustworthiness (Pollach, 2005)[63].

- *Complex technological environment*. Especially in view of the rapid pace of technological progress, it is also wrong to assume that data subjects are familiar enough with the context and have a clear understanding of how and for what purposes their data is being processed (Schermer et al., 2014[24]; Carolan, 2016[3]; Obar & Oeldorf-Hirsch, 2018)[7]; Van Ooijen & Vrabec, 2019[29]). Empirical data collected by Park (2013)[64] suggests that users are far from competent when exercising privacy control, and that while their knowledge is critical to their privacy behaviour, the majority of users have a minuscule understanding of surveillance practices commonly implemented in websites; for this reason, policy that doesn't take into account this knowledge gap might be fundamentally flawed[64].

- *Limited foreseeability*. The fast development of new technologies undermines not only users' understanding of the environment and the relevance of many legal definitions, but makes it also basically impossible to anticipate what kind of insights could be inferred from the gathered data in the future (Carolan, 2016)[3]. This is commonly known as the Collingridge dilemma: while it is possible to influence the development of new technologies when they first emerge, their implications are often still too unpredictable to do so, and only become manifest when said technologies are already entrenched in societal dynamics and are therefore difficult to control (Collingridge, 1980)[65].

6.3 Behavioural problems

In the field of behavioural economics, it is well-known that consumers don't always follow rational decision-making processes, but are often subject to a variety of cognitive biases that affect their judgement and risk assessment (Kahneman & Tversky, 1984[27]; Kahneman et al., 1991[66]; Solove, 2012[67]). Online environments make no exception: it is argued that digital contexts foster a variety of situational influences such as heuristics and biases that intuitively impel the giving of consent, even in the case of engaged users (Carolan, 2016[3]; Kokolakis, 2017[49]), and for this reason, researchers have often suggested that online privacy policies should require minimum degrees of rational and informed decision-making or even include a default protection system such as the one embedded in fair frameworks (Jensen & Potts, 2004[1]; Acquisti et al., 2015[2]). The task of identifying a common framework of protection, however, could be hindered by the fact that privacy preferences are highly contextual (Nissenbaum, 2004)[68], and data subjects may have different concerns depending on the particular implications of each instance of data processing.
The following is an overview of the cognitive influences mentioned in the literature reviewed; due to the multi-faceted nature of the matter, a number of potential issues could have been disregarded.

- *Availability heuristic*. Individuals reportedly display a tendency to base their consent decisions on information that is easily retrievable rather than meaningful. (Solove, 2012[67]; Carolan, 2016[3]).

- *Optimism bias*. Privacy behaviour is influenced by the widespread inclination to believe that we are less likely to experience negative events compared to others (Acquisti & Grossklags, 2005[28]; Kokolakis, 2017[49]).

- *Control illusion*. It appears that, paradoxically, the provision of control itself suffices to create an illusion of safety, leading individuals to expose themselves to higher privacy risks (Acquisti et al., 2015[2]; Kokolakis, 2017[49]).

- *Confirmation bias*. Data subjects tend to look for information that confirms their original intuition, even if they have no special interest in the resulting insights being true (Carolan, 2016[3]; Kokolakis, 2017[49]; Gerber et al., 2018[50]).

- *Status quo bias*. According to plenty of studies, privacy behaviour is also influenced by the fact that frequently repeated actions tend to be framed as default; this bias is extremely relevant with respect to the affirmative act required by the GDPR, and helps explain how ticking the consent checkbox is not necessarily a demonstration of autonomous behaviour (Kahneman & Tversky, 1984[27]; Acquisti & Grossklags, 2005[28]; Carolan, 2016[3]; Steinfeld, 2016[25]; Van Ooijen & Vrabec, 2019[29]).
- *Hyperbolic discounting bias*. This phenomenon pushes subjects to evaluate events in a time-inconsistent manner: when assessing privacy risks, users reportedly evaluate long-term benefits less than short-term ones, hence disregarding long-term privacy costs (Acquisti & Grossklags, 2004[69]; Carolan, 2016[3]; Kokolakis, 2017[49]).

- *Lack of personal experience and risk awareness*. When users are asked for their consent, their evaluation of costs and benefits is also compromised by lack of personal experience; few data subjects have in fact actually experienced privacy violations (at least as far as they are aware), and risk assessment is hence usually based on heuristics and second-hand knowledge. However, it is argued that only through first-hand experiences one can form an attitude that is stable enough to significantly influence behaviour (Dienlin & Trepte, 2015[70]; Gerber et al., 2018[50]).

- *Misplaced trust*. Although, as pointed out by Steinfeld (2016)[25], user engagement with a website can lead to increased trust and better informed decisions, Schermer et al. (2014)[24] highlight that trust could be misplaced, and therefore if consent is used to legitimate instances of processing considered wrongful, users might feel like they have been misled. Since consent is a morally transformative act that affects normative expectations, this can cause consent desensitisation, whereby data subjects simply give consent when it is asked, rather than make an actual choice. For this reason, even controllers who carry out fully compliant activities can't trust that consent is meaningful [24].

7. Societal relevance

Research shows that while data protection laws in the EU are generally well-grounded on virtuous principles, they don't always produce the desired effect, especially when they apply to digital contexts. In light of the issues exposed, it's easy to see why the scientific community has repeatedly questioned the use of consent as a reliable proxy for user privacy preferences, maintaining that the aforementioned problems make the consent-oriented approach to data protection fundamentally flawed (Carolan, 2016)[3] and that "it is unreasonable to assume that anyone goes to the lengths required by current practice" (Jensen & Potts, 2004)[1]. Notwithstanding that consent is the expression of fundamental rights and values, there is ample evidence that enormous amounts of data are regularly processed on the basis of uninformed and unfreely given choices (Obar & Oeldorf-Hirsch, 2018[7]; Pardo & Métayer, 2019[30]; Utz et al., 2019[31]). The sole fact that we can't be sure whether data subjects have actually read policies suffices to call into question the relevance of privacy agreements that rely on consent as a legitimisation of the processing; however, even engaged users face a variety of practical obstacles and are subject to so many cognitive influences that it seems optimistic to suppose that their consent can indisputably be deemed meaningful.
These matters are particularly relevant if one considers that while, on one hand, institutions seem to make little use of such observations, on the other, service providers keep exploiting user data to devise ever more sophisticated nudging techniques (e.g. in 2009, Google's product manager remarkably had 41 shades of blue tested to investigate user clicking behaviour) (Carolan, 2016[3]; Plona, 2015[71]). In fact, as shown in a report called "Deceived by design" recently issued by the Norwegian Consumer Council (Forbrukerrådet, 2018)[72], even tech giants like Google, Facebook and Microsoft take advantage of cognitive biases when crafting

default settings, techniques and features of interface design, thereby pushing users to make privacy-intrusive choices. The fact that companies can exploit information asymmetries and increase profits by resorting to the use of such dark patterns, tricking data subjects into doing things that they might not want to do, reveals a clear misbalance in the relationship between data controllers and data subjects that poses huge threats to the inviolable right to privacy.
As mentioned by the European Digital Rights association (EDRi) in an open letter to EU Member States, "[…] without a strong Regulation, surveillance-driven business models will be able to cement their dominant positions and continue posing serious risks to our democratic processes"(European Digital Rights, 2019)[73].
Public outrage following the Cambridge Analytica scandal in early 2018 spoke volumes in relation to the widespread and growing concerns around the potential uses of personal data (Cadwalladr & Graham-Harrison, 2018)[74]. Unfortunately, phenomena of this kind keep occurring and no one seems to be held accountable (e.g., see Intelligence and Security Committee of Parliament, 2020)[75]. Cadwalladr (2020)[76] argues that we are going through an unstoppable digital contagion that has poisoned our information space, infected our public discourse and silently subverted our electoral processes. In her opinion, there is no doubt that new operations will be carried out to influence our political choices, and that the real question is whether our democratic systems are fit to survive.
In addition to this, there is evidence that data can be used in unprecedented ways, sometimes even by governmental agencies (Greenwald, 2014)[77]; data breaches are nowadays a relatively common phenomenon, and they are often carried out without users or authorities even knowing, with risks such as identity theft, financial/material damage, loss of confidentiality in professional contexts and damage to reputation (Tao et al., 2019)[78].

8. Considerations and future directions

As previously noted, consent materials usually put too much of a burden on users due to the amount and complexity of information contained, as well as to their architecture and framing.
The domain of human-computer interaction abounds with studies that could assist EU policy entrepreneurs in developing more accurate guidelines for accessibility and usability of policies. A variety of tools, metrics and workbenches can be used to assess user-friendliness, improve standardisation, derive semantic models and simplify both language and interfaces (Breaux & Anton, 2005[79]; Brodie et al., 2006[80]; Belli et al., 2017[81]; Drozd & Kirrane, 2019[82]). For instance, the Flesch Reading Ease Score (FRES) is a popular metric often used to evaluate the complexity of legal documents (Jensen & Potts, 2004)[1]. However, it is worth stressing that this kind of interventions might soon become irrelevant as a result of new technological developments.
In order to make processing more transparent and give users actual control over the data shared, data subjects should have a clear overview of who is processing their data, what type of information they have access to and for what purposes it's being processed. To attain this, they should be able to dispose of an accessible record of the various consent transactions and eventual third party processing carried out; clearly, this can only be achieved through the earlier identification of benchmarks and best practices, by which controllers could then be expected to abide. In pursuing this, when drafting new guidelines, the EDPB and the other competent authorities could start referring to the FAIR guiding principles (Wilkinson et al., 2016)[83]: this framework was originally developed to assist data stewards towards good management of scholarly scientific data and states that data should be Findable, Accessible, Interoperable and Reusable, both for people and for machines. Considering the different field of application and the sensitive nature of personal data, not all of these principles might apply in the same way. For example, from a data subject's perspective, findability and accessibility implementations would probably be more beneficial than ones aimed to improve interoperability and reusability; nonetheless, each pillar of this framework is envisaged to be independent and separable[83]. Furthermore, the European Union already supports the FAIR framework and is resorting to it in an effort to establish the Internet of Fair Data and Services (Van Reisen et al., 2019)[84]: the emergence of solid and sustainable infrastructures would make data management processes easier not only for data subjects, but also for controllers.
That being said, even though the implementation of similar solutions would probably be greatly beneficial to engaged and competent data subjects, it would not guarantee that all of them are knowledgeable and skilled enough to make use of them and to understand the implications of their choices.

Especially in cases where personal data and rights may be particularly at risk, institutions might want to consider libertarian paternalism and the application of nudging mechanisms, whereby the interface of the consent request could be strategically designed to encourage privacy-protective behaviour. Nudges can be a powerful tool, but they need to be crafted mindfully, as they could easily lose effectiveness or even backfire (Bicchieri & Dimant, 2019)[85]. On the flip side, nudging could well become a tool for actual manipulation, especially in cases in which choice preference is uncertain, and as long as individual autonomy is the main focus of policy, this doesn't seem like an optimal approach (Wilkinson , 2013)[86].

9. Conclusion

The present study analysed the evolution of the notion of consent to data processing within the European data protection framework. Past, present and future legislation was put in perspective with existing academic literature and with John Kingdon's Multiple Stream Framework[9] to pinpoint the main models of consent (presumed, informed, active and selective), which were then examined in light of existing scientific research. What emerges from this inquiry is that, despite each of these notions aimed to give users the means to make autonomous consent choices, they all overlooked different ranges of empirical obstacles to meaningful decision-making, such as the time required for consent to be actually informed or the exploitation of information asymmetries operated by some controllers to the detriment of data subjects (McDonald, 2008[62]; Forbrukerrådet, 2018[72]). Problems arising have different character and were thus clustered in three main categories (legal, practical and behavioural) with independent relevance; the manifoldness of the matter supports the idea that the consent strategy adopted by EU policymakers is flawed and that high-order changes need to be introduced in the policy stream.

In view of what discussed, there seems to be a need for policy to better address a multitude of problems that undermine the significance of the very principles on which consent is grounded: given that autonomy and informational self-determination are such prominent concepts in the European data protection framework, it is essential that institutions commit themselves to revising the current strategy and to setting more empirically-sensitive requirements for consent that take into account not only the choice made by data subjects, but the conditions under which it was made as well. On the basis of the issues addressed in this review, it can be affirmed that compliance shouldn't be given for granted, and that if controllers are allowed to choose with a fair degree of arbitrariness the measures that they consider appropriate for the processing of personal data, at the very least there should be more efficient and flexible tools to verify that the methods applied by them are actually fit to safeguard the fundamental rights of users. The technology-neutral approach is not necessarily inappropriate, but as described, it doesn't seem conducive to ensuring a satisfactory level of protection unless compliance can be thoroughly monitored and unless legal provisions can be said to be unequivocal.

Besides, policymakers should be wary of behavioural models based on a view of the data subject as a rational agent, for it is well-known that this is not the case; it is necessary that, when drafting new provisions, institutions better take into account the fact that digital environments foster a number of situational influences that affect the choices made by users and evaluate the introduction of additional restrictions to the use of consent as a legitimating ground of the processing.

The EU data protection framework aims to give data subjects autonomy, but it is debatable whether they are actually able to exercise it: in fact, users are often nor competent nor rational when it comes to the management of their own privacy preferences. It should be noted, however, that requirements set by the current strategy have questionable effectiveness even for skilled and engaged data subjects: the results of the aforementioned report of the Norwegian Consumer Council (Forbrukerrådet, 2020)[34] are exemplary of how intricate and tedious the task of supervising the processing of one's personal data can be on a practical level.

On a side note, typical policy procedures seem too lengthy and time-consuming if we consider the ever growing number of risks posed by the emergence of novel technologies; the data protection framework cannot be but more dynamic in order to face new challenges more effectively.

Ultimately, in light of what discussed, it can be said that, despite the efforts made by policymakers, none of the notions of consent put forward over time actually granted data subjects a concrete level of protection of their fundamental rights, primarily because each of them implied an overestimation of the cognitive resources of the average user, but also because

liable entities were never given unequivocal compliance guidelines; on top of that, privacy violations go often unpunished. Although the GDPR undoubtedly empowered many engaged and competent data subjects, it appears as if it exacerbated some problems, leading to widespread desensitisation towards the significance of consent; the tenet of data protection by design and by default remains for now a flight of fancy.

Part 2

Scenarios for meaningful consent: Aligning theory and practice

Abstract: *In the previous chapter, we discussed the ethical grounding of consent to data processing and the chronological evolution of its legal enactment, identifying different notions and pinpointing problems attributed to each of them; on the basis of empirical evidence exposed by researchers, we concluded that none of the consent models adopted over time in EU laws were fit to effectively protect the privacy of data subjects. Although the right to data protection gained increasing importance and recognition, in fact, there is still a substantial gap between legal theory and its actual application: we argue that any notion of consent to data processing will be crippled insofar as it will overlook the concrete obstacles to the autonomy of data subjects. In the present chapter, the significance of the detachment of consent practice from its theoretical framework is explored, and scenario planning is used to investigate the question as to how users could be made autonomous in practice, as well as to what would happen if consent was regarded as a heteronomous decision instead. The implications of the emerging scenarios are then discussed and used as grounds for a more general reflection on the problems of data protection.*

1. Introduction

The EU data protection framework is grounded on the view of consent as the materialisation of an autonomous choice made by the data subject, yet as we have seen, a multitude of empirical insights challenge this assumption. Even if we were to believe that users would be willing to devote considerable amounts of their time to reading consent materials, in fact, it is unwise to expect them to understand what is entailed in practice by the choice to give consent, especially given that the increasing complexity of the environment is also at the root of the ambiguity of legal provisions.

According to the GDPR, the consent of the data subject is not the only legitimating ground for the processing of personal data, but as long as data controllers can demonstrate their compliance and the effectiveness of the measures taken, it can be deemed a satisfactory lawful basis (Art. 6(1a), Rec. 42, 74)[6].

This is problematic in two different respects. First, because the rectitude of the controllers' proceedings is to be evaluated against the observance of rules that disregard the congenital incompetence and limited rationality of users (i.e. the law presumes that data subjects are able to understand how their data is processed and evaluate costs and benefits accordingly), and as a result, in full compliance with the current framework, not only can deceitful controllers exploit information asymmetries and cognitive vulnerabilities, but also honest ones are at risk of committing privacy violations.

From this stems a second fundamental issue, namely that plenty of unlawful consent requests remain off the radar. In the progression of EU data protection laws, in order to encourage honest compliance, increasingly stronger obligations were placed on data controllers with respect to their responsibility and liability. In certain circumstances (e.g. for large-scale monitoring of personal data), data controllers and processors shall appoint a Data Protection Officer (DPO), who, among others, has the duty of providing expert advice on impact assessments of instances of processing that pose high risks to the rights and freedoms of natural persons (Art 35, 37, 39)[6]. Besides, in each Member State, an independent supervisory authority is entrusted with the task of overseeing and enforcing the consistent application of the regulation and is responsible for eventual administrative or judicial remedy in the event of complaints lodged by data subjects (Art. 51, 57, 77)[6]. However, if the party who is directly affected can't spot infringements, how can compliance be ensured for such a great quantity of controllers? […]

If the measures adopted to protect the autonomy of data subjects work only in theory, the ethical grounding underlying the validity of consent loses its relevance, and consent becomes, in practice, a free-standing justificatory standard.

Kosta (2013)[12] argues that although the pivotal role of consent in a rights-based approach to data protection is indisputable, consent per se does not ensure the protection of the privacy of the individual; in particular, believing that the average user is able to understand the implications resulting from the use of cookies is a utopia, and for this reason, the sole reliance

on consent as a legitimisation proxy for privacy-invasive actions could be indicative of a *fixation* with consent. This term was introduced in 2004 by Brownsword in a paper titled "The cult of consent: fixation and fallacy", in which he addressed the issues arising from the detachment of consent from its ethical and legal framework[87].
In the next section, the concept of consent fixation is elaborated, and in section 3 the risks associated with it are explored in relation to current data protection laws. Section 4 discusses the implications related to an unrealistic behavioural model of users and suggests alternatives. In section 5, the problem is summarised and the research questions are developed. Section 6 describes the research design and motivates the choice of the methodological tools used to investigate the questions, highlighting the need for fresh thinking and the benefits of a vision-oriented approach rather than a goal-oriented one. In section 7, the introduction of extreme changes in the current data protection framework is evaluated using scenario planning, and the hypothetical consequences of the two emerging scenarios are presented. Section 8 grounds scenarios in reality by discussing their strengths and weaknesses in relation to scientific research and presents the resulting considerations. Section 9 elaborates on study limitations and possible future directions. Conclusions are summed up in section 10.

2. The dangers of consent as a free-standing ethic

Brownsword (2004)[87] maintains that, despite the broad cultural bandwidth, the views of theorists on consent are typically bilateral, and oscillate between a utilitarian view and a rights-based one (a third position, the dignitarian alliance, is specific to the field of bioethics). Utilitarians don't attribute any particular importance to individual autonomy, but rather focus on the advantages and disadvantages of consent collection, with an emphasis on practicability and costs. In their view, there is no golden rule for the aptness of consent, and the evaluation always depends on context, convenience, contingency and circumstance; on the other hand, human rights proponents assert the significance of the autonomy of citizens and highlight the role of consent as a signal for the creation of a new relationship or for a change of position, whereby the choice to give consent represents a conscious and thought-out justification for potentially harmful activities.
If the current notion of consent were to be examined against this background, due largely to the fundamental nature of the right to data protection and the relative significance of individual autonomy and self-determination, it could be said that the European stance is primarily rights-based; however, as shown in the previous chapter, the present approach is little empirically-sensitive, for it erroneously presumes that when they give their consent, data subjects are making a decision based on personal reflection rather than on external influence. Indeed, as maintained by Carolan (2016)[3], consent has obvious limitations as a means to support individual autonomy, since it focuses on the choice but much less on the conditions under which said choice was made. The assumption that data subjects are rational agents who have a good understanding of the context has kept undermining the relevance of data protection laws since the emergence of the earlier models of consent, and the belief that consent to data processing is the expression of an autonomous choice appears ever more like a fictional concept. But what is the point of enshrining the right to data protection in a fundamental rights framework if the very principles that should be given utmost importance (i.e. informational self-determination and autonomy) are then disregarded in common practice?
As argued by Brownsword, there are two threats to the integrity of a culture of consent, if the latter is treated as a free-standing justificatory standard: the threat of under-valuation and that of over-valuation. When under-valuation occurs, consent is collected casually and is typically presumed or implied; such consent is reduced to a bureaucratic process and used as a "lazy justification", while often turning out to be a fiction of law. On the contrary, consent is over-valued when it is seen as the key to ethical and legal justification and a community becomes fixated with it: Brownsword referred to this as "consent-fetishism" and claimed that if we want to prevent a healthy culture of consent from transforming into an unhealthy cult, it is crucial that we are mindful of the symptoms of fixation. Where the respect for human rights and agency is not taken as axiomatic and consent is no longer treated as rooted in a larger theory of ethical or legal justification but becomes a free-standing ethic, in fact, the integrity of the culture is undermined by different possible fallacies. If the community believes that where there is no consent, there *must be* a wrong, a Fallacy of Necessity takes place; in contrast, a Fallacy of Sufficiency is committed when it is assumed that where there is consent, there *can be no* wrong[87].

The analogies between the effects of the aforementioned threats and the issues reportedly associated with the European notions of consent are not too hard to spot. The next section focuses on the identification of these warning signs.

3. Fixation and fiction in EU data protection

If we analyse the evolution of consent to data processing in the European framework from Brownsword's perspective, it can be argued that the earliest threat jeopardising the significance of consent was that of under-valuation: by contemplating user acquiescence as an indicator of valid consent, in fact, Directive 95/46/EC[16] legitimated the default acceptance of policies, where consent was merely presumed and therefore practically reduced to a procedural justification. The autonomy of the choice of the data subject is, in this case, a secondary concern, sidelined by the fact that there actually was no real choice, but only the chance to withdraw from an agreement that was considered as accepted a priori.
When the focus started to shift on the importance of consent as an informed decision made by the data subject, the threat of over-valuation began to creep up on later consent notions: as illustrated in the previous chapter, the intrinsic complexity of the language featured in privacy policies and the increasing sophistication of the environment made it ever so hard, even for engaged users, to understand the implications of their consent choices. The presumption ingrained in data protection laws ever since the ePrivacy Directive was adopted that the average user can develop the appropriate level of knowledge for consent to be truly informed was, since then, challenged by the work of plenty of researchers (Van Eijk et al., 2012[88]; Jensen & Potts, 2014[1]; Schermer et al., 2014[24]; Carolan, 2016[3]; Steinfeld, 2016[25]; Obar & Oeldorf-Hirsch, 2018)[7]; Van Ooijen & Vrabec, 2019[29]).
Knowing that the over-valuation of consent can lead to the aforementioned fallacies, it doesn't seem like a coincidence that the REFIT evaluation ran in 2016 by the Commission[35] found the consent rule carried along by the ePrivacy Directive to be both under-inclusive and over-inclusive; by limiting non-intrusive practices, current legal provisions appear to be committing the Fallacy of Necessity, whereby it is believed that if there is no consent, there must be a wrong; on the contrary, if laws don't protect data subjects from certain privacy-invasive instances of processing such as device fingerprinting and overlook the exploitation of information asymmetries and dark patterns, the integrity of the present notion is undermined by the Fallacy of Sufficiency as well, for it is assumed that where there is consent, there is no wrong.
Furthermore, although the focus put by the GDPR on individual control is virtuous from a rights-based perspective, the idea that activity successfully counteracts inertia is misguided, as maintained and demonstrated in a variety of studies (Acquisti & Grossklags, 2005[28]; Carolan, 2016[3]; Steinfeld, 2016[25]; Van Ooijen & Vrabec, 2019[29]): due to cognitive limitations (notably the status quo bias), in fact, the act of ticking a checkbox in online environments is often far from being the expression of an autonomous choice, and it would be a disservice to European consumers to believe otherwise.
According to the drafted provisions of the new ePrivacy Regulation, the model of selective consent that is supposed to replace that of informed consent brought forward by the ePrivacy Directive is likely going to alleviate some issues, first and foremost the problem of consent fatigue (provided that controllers will voluntarily choose to centralise consent requests and stop resorting to the old notice and consent paradigm); however, this would call for increased participation from data subjects, which, in light of what discussed earlier, seems like an optimistic expectation. Besides, the absence of specific and technical interface design guidelines might still lead to settings that are too complex for the average user and too burdensome also for expert ones. Moreover, in case privacy-invasive defaults are not ruled out, centralised consent could even be a backward step, as processing would take place without data subjects knowing. On top of that, it should be noted that by choosing browsers as consent request mediators, it is implied that these would honour fully the principle of data protection by design and by default; knowing that Google, the company who owns the web browser with the biggest market share [89], was among the tech giants who were accused by the Norwegian Consumer Council of deceiving users by design through the use of dark patterns and information asymmetries[72], this presumption also seems far-fetched.
In addition, it appears as if once again, new provisions will disregard one of the biggest obstacles to the autonomy of users' choices, namely that of incompetence: despite the explicit reference to the fact that "end-users face requests to accept tracking cookies without

understanding their meaning"(European Commission, 2017)[8], not only will the new regulation keep relying on the erroneous assumption that data subjects are able to understand how their personal information is processed, but it will also assume that they are capable of discerning among the implications of the acceptance of different types of tracking devices.
On the basis of these considerations and of what discussed in the previous chapter, we argue that, despite its theoretical grounding, consent to data processing is not, in its material form, the functional expression of informational self-determination and autonomy, but has rather kept serving as a procedural justification for the benefit of both data controllers, whose business models rely on the processing of personal data, and data subjects, who fancy customised services.
Having said that, a problem arises when we acknowledge the evident expertise gap between these two counterparts and the fact that compared to users, controllers presumably operate more rationally to maximise their profits and avoid the immediate penalties. At the same time, while the worst scenario for controllers may be that to incur in administrative fines, the stakes are much higher for data subjects, as apart from individual fundamental rights, the collective good is also compromised by the processing of personal information. Rodotà (2007)[45], a member of the Convention that drafted the Charter (Deloche-Gaudez, 2001)[90], maintained that a strong protection of personal data remains a "necessary utopia" (quoting S. Simitis) if we want to safeguard the democratic nature of our political systems, and argued that reality is being increasingly alienated from the fundamental rights framework because some of the tenets underlying the data protection system are being "continuously eroded or downright overridden by alleging the prevailing interests of security and market logic"[45].
In "*The social power of algorithms*", Beer (2017)[91] warns us against the threats of fixation by describing Big Data as a soft, yet pervasive and potent form of control: as stated by him, the data-determined filter bubbles in which we retreat prevent us from being exposed to experiences that are vital to our individual flourishing and democratic engagement, and consequently, before giving up to the allures of Big Data, we must be aware of their regulatory power and find practically effective measures that better protect us from hypernudging (i.e., Big Data analytic nudging).
If we persevere in putting the spotlight on individual autonomy (therefore keeping a rights-based approach) and assign data subjects the full supervision of their privacy preferences, it goes without saying that we must find a way to regulate the environment in such a manner as to enable them to take actually autonomous choices; but to what extent does it make sense to make users autonomous, when we consider that their own incompetence and faulty rationality prevent them from being good overseers of their reported interests? In other terms, can users be protected from their own cognitive limitations?

4. Homo not very economicus

In the context of behavioural economics, there is a term that specifically denotes the assumption that consumers act rationally and in their best interests, namely that of *Homo economicus*. The model of the "economic human" draws from neoclassical economic theory and presupposes the belief that consumers, knowing what they want and how to get it, act in their own self-interest through rational and time-consistent thought processes (i.e. as rational agents); needless to say, the practical implications of this supposition were often challenged not only by theoretical analyses, but experimental evidence as well (Gintis, 2000[92]; Henrich et al., 2001[93]; Reisch & Zhao, 2017[94]). Many recent studies lay their theoretical foundations on the work carried out by Herbert Simon, one of the first researchers to proclaim the importance of devising actually empirically-sensitive models of human behaviour that derive from systematic analyses of behavioural phenomena; such models view decision-making as affected by *bounded rationality,* that is to say by limitations of knowledge and computational capacity (Simon, 1955[95]; Simon, 1990[96]).
Hoofnagle & Urban (2014)[97] tested the empirical relevance of the Homo Economicus model in the specific context of the notice and consent regime, and reveal that many users base the negotiation of their privacy on fundamental misunderstandings about business practices, privacy protections and restrictions upon the processing of data; as reported, this confusion may also lead data subjects to expect to be granted more protection than they actually are. For these reasons, they recommend that better policy is developed on the basis of more accurate depictions of users' knowledge and preferences: for example, there should be incentives to close

the knowledge gap between consumers and companies, and the expectations of users as regards the protection of their personal information should be better aligned with reality[97].
In light of these matters, it can be argued that for an approach based on personal autonomy to work in practice, it is essential that policy takes into account the cognitive deficiencies of data subjects. Once ascertained that these exist and admitting that models can be developed to predict the irrational habits of users, however, the question arises as to what extent can the legal environment be modified to make up for their cognitive weaknesses and still produce autonomous choices. It seems safe to assume that, as long as the expertise gap between data subjects and controllers won't be truly closed and users will lack the cognitive resources to actually *understand* the implications of their choices, consent will, at least to some extent, keep depending on external influence, hence compromising any notion relying on a view of consent as a completely autonomous act.
Ultimately, if users can't be fully autonomous, should the ethical framework transition from the rights-based approach to a utilitarian one, where individual autonomy and self-determination are overshadowed in favour of the public good? And considering the absence of clear and objective measures of welfare, what purpose should said consent serve?
In the next section, the problem will be summarised and the focal question articulated.

5. Research question

The question of how to make autonomous consent work in practice is particularly thorny: as we have seen, not only are the issues attributed to the various notions of consent over time many and complex, but they're also different in nature, and accordingly, even if a whole cluster of problems is removed from the equation, the others would likely still pose significant challenges to the meaningfulness of the consent choices made by data subjects. For example, on the off chance that novel interaction frameworks are devised so as to take into account and minimise all behavioural issues by means of accurate, empirically-grounded behavioural models, that wouldn't ensure that users set their privacy preferences on the basis of personal reflection, as many of them would remain insufficiently educated or digitally literate; at the same time, the consent of competent data subjects could still be impaired by limited time or by illegal and coercive request techniques. In such a scenario, having behaviourally-sensitive models of incompetent individuals may even pose new risks to their autonomy, as greater information asymmetries could be exploited to influence their natural decision-making processes in ways that don't reflect their real interests.
Byung-Chul Han (2017)[98] maintains that neoliberalism has turned citizens into consumers, and that "the freedom of the citizen yields to the passivity of the consumer". Despite recognising the power of Big Data as a highly efficient tool that allows for comprehensive knowledge of the dynamics of social communication, in Han's opinion, said knowledge is a threat to free will and leads to domination and control, as it enables intervention and psychological influence to take place on a pre-reflexive level, or in other words, escaping full awareness. Though some consider Han's views pessimistic, the possibility that Big Data are exploited for political purposes can't be ruled out, especially in light of scandals such as that of Cambridge Analytica.
Having acknowledged the shortcomings of an approach to data protection that relies so extensively on the autonomy of data subjects and on the liability of controllers, one has to wonder if a rights-based position can ever grant an effective protection of personal data, or if it actually is a pipe dream; closing the knowledge gap between data subjects and controllers, for one, appears to be a conditio sine qua non of a more balanced environment, but that would entail substantial societal developments that don't seem achievable in the immediate future, even more so given that technology keeps becoming more sophisticate.
The next part of the present research is going to investigate the question as to how the problems of consent could be overcome: can resources be found to enhance the cognitive resources of users and make up for their incompetence and faulty rationality, or should we aim to make data protection laws practically effective by shifting their focus away from individual autonomy, prioritising instead the welfare of the whole community? To put it simply, should we attempt to modify practice in order for it to reflect theory or vice versa?
The following section will illustrate and motivate the design-related decisions and methodological framework chosen to explore these questions.

6. Research design and methodology

Studies carried out on the problems of consent usually tend to focus on the identification of specific issues and attempt to come up with immediate solutions to counteract them; however, this approach appears limited if one considers the fast pace of technological development and the different nature of the problems involved. Inquiries based on methodological tools such as planning and policy analysis typically feature a goal-oriented stance that implies a predictive character, where the future is viewed as bounded by specific, preferred ends to achieve; while this kind of strategy is undoubtedly useful when the aim is that of stimulating incremental policy change, this approach is not ideal in times of rapid transformations and when the focus lies on the introduction of new, fundamentally different conditions (Inayatullah, 2013)[99]. Moreover, these methods are often based on rational-economic models of decision-making, which, as we have seen, do not take into account the behavioural inconsistencies displayed by consumers. Finally, while a number of practical solutions were already proposed by researchers as means to make up for some of the most evident issues (e.g. language and interface complexity)(Breaux & Anton, 2005[79]; Brodie et al., 2006[80]; Drozd & Kirrane, 2019[82]), none of these implementations seem to have been included in the policy agenda.

For all of these reasons, the present study will adopt a vision-oriented approach rather than a goal-oriented one, aiming not so much to find ways to make laws immediately more effective as to support future policy decisions by challenging present structures and evaluating the possible effects of dramatic changes. The intention is not that of finding solutions to the problems of consent, but rather that of evaluating possible alternatives by stretching the realm of possibilities. These alternatives are plausible, but not necessarily probable, and are useful to evaluate critically the strength and weaknesses of different approaches, as well as to spark dialogue among readers and to encourage fresh thinking.

One of the main techniques used by scholars to envision alternative realities is scenario-planning, which is a methodology that typically pertains to the discipline of futures studies. Scenarios are neither forecasts nor visions of desired futures, but rather descriptions of plausible futures, through which one attempts to answer the question of "What could conceivably happen (if…)?"(Lindgren & Bandhold, 2003)[100]. Rather than focusing on the future, we chose to apply this methodology to envision alternative present realities. To run this investigation, a double-variable model is used, which is one of the dominating frameworks in scenario design and is considered particularly suitable to the development of new strategies[99] [100], whereby two main driving uncertainties are selected and positioned as axes of a cross. Each of these two main forces is a blend of different driving factors that are relevant to the focal question, and is expressed on the relative orthogonal axis as a continuum of possibilities; the four corners of the cross represent the main opposing outcomes of the combination of the uncertainties. Some researchers divide the uncertainties in *predetermined* and *critical*, the former being forces that are expected to shape the world with fair certainty and are outside of our control, and the latter being the key elements of our focal issue, which are highly uncertain in terms of future resolution (Wilkinson, 1995[101]; Rockefeller Foundation, 2010[102]; Ramirez & Wilkinson, 2016[103]).

If we apply this framework to our research questions, the main forces acting on consent are 1) those contingent on users and their poor cognitive abilities (e.g. biases, low computational capacity, illiteracy) and 2) those depending on policy and the way in which the environment is regulated (including drivers that influence the practices operated by data controllers).

As many of the uncertainties related to the cognitive resources of users stem from intrinsic characteristics of human nature, these can only be taken into account by policy, but not controlled; such forces will therefore be considered predetermined. On the other hand, users could indeed be relieved of their burdens through policy decisions, albeit with debatable implications: even if that would imply substantial and high-order changes in the ethical framework of data protection, consent could in fact become a heteronomous act as opposed to an autonomous one, meaning that the choice of data subjects could be supervised and influenced by authorised external actors. The drivers of the second bundle can hence be said critical (Fig. 2).

Axis of uncertainty n°1 shifts from *cognitive weakness* to *cognitive power*, and axis n°2 moves from *autonomous consent* to *heteronomous consent*. The resulting matrix is illustrated in Figure 2.

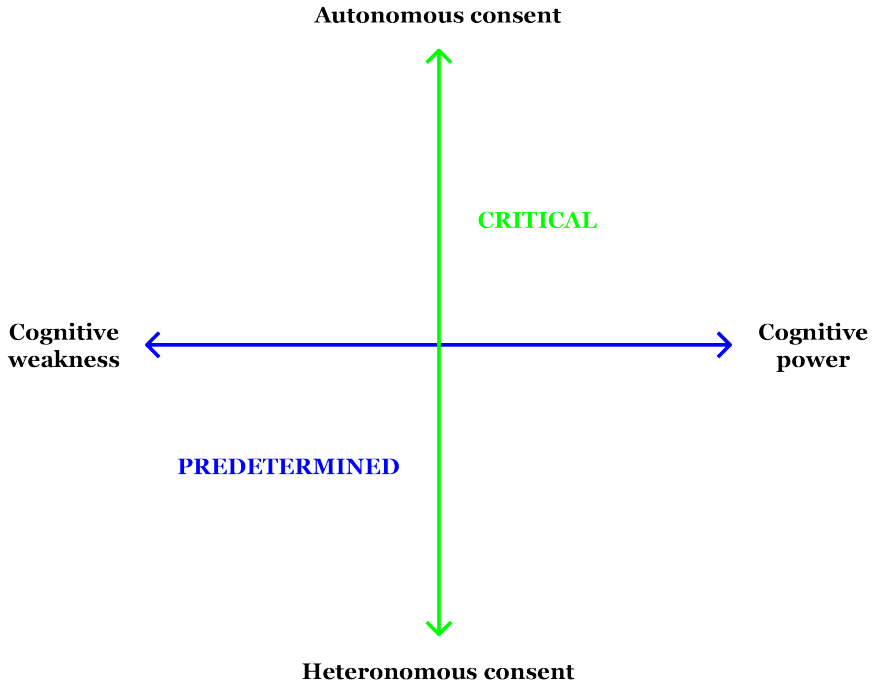

Figure 2.

In line with this setting, the current EU approach to data protection can be pinpointed somewhere in the top-left quadrant; for said area represents the current state of things, its evaluation is irrelevant to this inquiry. At the same time, admitting that a way to counteract the cognitive limitations of data subjects is found, existing policy could be said to be aligned to reality and therefore presumably effective in practice, for which reason there wouldn't be a need to amend it; consequently, the combination of cognitive power with heteronomous consent is also beside the point of this investigation, and the bottom-right quadrant can be excluded from the analysis.
On the above grounds, the following scrutiny will focus on the two remaining quadrants: the top-right scenario, which we will refer to as *El Dorado*, will discuss the possibility that a way is found to enhance users' cognitive resources so as to make them actually autonomous agents and the resulting implications, and the bottom-left one, which will be named the *Digital Tyranny*, will illustrate the hypothetical situation in which data subjects remain incompetent and irrational and conditions for consent are set to rely on heteronomous rather than autonomous decisions (Fig. 3).
The resulting insights and the main arising challenges will then be highlighted and discussed.

7. Scenarios for meaningful consent

Once ascertained that the EU data protection approach was consistently crippled by the conflict of theory and practice, we will now contemplate two alternative scenarios in which the legal framework surrounding consent could be said to be more practically effective, regardless of the side effects: we envision on one hand El Dorado, a world in which data subjects are given financial rewards as incentives to conquer their vulnerabilities and engage in the active supervision of the processing of their personal data, and on the other the Digital Tyranny, a reality in which public authorities bridge the imbalance between data subjects and data controllers by interceding in determining whether individuals should consent or not to the processing of the information they produce.

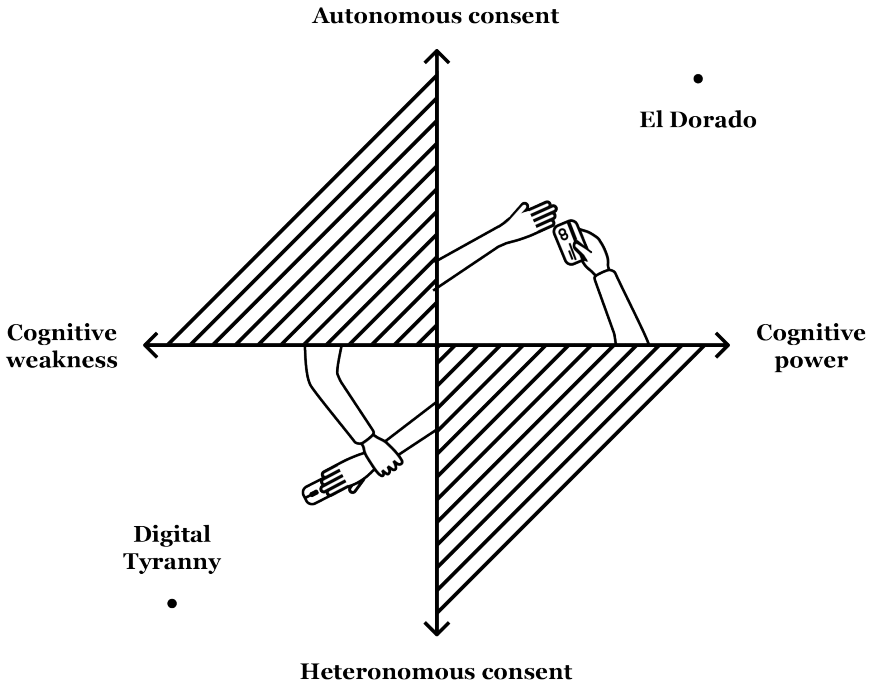

Figure 3.

7.1 From theory to practice

If the aim is that of giving users cognitive power so as to enable them to give or withdraw their consent autonomously, different types of interventions should be carried out. In the previous chapter, a variety of obstacles to meaningful consent were identified, with either legal, practical or behavioural nature. Although many of these problems are out of institutional control, part of them could be solved or, at least, alleviated: for instance, technology-specific instruments could be implemented relatively easily, and though there is no way to transform data subjects into rational entities, there might be means to incentivise their engagement.
Admitting that simplifying the context past a certain limit is impracticable due to the intrinsic characteristics of both the technical and legal setting, we must then find tools to enhance the cognitive resources of users regardless of how sophisticated the environment might be. Suggestions on how to best tackle these issues might include the standardisation of policies and legal language or the use of privacy-protective defaults, but the challenge here is far greater: not only do data subjects need to understand the implications of their choices, but they must also *want* to understand them enough to transform their attitudes into actual behaviours. So how do we sensitise people to the true meaning of their consent?

7.1.1 El Dorado

Let us suppose that Member States allocate more funds to DPAs with the specific aim of reinforcing the data protection framework. These newly-acquired resources are then devoted to hiring specialist tech staff, taking legal action against infringements, developing new IT tools and offering free online courses on data protection to all EU citizens. An official Software Development Kit (SDK) is released, and controllers are required to make exclusive use of authorised packages; user-friendliness is improved by creating standardised consent request forms and language models on the basis of scientific insights. Investigative power is boosted by taking advantage of machine operators to crawl the Web and popular mobile app marketplaces to identify those who don't comply.
Consent forms are then equipped with additional features. A rating system is introduced, and each user can evaluate the transparency and fairness of the processing on an ordinary scale; the overall grade becomes then prominently visible. This is achieved by implementing the functionalities of a service such as ToS;DR (Terms of Service; Didn't Read), an open-source browser add-on maintained by volunteering participants who rate and label TOS and privacy

policies based on how abstruse and privacy-invasive their terms are (Azmayesh et al., 2012) [104]. A "report" button is also included in the new models, so that everyone can request verification of notices that contain illegal or shady terms directly from the relative domain, and eventually lodge a complaint. Each DPA's public relations office is now reachable online and is tasked with the supervision of reports submitted by users, as well as with the provision of real-time feedback to those in doubt. In an attempt to counteract the status quo bias, the "agree" button is assigned a dynamic position that changes randomly on page load.
Moreover, as users value short-term benefits over long-term costs, the reading of policies is encouraged through immediate financial incentives. A timer is included in the new standardised consent forms, and based on the time spent by users on the reading of agreements, they will receive a monetary reward - the higher the time, the higher the profit, up until the estimated ideal reading time is reached. To demonstrate that they have actually read notices, in order to obtain their reward, data subjects will be asked one question, generated by the software, regarding the consent material they just read. Provided their answers are correct, their digital credit, stored on a dedicated platform, is immediately updated; these resources can then be spent on whatever goods are offered by the numerous partnering websites.
A lottery is organised, and each year, some of the users with greater rating contributions and longest reading times are randomly selected and obtain massive cash prizes.
Under this framework, it is necessary to track some of the information produced by data subjects, such as the time spent reading policies, the amount of money earned or the ratings associated to each user. DPAs would act as a third party, limiting the collection of data as much as possible and only processing those strictly necessary to the performance of the service.
Although the privacy benefits of this service are expected to override the costs, opt-in is required for obvious reasons.

7.1.2 Implications

In El Dorado, a great deal of data subjects have benefitted from the free courses on data protection and have taken advantage of the reward system, devoting more psychological resources to the supervision of their data; in addition, the compulsory use of the authorised SDK, the report button and the web presence of the public relations office have notably promoted compliance.
However, in this scenario, when users check the daily weather forecast to see if they need their umbrella or want to find recipes to impress their mother-in-law when she shows up unannounced, they still don't have the time to read consent materials; even though they might have taken data protection courses and policies are simplified and shortened as much as possible, understanding how a particular controller is going to process their data often still takes too long. In those cases, they might rely on ratings, but not all services have been reviewed; besides, ratings are often unreliable since many data subjects submit as many of them as possible in the hope of winning the big cash prize. Plenty of users remain uninterested in data protection but try to profit from the reward system nonetheless by buying multiple devices from which they access as many consent materials as possible.
For a great number of wealthy data subjects, financial gain is not a sufficient incentive to change their behaviour and they keep giving their consent without paying attention to how their personal information is processed. At the same time, many users still value customisation over privacy, and only read notices in their free time in the hope of making some money out of it.
Children use digital platforms without understanding that they're giving away their data, and remain unable to grasp the meaning of policies.
Though the Web is crawled in the search of privacy violations, new services keep emerging and many of them still operate illegally.

7.2 From practice to theory

Even if something like El Dorado takes place, as highlighted, many problems undermining the significance of consent would likely remain significant, therefore continuing to compromise the practical relevance of EU data protection laws; this raises the question, shall we then attempt to make laws more practically effective by altering the conceptual framework on which consent is grounded?
Before going further, it should be stressed that there are significant reasons why consent is envisioned as the functional expression of individual autonomy. The Preamble to the Charter of Fundamental Rights[4] states expressly that the European Union "places the individual at the

heart of its activities": according to Rodotà (2007)[45], this implies that the autonomous and fundamental right to data protection contributes to the constitutionalisation of the person and is hence an essential tool to freely develop one's personality. In human-rights thinking, consent represents in fact a means to legitimate actions that wouldn't otherwise be acceptable (Kosta, 2013[12]; Brownsword, 2004[87]). That being said, there is a common misconception about privacy, namely that it is reducible to a singular essence, and people often justify their lack of concern with the argument that they have nothing to hide (Solove, 2007)[105]. However, it is well known that consenting to the processing of data doesn't impose privacy costs only on the single users who do, but on others too, especially in networked environments: in the presence of large data sets, in fact, personality traits of users who refrain from sharing their information can be inferred from data shared by members of their network (MacCarthy, 2010[106]; Hermstruwer, 2017[107]). Edward Snowden, the whistleblower who exposed the NSA surveillance programmes[74], memorably rebutted the nothing to hide argument stating that "[...] Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."[108]
The social dimension of consent magnifies the risks arising from the incompetence and faulty rationality of the average user; should individual liberties then be overridden in the interest of collective ones?

7.2.1 Digital Tyranny

Let us imagine, for the sake of argument, that in response to scientific evidence, policymakers, legislators and DPAs finally acknowledge the difficulties faced by average users in controlling their privacy preferences, and decide that in order to protect both individual and societal welfare, consent can no longer be held as a demonstration of autonomous wishes, but should instead become a heteronomous decision. Admitted that there is no way to make data subjects become expert supervisors of their personal data in the near future, new supervisors need to be appointed; accordingly, the giving of consent becomes conditional on the approval of these entities. Each user is thus assigned his/her own Personal Data Manager (PDM); due to evident logistic problems, there cannot be human PDMs for all data subjects, and this role is assigned to digital agents. Whenever data controllers wish to process data that are not necessary to the performance of a contract, they do not only need the consent of data subjects, but that of their PDM as well. An official SDK is created, and controllers are required to make use of it to forward consents to PDMs prior to carrying out the processing.
The choice of whether to approve or reject consent requests is not operated on the basis of individual preferences, as these are often unclear, but is made by taking into account the type and amount of data that each controller owns; once a certain threshold is reached (set proportionally to the type of information collected and the number of users tracked), controllers are not allowed to carry out additional processing unless their DPO can produce evidence that they have erased all the data in their possession. These limits do not apply to the processing of data carried out by public research institutes, as the welfare of society would be compromised too greatly.
Users who expressly wish to have their personal information processed are required to take an examination so as to substantiate their wish and to demonstrate that they are actually competent enough to adequately evaluate risks and benefits; provided said test is passed, their PDM will tag their fingerprints accordingly, but they might still incur in restrictions depending on the volume of data shared. Every so often, a new test will be administered to verify that their skills are up-to-date. Incompetent data subjects who suffer from the processing limitations and struggle to give up highly customised services are encouraged to become educated and are offered online courses targeted to pass the examination.
To ensure that compliance is honoured, machine aid is also sought in crawling the Web and the various app marketplaces in order to identify unlawful processing and privacy violations; all controllers carrying out illegal activity are fined and their services are either quarantined or shut down.
Needless to say, PDMs need to keep track of both user and controller activity; these data are stored on dedicated servers situated in confidential locations in each Member State and can only be accessed by verified profiles. Users have the right to access and erase their data from this server, would they wish to do so, but erasure from the central server results in an obligation on data controllers to do the same; the DPO must again corroborate compliance.

7.2.2 Implications

In the world of the Digital Tyranny, large private gatherings of personal data are significantly prevented, and the freedom of society is better protected from the interests of the market and from those of many obscure characters who wish to exploit the vulnerabilities of users. Besides, non-compliance is more effectively inhibited by placing increased obligations on controllers and actually verifying that these are respected.
However, neither does this mean that data subjects are pleased with the new data protection framework, nor that their freedom is altogether safe. The technological experience, in fact, is much less adaptable, and finding relevant content is a way more laborious task; even if that pushes several users to become experts and try the examination, occasionally they are still denied access to services because controllers have reached the maximum limits of processing.
Sometimes, notably during electoral campaigns, particular news are displayed to users on multiple platforms and with suspicious prominence.
The awareness of governmental tracking reduces considerably online expression and activity; the most privacy-concerned and knowledgeable data subjects seek refuge on unauthorised digital networks.
The availability of the centralised databases boosts advances in public research, and the pace of progress increases dramatically, especially in fields related to the natural sciences.
The danger of data breaches is stronger than ever and servers are continuously under attack.

8. Discussion

Two very different scenarios for the problems of consent were envisioned. On one hand, we pictured the introduction of drastic measures to encourage data subjects to become autonomous, providing them with standardised and simplified information and with shortcuts to understand consent materials, with both a social and an authoritative dimension to rely on (i.e., user ratings and real-time feedback from DPAs); interest in personal data supervision is incentivised by leveraging on users' tendency to favour immediate rewards. On the other hand, the very ethical framework on which consent is grounded is challenged by assuming that data subjects are stripped of their individual and fundamental rights, in a bid to prevent them from recklessly giving away their personal information and thus undermine the freedom of society. In the present section, these scenarios are examined with a more ground-based approach and put in perspective with existing research.

8.1 Scenario 1: El Dorado

In El Dorado, the right to data protection is considered so valuable that users are encouraged with all means available to overcome their cognitive limitations. Under this framework, policy respects their autonomy, but attempts to not over-value it: while data subjects remain the sole overseers of the processing of their personal information, they can count on additional tools to easily retrieve some of the information that they need to make meaningful choices. The knowledge gap is perhaps still open, but for users who do have privacy-protective intentions, its span is less wide.
Ratings are introduced on the grounds that, though privacy behaviour depends strongly on individual preferences, it can be altered by social influence. When users have low ability to carry out the behaviour, in fact, they tend to rely on peers and to learn privacy practices from them (Mendel & Toch, 2017)[109]. Descriptive social norms are indeed powerful influences and can be used to nudge behaviour (Bicchieri & Dimant, 2019)[85]. Besides, rating systems could potentially encourage compliance.
By pairing laws with technology-specific instruments, many of the shortcomings of the technology-neutral approach can be prevented: the standardisation of consent interfaces through SDKs, for one, would ensure that data controllers actually give subjects the chance to make meaningful choices and stop resorting to instruments such as tracking walls. On the flip side, though this matter is out of scope, the implementation of certain requirements might be quite expensive for controllers (McAllister 2017)[110].
In this scenario, the inclination of users to overvalue immediate benefits is exploited in their own interest by rewarding privacy-protective behaviour; this could be interpreted as nudging, and it is debatable whether such an intervention would compromise the autonomy of users.

Although plenty of researchers have examined the behaviour of users when they are presented with privacy/monetary trade-offs (e.g., Acquisti & Grossklags, 2003[111]; Hann et al., 2007[112]), to our best knowledge there are no existing studies that focus on the effect of financial gains on privacy behaviour when these are opposed to a different kind of reward (i.e. immediate service access). Be that as it may, the monetary nature of the reward is somehow arbitrary, and could easily be substituted by different types of benefits. It should be noted that, in the event that rewards are used, particular attention must be placed on motivation, as they may, in certain cases, undermine it (Cialdini et al., 1998)[113].
That being said, El Dorado shows that, even if policymakers go to much greater lengths in the attempt to encourage users to get involved in data protection, there seem to be insurmountable limits as regards both the data subjects' cognitive power and the extent to which the environment can be simplified. While full autonomy is perhaps indeed a pipe dream, however, there could be a variety of solutions to implement so as to enhance autonomy significantly: if DPAs were provided with more funds and technical staff, for instance, the knowledge gap between data subjects and controllers could be reduced (e.g. by giving users expert advice) and non-compliance would be prosecuted more effectively.

8.2 Scenario 2: Digital Tyranny

As opposed to El Dorado, the framework of data protection envisioned in the Digital Tyranny scenario views the obstacles of individual autonomy as unconquerable and, by reason of the harm that these bestow upon the community, moves away from the typical rights-based respect for individual liberties in order to support the collective welfare instead, approaching the issue with what could be deemed a more utilitarian perspective (assuming that the measure of welfare chosen is the preservation of societal freedom from private interests).
It does so by taking a paradoxical compromise, whereby greater amounts of data are processed so as to gain more regulatory power and control on the private (ab)use of data, which, as discussed earlier, poses substantial risks to the dignity and freedom of the community as a whole. In such a scenario, the emergence of multiple private data monopolies would be prevented by creating a single, public one; this approach, however, comes with conspicuous pitfalls.
To begin with, there are self-evident ethical problems in taking the right to an autonomous choice away from data subjects: the word autonomy literally means "*self law*" in Greek, and entails, among others, the freedom for oneself to self-govern with no external interference[13]. To make the consent of data subjects heteronomous in their own interests would mean to adopt a paternalistic stance, and paternalism is harshly critiqued by human rights proponents, even in its softer forms, in view of the fact that it subjugates the liberty of individuals to welfare judgments made by some other planner with which they might not agree (Mitchell, 2004)[114]. In addition, paternalistic solutions presuppose a level of citizen trust that governments often do not enjoy (Kapsner & Sandfuchs, 2015)[115].
While democratic processes and political equilibria in this scenario would be relatively safer from the interests of private companies, they could still be subject to those of public authorities. Even though the governments of all European Member States share a democratic character, it is well-known that sometimes even democracies can unduly track users or manipulate information to their advantage, occasionally even partnering with private businesses. Some examples: an investigation conducted by Appelbaum et al. (2014)[116] revealed that users worldwide are tracked by the NSA just for using privacy-enhancing software; YouTube seems to have been removing comments that insulted China's Communist Party (Vincent, 2020)[117]; Google was planning to launch a censored version of its search engine in China that would have reportedly blacklisted websites and search terms about human rights, democracy, religion, and peaceful protest (Gallagher, 2018)[118]; an Egyptian cartoonist was sentenced to three years in jail for posting an edited picture of President Abdel Fattah el-Sisi with Mickey Mouse ears (Walsh & Ismail, 2016)[119].
As it turns out, an incredibly high number of governments are already deploying advanced tools to identify and monitor users on immense scales. A report issued in 2019 by Freedom House, an organisation that researches issues related to democracy, political rights and civil liberties, showed that of 65 countries covered (not all European, but making up 87% of the world's internet user population), 40 have instituted advanced social media monitoring programmes, and that this trend is rapidly accelerating. 47 of these countries featured arrests of users for political, social, or religious speech (Shahbaz & Funk, 2019)[120].

Actually, it appears that governments can already resort to surveillance techniques if they wish to do so; nonetheless, centralised data would produce more accurate predictions, and eventual data breaches would pose greater risks to the dignity and freedom of citizens, as for instance in case of cross-border influence operations, which are becoming an increasingly common problem[75][76][120].
These are only some of the biggest issues that the Digital Tyranny model would entail; ultimately, by attempting to protect users from certain types of influence, they would be more vulnerable to some others, and to a greater extent.
In conclusion, if our aim is that of giving users actual data protection and freedom, the subjugation of individual liberties doesn't seem like the right plan of action.

9. Limitations and future directions

The methodology chosen to carry out this study is, by definition, quite speculative; though scenario planning allows to stress and bring to light certain issues and to evaluate possible solutions, the same combination of the axes could lead to multiple other outcomes, and those that were discussed were chosen with a fair degree of arbitrariness. The decision to encourage users to become involved in the supervision of their personal data through financial gain, for instance, is only one of the possible arrangements, and monetary rewards could be substituted for example by social ones instead.
Moreover, the present inquiry disregards almost completely the point of view of data controllers, and doesn't venture into the identification of the problems that the current model of data protection and those presented in the envisioned scenarios might entail for these entities. It should therefore be noted that the strengthening of the data protection framework might pose new challenges to the healthy development of the Digital Single Market.
Matters addressed when developing scenarios are approached rather conceptually, and plenty of technical issues arising from the relative settings were likely overlooked. Besides, the data protection systems presented in the scenarios focus mainly on the processing of data that is carried out through browsers and mobile apps, but they don't necessarily apply to the whole range of emerging technologies such as VoIP and OTT platforms.
Future research could investigate the effect of rewards on privacy behaviour in the specific case of consent materials, study the impact of rating systems on compliance or devise interaction models of social machines designed to support DPAs in exercising their investigative and corrective powers.

10. Conclusion

This research aims to challenge present structures in a provocative way. Though the reasons why citizens should be granted individual autonomy could be said to be obvious, this analysis strives to highlight the importance of aligning the theoretical framework surrounding consent in data protection as much as possible with its actual enactment. Though full autonomy is likely unachievable, the risks posed to both individual and societal freedom by the processing of user data make it imperative to devise a more effective regulatory system that can grant data subjects the chance to make actually meaningful choices, possibly by offering them the assistance of some trusted figures.
Whilst the focus of the present research is put primarily on consent, the intention was that of using it as a pivot to bring to light a variety of other issues associated with the inadequacies of legal provisions in relation to behavioural research and to common technological practices, or, in other words, with their failure to take into account the empirical side of the current data protection strategy.
There are two main reasons why the relevance of consent to data processing appears marginal, if we consider the magnitude of the dangers discussed: first, because it presupposes compliance, and second because behavioural insights can still be inferred from data that are considered necessary to the performance of contracts. Despite the relatively strong framework of protection brought forward by the adoption of the GDPR, in fact, privacy violations and non-compliance remain sadly ubiquitous. Besides, behavioural surplus, as Shoshana Zuboff (2019) [121] calls it, can be inferred from many types of data, and definitely not just from those for which user consent is required; the problem of data protection is clearly much bigger than consent.

That being said, if the issues related to consent were addressed more effectively and the limitations to the autonomy of users were better taken into account by policymakers, the whole framework of protection would likely benefit from it.
The matter of making consent autonomous in practice doesn't seem attainable, if we look at consent as a fully autonomous act. However, there is considerable room for improvement with regard to the way in which the current data protection framework regulates the environment: for one, it is necessary that policy ceases to regard the data subject as a homo economicus and shifts to more empirically-grounded behavioural models such as that of bounded rationality. As importantly, flexible technological instruments need to be paired with laws to counteract their static nature and their technological agnosticism, which is particularly significant in order to encourage compliance.
Ultimately, policy that grants partial individual autonomy appears like a preferable alternative to a system that takes away our individual rights, even if it is made in the interests of the whole community; though the dangers of governmental surveillance and cross-border psyops are already tangible, autonomy remains a necessary utopia.

Acknowledgements

We thank Mirjam van Reisen, Valentina Pavel, Maja Nišević and Giulio Barbero for providing us with useful feedback which allowed us to improve the quality of this research.
I (Gaia Manganello) would also like to thank Peter van der Putten for supporting me in overcoming the obstacles that I encountered throughout this process and Maarten Lamers for offering a helping hand when it was very much needed.

Reference

[1] Jensen, C., & Potts, C. (2004, April). Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (pp. 471-478). ACM.
[2] Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514.
[3] Carolan, E. (2016). The continuing problems with online consent under the EU's emerging data protection principles. *Computer Law & Security Review*, *32*(3), 462-473.
[4] European Parliament, Office for Official Publications of the European Communities. (2000). Charter of fundamental rights of the European Union. Luxembourg: Office for Official Publications of the European Communities. Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf
[5] European Parliament and Council. (2002, July 12). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN
[6] European Parliament and Council. (2016, April 27). Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Advancement of Such Data. Retrieved from https://gdpr-info.eu
[7] Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 1-20.
[8] European Commission. (2017, January 10). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Retrieved November 4, 2019 from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=EN
[9] Kingdon, John W. (1984). Agendas, alternatives, and public policies. Boston: Little, Brown.
[10] European Union Agency for Fundamental Rights. (2018). Handbook on European data protection law. Retrieved November 15, 2019 from https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law
[11] Manson, N. C., & O'Neill, O. (2007). Rethinking informed consent in bioethics. Cambridge University Press.
[12] Kosta, E. (2013). Consent in European data protection law. Martinus Nijhoff Publishers.
[13] Feinberg, J. (1982). Autonomy, sovereignty, and privacy: Moral ideals in the constitution. *Notre Dame L. Rev.*, *58*, 445.
[14] European Union. (2007, December 17). Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community. 2007/C 306/01. Retrieved February 7, 2020 from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12007L/TXT&from=EN
[15] Article 29 Working Party. (2011, July 13). Opinion 15/2011 on the definition of consent. Retrieved January 20, 2020 from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf
[16] European Parliament and Council. (1995, October 24). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en
[17] Article 29 Data Protection Working Party. (2009, 1 December). The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the

fundamental right to protection of personal data. Retrieved from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf
[18] European Commission. (2010, November 11). Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52010DC0609&from=en
[19] European Data Protection Supervisor. (2015, July 27). Opinion 3/2015 (with addendum). Europe's big opportunity EDPS recommendations on the EU's options for data protection reform. Retrieved from: https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_en.pdf
[20] European Data Protection Board. (2019, March 12). Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. Retrieved December 15, 2019 from: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf
[21] Article 29 Working Party. (2018, April 10). Guidelines on consent under Regulation 2016/679. Retrieved December 15, 2019 from: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
[22] G Karácsony, G. (2019). Managing Personal Data in a Digital Environment-Did GDPR's Concept of Informed Consent Really Give Us Control?. Počítačové právo, UI, ochrana údajov a najväčšie technologické trendy. Zborník príspevkov z medzinárodnej vedeckej konferencie. Vysoká skola Dabubius.
[23] Jesus, V., & Mustare, S. (2019, August). I Did Not Accept That: Demonstrating Consent in Online Collection of Personal Data. In *International Conference on Trust and Privacy in Digital Business* (pp. 33-45). Springer, Cham.
[24] Schermer, B. W., Custers, B., & van der Hof, S. (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.
[25] Steinfeld, N. (2016). "I agree to the terms and conditions":(How) do users read privacy policies online? An eye-tracking experiment. *Computers in human behavior*, *55*, 992-1000.
[26] Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*.
[27] Kahneman, D., & Tversky, A. (1984). Choices, values, and frames. American Psychologist, 39(4), 341–350.
[28] Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE security & privacy*, *3*(1), 26-33.
[29] Van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of consumer policy*, *42*(1), 91-107.
[30] Pardo, R., & Métayer, D. L. (2019). Analysis of Privacy Policies to Enhance Informed Consent. *arXiv preprint arXiv:1903.06068*.
[31] Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019, November). (Un) informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 973-990). ACM.
[32] Zuiderveen Borgesius, F. J., Kruikemeier, S., Boerman, S. C., & Helberger, N. (2017). Tracking walls, take-it-or-leave-it choices, the GDPR, and the ePrivacy regulation. *Eur. Data Prot. L. Rev.*, *3*, 353.
[33] European Data Protection Board. (2020, May 4). Guidelines 05/2020 on consent under Regulation 2016/679. Retrieved from: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf
[34] Forbrukerrådet. (2020, January 14). Out of control. Retrieved June 2, 2020 from: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf
[35] European Commission. (2016, October 3). REFIT Evaluation and Impact Assessment of Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Retrieved December 16, 2019 from: https://ec.europa.eu/smart-regulation/roadmaps/docs/2016_cnect_013_review_eprivacy_en.pdf

[36] European Digital Rights. (2019, November 22). ePrivacy: EU Member States push crucial reform on privacy norms close to a dead end. Retrieved December 17, 2019 from: https://edri.org/eprivacy-eu-member-states-push-crucial-reform-on-privacy-norms-close-to-a-dead-end/
[37] European Parliament and Council. (2009, November 25). Directive 2009/136/EC. Retrieved December 17, 2019 from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0136&from=EN
[38] European Data Protection Supervisor. (2017, October 5). EDPS recommendations on specific aspects of the proposed ePrivacy Regulation. Retrieved December 17, 2019 from: https://edps.europa.eu/sites/edp/files/publication/17-10-05_edps_recommendations_on_ep_amendments_en.pdf
[39] Article 29 Working Party. (2017, April 4). Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC). Retrieved December 17, 2019 from: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610140
[40] European Economic and Social Committee. (2017, October 13). Opinion of the European Economic and Social Committee on the 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)'. Retrieved December 17, 2019 from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017AE0655&from=EN
[41] European Court of Justice. (2019, October 1). Case C–673/17. Retrieved December 14, 2019 from: http://curia.europa.eu/juris/celex.jsf?celex=62017CJ0673&lang1=en&type=TXT&ancre=
[42] Marvin, G. (2017, September 8). Google responds to Apple's Intelligent Tracking Prevention with AdWords tracking update. *Search Engine Land*. Retrieved February 6, 2020 from: https://searchengineland.com/google-analytics-adwords-response-apple-intelligent-tracking-prevention-282233
[43] Flynn, K. (2018, October 9). WTF are Facebook's first-party cookies for pixel? *Digiday*. Retrieved February 6, 2020 from: https://digiday.com/marketing/wtf-what-are-facebooks-first-party-cookies-pixel/
[44] Council of the European Union. (2020, May 29). Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Progress report. Retrieved from: https://www.consilium.europa.eu/media/44301/st_8204_2020_init_en.pdf
[45] Rodotà, S. (2007, October 12/13). Data protection as a fundamental right. *Keynote speech for "Reinventing Data Protection" International Conference.*
[46] Fouad, I., Santos, C., Al Kassar, F., Bielova, N., & Calzavara, S. (2020, July). On Compliance of Cookie Purposes with the Purpose Specification Principle. In *IWPE*.
[47] Meinert, D. B., Peterson, D. K., Criswell, J. R., & Crossland, M. D. (2006). Privacy policy statements and consumer willingness to provide personal information. *Journal of Electronic Commerce in Organizations (JECO)*, *4*(1), 1-17.
[48] Marotta-Wurgler, F. (2012). Does Contract Disclosure Matter?. *Journal of Institutional and Theoretical Economics JITE*, *168*(1), 94-119.
[49] Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, *64*, 122-134.
[50] s, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226-261.
[51] Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32-48.
[52] Acquisti, A., Adjerid, I., & Brandimarte, L. (2013). Gone in 15 seconds: The limits of privacy transparency and control. *IEEE Security & Privacy*, *11*(4), 72-74.
[53] Curren, L., & Kaye, J. (2010). Revoking consent: A 'blind spot'in data protection law?. *Computer law & Security review*, *26*(3), 273-283.
[54] Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, *29*(5), 509-521.
[55] Kamara, I. (2017). Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation'mandate'. *European journal of law and technology*, *8*(1).

[56] Ataei, M., Degbelo, A., Kray, C., & Santos, V. (2018). Complying with privacy legislation: from legal text to implementation of privacy-aware location-based services. *ISPRS International Journal of Geo-Information*, *7*(11), 442.
[57] Madge, R. (2017, August 27). Five loopholes in the GDPR. *Medium*. Retrieved December 18, 2019 from: https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b
[58] Ryan, J., & Toner, A. (2020, April). Europe's governments are failing the GDPR. *Brave*. Retrieved from: https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf
[59] Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P. A., & Santos, I. (2019, July). Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security* (pp. 340-351).
[60] Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020, April). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1-13).
[61] Vlajic, N., El Masri, M., Riva, G. M., Barry, M., & Doran, D. (2018, January). Online Tracking of Kids and Teens by Means of Invisible Images: COPPA vs. GDPR. In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security* (pp. 96-103).
[62] McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *Isjlp*, *4*, 543.
[63] Pollach, I. (2005). A typology of communicative strategies in online privacy policies: Ethics, power and informed consent. *Journal of Business Ethics*, *62*(3), 221.
[64] Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215-236.
[65] Collingridge, D. (1980). The social control of technology.
[66] Kahneman, D., Knetsch, J. L., & Thaler, R. H. (1991). Anomalies: the endowment effect, loss aversion, and status quo bias. The Journal of Economic Perspectives, 5(1), 193–206.
[67] Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev.*, *126*, 1880.
[68] Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, *79*, 119.
[69] Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior. In *Economics of information security* (pp. 165-178). Springer, Boston, MA.
[70] Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in–depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology*, *45*(3), 285-297.
[71] Plona, A. (2015, June 22). Threats of A/B tests and UX research: adoption time and incrementalism. *Medium*. Retrieved November 14, 2019 from https://medium.com/pminsider/threats-of-a-b-tests-and-ux-research-adoption-time-and-incrementalism-991c0c3c61b6
[72] Forbrukerrådet. (2018, June 27). Deceived by Design. Retrieved December 14, 2019 from: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf
[73] European Digital Rights. (2019, October 11). Open letter to EU Member States. Retrieved December 11, 2019 from: https://edri.org/files/eprivacy/ePrivacy_NGO_letter_20191011.pdf
[74] Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*, *17*, 22.
[75] Intelligence and Security Committee of Parliament. (2020, July 21). Russia. Retrieved from: https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl
[76] Cadwalladr, C. (2020, July 26). If you're not terrified about Facebook, you haven't been paying attention. *The Guardian*.
[77] Greenwald, G. (2014). No place to hide: Edward Snowden, the NSA, and the US surveillance state. Macmillan.
[78] Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems*, *98*, 660-671.
[79] Breaux, T. D., & Anton, A. I. (2005, June). Deriving semantic models from privacy policies. In *Sixth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'05)* (pp. 67-76). IEEE.

[80] Brodie, C. A., Karat, C. M., & Karat, J. (2006, July). An empirical study of natural language parsing of privacy policy rules using the SPARCLE policy workbench. In *Proceedings of the second symposium on Usable privacy and security* (pp. 8-19). ACM.
[81] Belli, L., Schwartz, M., & Louzada, L. (2017). Selling your soul while negotiating the conditions: from notice and consent to data control by design. *Health and Technology*, *7*(4), 453-467.
[82] Drozd, O., & Kirrane, S. (2019, August). I Agree: Customize your Personal Data Processing with the CoRe User Interface. In *International Conference on Trust and Privacy in Digital Business* (pp. 17-32). Springer, Cham.
[83] Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., ... & Bouwman, J. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific data*, *3*.
[84] Van Reisen, M., Stokmans, M., Basajja, M., Ong'ayo, A. O., Kirkpatrick, C., & Mons, B. (2019). Towards the Tipping Point for FAIR Implementation. *Data Intelligence*, 264-275.
[85] Bicchieri, C., & Dimant, E. (2019). Nudging with care: The risks and benefits of social information. *Public Choice, Forthcoming*.
[86] Wilkinson, T. M. (2013). Nudging and manipulation. *Political Studies*, *61*(2), 341-355.
[87] Brownsword, R. (2004). The cult of consent: fixation and fallacy. *King's Law Journal*, *15*(2), 223-251.
[88] Van Eijk, N., Helberger, N., Kool, L., van der Plas, A., & van der Sloot, B. (2012). Online tracking: Questioning the power of informed consent.
[89] StatCounter. (2019). Browser Market Share Worldwide. Retrieved from: https://gs.statcounter.com/browsermarket-share
[90] Deloche-Gaudez, F. (2001). The Convention on a Charter of Fundamental Rights: A method for the future?
[91] Beer, D. (2017). The social power of algorithms.
[92] Gintis, H. (2000). Beyond Homo economicus: evidence from experimental economics. *Ecological economics*, *35*(3), 311-322.
[93] Henrich, J., Boyd, R., Bowles, S., Camerer, C., Fehr, E., Gintis, H., & McElreath, R. (2001). In search of homo economicus: behavioral experiments in 15 small-scale societies. *American Economic Review*, *91*(2), 73-78.
[94] Reisch, L. A., & Zhao, M. (2017). Behavioural economics, consumer behaviour and consumer policy: state of the art. *Behavioural Public Policy*, *1*(2), 190-206.
[95] Simon, H. A. (1955). A behavioral model of rational choice. *The quarterly journal of economics*, *69*(1), 99-118.
[96] Simon, H. A. (1990). Bounded rationality. In *Utility and probability* (pp. 15-18). Palgrave Macmillan, London.
[97] Hoofnagle, C. J., & Urban, J. M. (2014). Alan Westin's Privacy Homo Economicus. *Wake Forest Law Review*.
[98] Han, B. C. (2017). Psychopolitics: Neoliberalism and new technologies of power. Verso Books.
[99] Inayatullah, S. (2013). Futures studies: theories and methods. *There's a future: Visions for a Better World, BBVA, Madrid*, 36-66.
[100] Lindgren, M., & Bandhold, H. (2003). *Scenario planning*. Palgrave.
[101] Wilkinson, L. (1995). How to build scenarios. *Wired*, *3*(10), 74-81.
[102] Rockefeller Foundation. (2010). Scenarios for the future of technology and international development.
[103] Ramirez, R., & Wilkinson, A. (2016). Strategic reframing: The Oxford scenario planning approach. Oxford University Press.
[104] Azmayesh, S., Borchardt, J.-C., De Jong, M., McGowan, I., Mullen, E., Roy, H., Stout, J. & Talib, C. (2012). Terms of Service; Didn't Read. Retrieved from: https://tosdr.org/index.html
[105] Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.*, *44*, 745.
[106] MacCarthy, M. (2010). New directions in privacy: Disclosure, unfairness and externalities. *ISJLP*, *6*, 425.
[107] Hermstruwer, Y. (2017). Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, *8*, 9.
[108] Snowden, E. (2015, May 21). Just days left to kill mass surveillance under Section 215 of the Patriot Act. We are Edward Snowden and the ACLU's Jameel Jaffer. AUA. *Reddit*. Retrieved

from: https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under/crglgh2/
[109] Mendel, T., & Toch, E. (2017, February). Susceptibility to social influence of privacy behaviors: Peer versus authoritative sources. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (pp. 581-593).
[110] McAllister, C. (2017). What About Small Businesses: The GDPR and Its Consequences for Small, US-Based Companies. *Brook. J. Corp. Fin. & Com. L.*, *12*, 187.
[111] Acquisti, A., & Grossklags, J. (2003, May). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. In *2nd Annual Workshop on Economics and Information Security-WEIS* (Vol. 3, pp. 1-27).
[112] Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, *24*(2), 13-42.
[113] Cialdini, R. B., Eisenberg, N., Green, B. L., Rhoads, K., & Bator, R. (1998). Undermining the Undermining Effect of Reward on Sustained Interest 1. *Journal of applied social psychology*, *28*(3), 249-263.
[114] Mitchell, G. (2004). Libertarian paternalism is an oxymoron. *Nw. UL Rev.*, *99*, 1245.
[115] Kapsner, A., & Sandfuchs, B. (2015). Nudging as a threat to privacy. *Review of Philosophy and Psychology*, *6*(3), 455-468.
[116] Appelbaum, J. R., Gibson, A., Goetz, J., Kabisch, V., Kampf, L., & Ryge, L. (2014). NSA targets the privacy-conscious. Web publication/site, NDR. Retrieved from https://daserste.ndr.de/panorama/aktuell/NSA-targets-the-privacy-conscious,nsa230.html
[117] Vincent, J. (2020, May 26). YouTube is deleting comments with two phrases that insult China's Communist Party. *The Verge*. Retrieved from: https://www.theverge.com/2020/5/26/21270290/youtube-deleting-comments-censorship-chinese-communist-party-ccp
[118] Gallagher, R. (2018, August 1). Google plans to launch censored search engine in China, leaked documents reveal. *The Intercept*. Retrieved from: https://theintercept.com/2018/08/01/google-china-search-engine-censorship/
[119] Walsh, D. & Ismail, A. (2016, January 31). Cartoonist Is Arrested as Egypt Cracks Down on Critics. The New York Times. Retrieved from: https://www.nytimes.com/2016/02/01/world/middleeast/egypt-islam-gawish-cartoonist.html
[120] Shahbaz, A. & Funk, A. (2019). The Crisis of Social Media. *Freedom House*. Retrieved from: https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf
[121] Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019. Profile Books.