Giannopoulou, Alexandra

Article

Algorithmic systems: The consent is in the detail?

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Giannopoulou, Alexandra (2020) : Algorithmic systems: The consent is in the detail?, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 9, Iss. 1, pp. 1-19, https://doi.org/10.14763/2020.1.1452

This Version is available at:
https://hdl.handle.net/10419/216218

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | Issue 1

Algorithmic systems: the consent is in the detail?

Alexandra Giannopoulou
Blockchain and Society Lab, University of Amsterdam, Netherlands, a.giannopoulou@uva.nl

Published on 23 Mar 2020 | DOI: 10.14763/2020.1.1452

Abstract: Applications of algorithmically informed decisions are becoming entrenched in society, with data processing being their main process and ingredient. While these applications are progressively gaining momentum, established data protection and privacy rules have struggled to incorporate the particularities of data-intensive information societies. Consequently, there is a misalignment created between algorithmic processing of personal data and the corresponding regulatory frameworks since they both strive for meaningful control over personal data. However, the challenges to the traditional role and the concept of consent are particularly manifest. This article examines the transformation of consent in order to assess how the concept in itself as well as the applied models of consent can be reconciled to correspond not only to current data protection normative frameworks but also to algorithmic processing technologies. This particularly pressing area of safeguarding a fundamental aspect of individual control over personal data in the algorithmic era is interlinked with practical implementations of consent in the technology used. Moreover, it relates to adopted interpretations of the concept of consent, to the scope of application of personal data, as well as to the obligations enshrined in them. What makes consent efficient as a data protection tool? Can its previous glory be maintained within the current techno-legal challenges?

Keywords: Algorithms, GDPR, Data protection, Consent

Article information

Received: 12 Apr 2019 **Reviewed:** 21 Mar 2020 **Published:** 23 Mar 2020

Funding: The Lab has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under grant agreement No 759681.
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/articles/analysis/algorithmic-systems-consent-detail

Citation: Giannopoulou, A. (2020). Algorithmic systems: the consent is in the detail?. *Internet Policy Review*, *9*(1). DOI: 10.14763/2020.1.1452

INTRODUCTION

Over the last decade, algorithmic dominance has transformed both individual and collective activities by making data collection and processing ubiquitous, consequently altering

foundational decision-making processes. This paper will map out the difficulties in applying traditional consent models to data-driven algorithmic systems on the one hand, and the diversity of existing solutions on the other. Firstly, we turn our attention towards the innovation-driven consent systems that have been consistently developed: from signaling to AI-guided models, consent is seen as an opportunity to mediate the expression of autonomy through technological applications. Secondly, we proceed to outline theoretical frameworks that have supported alternative consent implementations. Finally, we attempt to reframe the approach towards the incompatibility between data protection and algorithmic processing in order to highlight new - regulatory, governance, and technological - pathways that aim to release the accumulated tension towards consent as a singular expression of individual empowerment. We conclude by showcasing that concentrated efforts have shifted towards solutions that improve the negotiating power between actors and that ensure the existence of appropriate mechanisms at play in order to safeguard autonomy. Expression of consent is not a dual function, but can exist on a spectrum through a variety of theoretical, normative or techno-governance mechanisms.

The broad vision of algorithmic data processing systems[1] is to reengineer current social power structures by creating decision-making 'fair' and 'transparent' mechanisms whose effects would serve the broader societal good (Mayer-Schönberger & Cukier, 2013). From smart home applications to voice assistants,[2] wearable sensors, and social reputation systems, the knowledge and market potential compounded by building models and observing patterns have put algorithmic data processing at the centre of a data-driven society along with the realisation of challenges that they carry for entrenched legal norms. Admittedly, personal data protection and algorithmic processing regularly collide because of the creation of power asymmetries between citizens and data processing entities. The continued reliance on consent to legitimise algorithmic processing of personal data has consistently been under scrutiny due to "the mountain of evidence" pointing to the "privacy disconnect" between norms and current practices. (Van Hoboken, 2019).

Research on consent has repeatedly pointed out its inefficiency (Koops, 2014; Barocas & Nissenbaum, 2014; Cohen, 2019) and proposed new techno-legal structures that would make it more *pro forma* efficient (Calo, 2013). Citizen empowerment expressed through individual control over personal data is being consistently held in a precarious position due to the expansive nature of these systems.[3] Following high-profile cases that brought significant data processing misuses to the public's attention and partially catalysed important legal reforms,[4] the lack of control over the fate of the data once collected has exasperated the need for meaningful data-control, informed consent, and the re-balancing of the radical power inequalities around data collection and processing. In fact, from a historical perspective, it was the response to similar emerging inequalities that led the framing of data protection rules in Europe even if consent appears only later in data protection legislation. More specifically, the OECD Guidelines introduced in 1980[5] and the Data Protection Directive of 1995[6] brought forward the role of individual consent in personal data processing (Kosta, 2013). According to Simmons, "consent is the deliberate (and communicatively successful) performance of acts or omissions whose conventional or contextual point is to communicate to others the agent's intention to undertake new obligations and/or convey to others new rights (with respect to the agent)" (2010). A look at the historical context of consent (Westin, 1967) reveals that the conceptualisation of the notions of privacy and data protection is distilled towards the concept of control (Hartzog 2018) over information that can be linked to natural persons and thus data subjects.[7] In fact, control - the "essence" of data protection and privacy - (Ausloos, 2018), acts both as a balancing act among different power actors involved in personal data flows and as a safeguard of fundamental rights

to privacy and to data protection. In the United States, control over personal data refers to the ability of individuals to evaluate situations and to make meaningful decisions about the collection and processing of the personal data. The concept of privacy self-management (Solove, 2013) refers to the "process of providing people with control over their personal data" in order to empower them to "decide for themselves how to weigh the costs and benefits of the collection, use, or disclosure of their information". The European legal framework adheres to the principle of data subject control as a foundational concept,[8] while also balancing out the regulatory burden by diffusing accountability across the network of participating key actors.

Control over data refers *inter alia* to individual agency, autonomy, and the ability to make rational choices based on the evaluation of the information provided about the use of the personal data.[9] In that regard, consent is an "essential guarantee of individual control over personal data" (Kosta & Cuijpers, 2014), without constituting its singular expression. Consent holds a prominent role in data protection as a manifestation of self-determination (Efroni et al, 2019) which also functions as an expression of individual autonomy.[10] It "plays a morally transformative role in interpersonal interactions" because it can "render permissible an otherwise impermissible act". (Edenbeg & Leta Jones, 2019). In the United States, consent is placed at the centre of privacy protection[11] (Solove, 2013; Hoofnagle, 2018: Reidenberg et al, 2015), while in Europe, the legal rules are based on the policy choice that consent could be rendered useless if not properly safeguarded.[12] As a matter of fact, consent in the GDPR constitutes one of the legal grounds for personal data processing (Art. 6 GDPR) provided that the expression of the consent presents the characteristics that depict the agency of the data subject (Art. 7 GDPR). The framing of what consent embodies has evolved along with the consecutive amendments to data protection laws, maintaining a still "cryptic" (Kosta, 2013) status. While article 2(a) of the Data Protection Directive 95/46/EC describes a freely given, specific and informed consent,[13] the GDPR has set up a stricter formulation that requires consent to be explicit for the processing of special categories of personal data. Consent must be given in a clear manner so as to indicate the intention of data subjects. GDPR Recital formulations[14] create guidelines for ensuring valid consent. What's more, the opinions published by the Article 29 Working Party (A29WP) on consent (A29WP, 2011; 2018) provide an additional but non-binding interpretation. For example, consent 'freely given' implies that data subjects should have the ability to exercise a real and genuine choice; consent is 'specific' and 'informed' when it is intelligible, referring clearly and precisely to the full scope, purposes and consequences of the data processing. Similarly, the Explanatory Report[15] of Modernized Convention 108[16] states that "(n)o undue influence or pressure which can be of an economic or other nature whether direct or indirect, may be exercised on the data subject and consent should not be regarded as freely given where the data subject has no genuine choice or is unable to refuse or withdraw consent without prejudice". Consent cannot be derived from silence, or pre-completed boxes and forms. Rather, it should be based on an appreciation and understanding of the implications of the data processing to which the data subject is consenting to.

If the reframing of consent in data protection rules has been instrumental in ensuring the continuous enhancement of the expression of user autonomy and control, new technologies are challenging its limits. There is growing skepticism over the efficiency of consent as a pervasive legal ground for legitimate personal data processing (Edwards & Veale, 2018; Kamarinou et al, 2016). The design of algorithmic data processing makes "the unpredictable and even unimaginable use of data a feature, not a bug" (Jones et al., 2018), which is directly at odds with the rights and obligations depicted in data protection rights and obligations such as the purpose specification obligation.[17] How can explicit (or even informed) consent be given for specified data processing purposes when the process itself is not transparent or when the purpose is

impossible to predict, specify, and explain *ex ante*? These questions are putting added pressure on the design of legally compliant systems. Consent faces thus a new challenge, requiring its adaptation by taking in consideration the particularities of the technology at hand.[18]

SECTION 1. TECHNOLOGICALLY ADEPT HUMAN CONSENT

The value of protecting personal data in the ecosystem of continuous learning - where collecting personal data is a *de facto* norm, is hard to estimate. Undoubtedly, there are endless possibilities in algorithmic data processing. In this highly intense data-driven environment, the expression of human autonomy and control make data protection and privacy compliance with the normative framework challenging.

TECHNOLOGICAL CHALLENGES OF CONSENT

The distribution of lawful grounds for personal data processing - normatively transposing the control principle through fair balancing - applies poorly in cases of algorithmic data processing. In fact, A29WP has concluded that in many cases of algorithmic data processing affecting individuals' lives (such as targeting, price discrimination, etc.), focus should be given on getting consent (A29WP, 2014). The technological conditions continuously weaken the ability to provide lawful consent, while the GDPR "places more focus on the concept of informed consent than ever"; it is a "paradoxical situation" (Van Hoboken, 2019). Consent is the only lawful processing ground to not include the necessity criterion making it ideal for algorithmic processes. In this technological environment, meaningful application of valid consent is challenging.[19] The difficulty lies in the implementation of consent mechanisms that are both compliant with the validity conditions of applicable regulations and which also convey the moral justifications of consent. The revision of consent mechanisms and consent design in order to instill control in the current technological realities has failed to address the paradox of consent.[20] According to Lilian Edwards and Michael Veale (2018),

> the new parameter that has been introduced by AI and machine learning algorithmic models is the lack of foresight by the data controller (let alone the data subjects) with regard to what the precise model, processing method and result of the data in question will be. This technological advancement makes data protection difficult to ensure because of the impossibility of ensuring an informed consent by the data subjects. In that regard, more specifically continuous validation of informed consent seems impossible because it refers to the assumption that a complete ex ante knowledge of the technology and of the evolution process of the algorithms will produce a fully informed consent.

The consent criteria that require valid consent to be both specific and informed is hard to reconcile in a reality involving AI and big data because "it implies that the data subject understands the facts and consequences of the processing and consent; information must be provided about all relevant aspects of the processing (…) Specifying the purposes of analysis can be difficult in big data." (Oostveen, 2018). More specifically, there is a discrepancy between the formal requirements of the law and the practices observed in real life applications of data protection[21] because these practices are often lacking in compliance checks and standards.

Hence, in this technological context, consent as a data protection essential tool risks being subject to erosion and reduced to a formality, being rendered illusory, or even meaningless. This criticism of consent applicability is not new among scholars (Zuiderveen Borgesius, 2014). From consent validity requirements to the definition of personal data (Purtova, 2018), and from the non-linear collection of data to the difficulty in *a priori* separating individuals' personal data, the roadblocks to data protection compliance are multiple. The shortcomings in conveying consent have guided reform proposals that focus on improving the consent seeking mechanisms. While these are not considered to be the panacea, they are put forward as a first step towards shaping a new paradigm for consent in data protection (Arnold, Hillebrand, & Waldburger, 2015): consent models have evolved from display pictograms to artificial intelligence helpers in order to maximise its effectiveness (Jones et al, 2018; Gal, 2018). Concentrated effort has tried to address the technical weaknesses as a means to predict or help shape informed preferences and in order to preserve "the institution of informed consent" (Efroni et al, 2019).

TECHNICAL IMPROVEMENT OF CONSENT

Focusing on information asymmetries created between data subjects and responsible actors, legibility is essential towards shaping the autonomous choice of the individual and thus the validity of the consent. According to article 12(7) GDPR, the information related to the personal data collection and processing can be provided to data subjects "in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically, they shall be machine-readable".[22] Considered as a "highly behaviorally-informed legal innovation" (Ducato & Strowel, 2018), this formulation provides guidance on creating informed and express digital consent mechanisms. Article 7(2) GDPR clarifies that when consent is required, it should be presented in "a manner, which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language". In that regard, the European Data Protection Board's (EDPB) guidelines[23] specify that information has to be presented "efficiently and succinctly, in order to avoid information fatigue". Data controllers can use "contextual pop-up notices, 3D touch or hover-over notices, and privacy dashboards. Non-written electronic means, which may be used in addition to a layered privacy statement/notice might include videos and smartphone or IoT voice alerts".

Among the projects that seek to improve the shortcomings of current digital consent practices, data protection signaling[24] (following the model of Creative Commons pictograms for copyright management clauses[25]), "privacy nudges" (Yin Soh, 2019), and "visceral notices" (Calo, 2013) are projects that focus on the design aspect of consent mechanisms, on the enforcement of the legal framework, or on both (Efroni et al, 2019). These proposals focus on optimising self-deliberation and autonomous choice of individuals through the improvement on the information received in order to decide. Taken a step further, another set of proposals examines how artificial intelligence can help in predicting "what information practices a user would consent to" (Jones et al, 2018) in order to streamline a generation of automated consent. This set of tools is approached as a way out of the dissonance between technology and individual agency which is foundational to the legal concept of consent. The algorithmic decision-making processes (Gal, 2018) are progressively making their way in that realm. In fact, traditional approaches to determining user autonomy of choice are constantly challenged by algorithmic assistants because they tend to further detach user control over data processing based on predetermined choice architectures and design choices.

The evolution of technical proposals to amend consent mechanisms follows the complexities of

the technologies at hand and aims to improve identified shortcomings in the establishment of a valid consent. For example, while privacy pictograms were developed to address readability issues (Hansen, 2009) related to data processing and privacy policies, privacy icons that are currently in the pipelines set higher goals by implementing a risk-based approach.[26] As a matter of fact, technology is used as a tool that will amend power and information asymmetries, with design, signaling, and content choices that facilitate (or even diminish) the decision-making processes for data subjects whose choices are also shaped by the obligations imputed on the responsible actors. However, increasing reliance on technologically-enabled (or technologically-facilitated) consent models demonstrates their shortcomings in the context of algorithmic processing of big data. In fact, the autonomy and user control - inherent in the consent foundation of privacy - start to break down in more complex and non-linear data processing activities such as those involving machine learning algorithms. Thus, compliance becomes challenged.

Finally, the weakening of the theoretical frameworks that have elevated consent as the ultimate tool for individual control is not a new issue. A common criticism of the current consent reliance (Barocas & Nissenbaum, 2014) finds the paradox in the "ultimate inefficacy of consent as a matter of individual choice and the absurdity of believing that notice and consent can fully specify the terms of interaction between data collector and data subject". Similarly, the justifications of the elevated consent requirements are criticised for "frequently fail(ing) to live up to the underlying moral value that justified their creation (…) In these cases, a gap opens up between legally valid consent and morally transformative consent" (Jones et al, 2018). Thus, the social, legal, and ethical underpinnings of consent within the data protection normative framework are challenged.

SECTION 2. THEORIES OF RESTRUCTURED CONSENT

The universal appeal of consent is putting it time and time again at the forefront of lawful personal data collection and processing prerogatives. The reliance on the notice-and-consent approach in the United States shows little signs of fading under the pressure of complex data flows[27] that have largely reshaped the appreciation of consent (Bietti, 2020) and of the distribution of accountability among liable actors (Mahieu, Van Hoboken, & Asghari, 2019). Given the failings of the current design and regulation of consent, there are theoretical constructs that chip away from the "liberty-based" consent in order to make efficient design and accountability choices (Cohen, 2019). Leaving the "macro" view of revising technical consent, academic theory has put under the microscope the inner working of consent in data protection. Contextual theory and paternalism are two examples of this effort.

CONTEXTUAL THEORY

According to contextual theory principles brought forward by Helen Nissenbaum (2009), the way out of the dissonance between consent and big data applications does not lie in the rejection of consent altogether but neither does it lie in resorting to technical consent design solutions. "In good faith, we have crammed into the notice and consent protocol all our moral and political anxieties, believing that this is the way to achieve the level playing field, to promote the autonomy of data subjects" (Barocas & Nissenbaum, 2014). Nissenbaum's work illustrates how the sensitivity of the data use is context-dependent, requiring thus a more granular application of data protection and consent rules. According to the contextual theory, the answer can be found beyond the design of optimal consent practices and towards the "contextualization" of

consent, which should not be viewed as a monolithic standalone concept. Rather, it should be placed in the bigger matrix of rights and obligations. "It is time for the background of rights, obligations, and legitimate expectations to be explored and enriched so that notice and consent can do the work for which it is best suited" (Barocas & Nissenbaum, 2014). This interpretation does not purport to minimise the value of individual autonomy depicted in the concept of consent. Instead, it is exactly because the authors realise the established reliance on consent for a lot of algorithmic personal data processing that they propose an approach, which could ensure its lasting impact. Data protection and informed consent have to be examined according to the purposes and context of the data processing activity as well as placed on the greater societal context of the activity in question. The authors trust that social and contextual ends are served better when consent is neither undervalued because of the apparent incompatibilities with algorithmic processing nor manipulated without reinforcing the individual.

While contextual approaches to data processing have become popular, the theory cannot easily adapt in the current data collection and processing realities that escape contextuality towards omnipotent technological capabilities and structures. The complex data flows make it harder to directly infer the data processing activities in such a way that could facilitate the contextualisation in question. Thus, contextual theory is challenged (Nissenbaum, 2019), if not "obliterated" (Ausloos, 2018) faced with big data and algorithmic processing, because of the lack of meaning in a lot of the data processing happening.[28]

PATERNALISTIC PROTECTION

While the consent mechanisms have been shown to suffer from structural misapplications, they have not yet managed to enable a structural shift due to the importance attached to the freedom of choice and autonomy represented through it. This holds true especially in the notice and consent system applicable in the United States, where any regulation of individual autonomy in privacy risks being tainted as "paternalistic". All approaches that consider the involvement of multiple actors in the data protection process aim to certainly reduce individual autonomy but with the goal of addressing the existing inefficacies in current consent practices. Supported by a growing body of scholarship (Cohen, 2019; Bietti, 2020; Allen, 2011), alternative approaches to privacy are examined; ones that envisage a technology redesign and a centralised oversight that aims to limit the reach of consent as the main data governance solution. However, there is still a negative connotation attached to the notion of paternalism even if it hinges not on consent restriction but on a multi-layered application of privacy regulation among the network of actors depending on the power (im)balances present and the role of human intervention in the processing of data.[29]

The turn towards a structural reform of privacy is motivated by the consent shortcomings - themselves a result of the complex data-intensive information flows that have long replaced the linear data collection practices with clearly articulated responsible actors. "Notice and choice/consent and purpose limitation all assume (for their effectiveness) that the functionality on offer can be stabilized enough to present to the users and that relevant changes to the functionality are rare enough to make a renegotiation of consent feasible" (Gürses & Van Hoboken, 2018). Julie Cohen argues that for privacy regulation to be effective it needs to escape liberal approaches supporting full individual autonomy towards more public scrutiny and transparency requirements (Cohen, 2019).[30] This approach can be effective within the algorithmic processing of data because of the absence of moral underpinnings of consent in the choices presented to individuals. Within this technological context, alternative privacy and consent mechanisms are welcomed through "soft" or more "rigid paternalistic" regulation and

have been implemented[31], for example, in parts of the GDPR too.

SECTION 3. BRIDGING THE GAP BETWEEN CONSENT AND ALGORITHMIC PROCESSING

Considering the complex data flows that make consent fallible in data processing algorithmic systems, we are witnessing how the solutions proposed not only stem from the regulatory field, but they also tend to extend towards common actions or technological design. Thus, they seem to step away from the individual nature of privacy protection in order to support community action within an appropriately balanced accountability network of actors in a technological market that is not driven by data monetisation.

LAWFUL GROUNDS FOR PERSONAL DATA PROCESSING

Observed weaknesses of current consent-based processing in algorithmic decision-making do not necessarily imply a regulatory shortcoming.[32] As a matter of fact, European rules prescribe alternative grounds for personal data processing. The balancing mechanism inherent in the controllers' legitimate interest (Article 6(1)f GDPR) has received considerable attention. Created as an open-ended concept in order to accommodate contextual balancing that does not correspond to a predetermined checklist of accepted "legitimate interests", article 6(1)f appears as a breeding ground for data controllers to pursue their processing without data subjects giving up on any of their rights and *ex post* control mechanisms. It constitutes a cornerstone provision with an explicit balancing act from the controller's side, but it also allows data subjects to check the performance of the balancing within the specific context of their personal data through the exercise of their rights. This construction permits for the subjective criteria to come into play in the individual appreciation of the processing as a legitimate interest of the data controller (A29WP, 2014).

The data controller's legitimate interests have received considerable attention even in the pre-GDPR era with regards to big data. In their premise, Moerel and Prins (2016) advocate for the substitution of the purpose limitation principle - and of all its issues within the big data environment - with that of legitimate interests. The proposal has received criticism in its conflation of legitimate interests and legitimate purposes (Ausloos, 2018; Kamara & de Hert, 2018). While the purpose limitation principle is admittedly challenged in the current algorithmic realities, its function within the checking mechanisms instituted within the GDPR cannot be conflated with that of the controllers' legitimate interests. As a matter of fact, the balancing exercise embedded within the legitimate interests of the controllers incorporates the accountability of the actors in questions, which have to convey their compliance with the article 5 GDPR principles and the overall respect of the fundamental right of privacy. In that sense, the legitimate interests of the controller incorporate the rationales of the GDPR and preserve data protection principles throughout data processing even if they cannot convey the direct relation between data subjects and data controllers that the consent mechanisms do.

BOTTOM-UP DATA GOVERNANCE

Stepping outside of the normative design solutions, a new form of approaching the power of the individual within the data protection management system is created: bottom up approaches emerge as a defense against power imbalance and the shortcomings of individual consent in the algorithmic processing of data. The creation of data cooperatives or data trusts has been progressively receiving a lot of scholarly and policy attention. It departs from the individualistic

approach of the consent mechanism but not towards the set of responsibilities that the accountability structure of the GDPR creates. Its premise is firstly conceptual in that it approaches data as a commons value, collectively governed by communities of people or elected parties acting in the interest of the community. The development of data cooperatives and data trusts[33] is not monolithic; the chosen data governance model is partially defined according to the principles the data collectivity is trying to highlight. There are collective data governance models focusing on monetisation, ownership, negotiating power, or simply enhancing data subject control (Delacroix & Lawrence, 2019). The creation of these cooperatives was motivated by the need to make up for the insufficiencies of the existing system in empowering individuals within the algorithmic data processing space. "To the extent there is value in intermediation, it seems that the value of individualized consent is very limited" (Bietti, 2020). Collective negotiation of data processing rules aimed at sector-specific data processing in order to convey a community model of consent is an alternative that aims to find a balance between individual autonomy and societal public interest. In sum, the creation of cooperative leveraging of grouped individual empowerment is aligned with the expression of privacy as a societal common good.

The process of decentralising data governance decision-making and empowering data subjects has also coincided with some technological solutions developed over decentralised ledgers (i.e., blockchains). The concept of a self-sovereign identity has gained in popularity (Wang & de Filippi, 2020), founded on fluid ideological premises that relate to maximisation of individual liberty and self-determination (Allen, 2016). Self-sovereign identity solutions transcribe the goal of autonomy and individual control through decentralisation and "user-centric design" over the usage, storage and transfer of one's digital data. Multiple projects currently in development promise to deliver a technological solution that embodies the individual autonomy over one's data. They are solutions that aim to achieve a redesign of how authorisations in data flows currently operate, and they aim to preserve the consent mechanism in full. Whether the existing - under development - self-sovereign identity solutions will actually manage to achieve it or not, is outside of the scope of the current paper.

RETHINKING DESIGN CHOICES

The post-GDPR era has illustrated how data protection rules remain constantly challenged with the economic model of an ever-developing 'data society' based on the algorithmic processing of (personal) data. In a process described as "turning privacy inside out", Cohen suggests that we should abandon theories organised around the presumptive autonomy of selves[34] and focus instead on the conditions necessary to produce sufficiently private and privacy-valuing subjects" (Cohen, 2020). She emphasises that while accountability mechanisms are essential and well placed, they have to move "beyond individualized choice and consent to emphasize responsibility, respect, and new modalities for effective regulatory oversight of algorithmic and data driven processes". It soon becomes apparent that a legal redesign is not enough to overcome the shortcomings of the autonomy-based existing data protection model. Rather, more focus should be placed on the level at which privacy design decisions are truly taken and that is at an infrastructural level currently not taken into consideration within the accountability structure of the GDPR nor within the consent design choices.

From the convoluted and dynamic models of privacy theories emerge proposals for rendering current technology development within an overarching privacy principle. Thus, the design of the technology has to become more "privacy-centric"; a type of design that does not aim for optimal user-experience and efficiency but in what is referred to as "desirable inefficiency" (Ohm & Frankle, 2018) or "seamful design" (Vertesi, 2014). The importance of technological design and accountability in data protection has been made apparent time and time again. As we have

previously explained, regulatory evolution of consent aimed at accommodating the moral concept of the expression of individual autonomy. Edenberg and Leta Jones explain that, "consent is not an exchange but a transformation of the relationship based on the autonomous willingness of one party to allow the act of the other party". (Edenberg & Leta Jones, 2019). Designing for privacy-centric systems requires to not only depart from the logic of preserving the individual autonomy against its purported disruptions but also to bring the accountability model on the level where the privacy design actually happens. As stressed by Bietti (2020) "there are good reasons to depart from the centrality of individualized notice and consent" when the power inequalities demand a regulatory intervention that should not be immediately dismissed as "paternalistic". While attention has been given to the technological design in the current European regulatory framework, the existing obligations do not convey the aforementioned logic. As a matter of fact, the data protection by design obligation responds to the accountability mechanism created by the GDPR but without including the contextual obligations that have to be created on diverse levels of technological creation. Furthermore, the shape of the obligation maintains the individual autonomy approach of the GDPR towards finding pathways that empower the individual in enforcing their rights by imposing measures on a group of responsible actors.

Reimagining design for privacy is a noble goal that has to balance the individual with market players. Considering the benefits and the inefficiencies of the existing systems and seeing that a balance between individual autonomy and accountability can be found, it is not truism to envisage a solution that radically transforms technological design without being "paternalistic". While regulatory interventions such as those of the GDPR do involve a level of intervention on the design level, they tend to put more focus on the regulation of processing of data rather than that of collection of data. The GDPR focuses more on lawful processing than on the limitation of collection and limits its reasoning to determining further the robustness of a given consent.[35] The enhancement of negotiating power of individuals through the generation of alternative mechanisms on the legal, technical, or governance level can reveal alternative relief to dissolve the tension created between consent and algorithmic processing of data.

CONCLUSION

Current applications of consent in the algorithmic processing technological reality escape the confines of individual autonomy and empowerment within a modern society. In this article, we have shown the progression of different solutions to this disconnect between consent and algorithmic data processing. The observed shortcomings and arguments brought forward within the context of different legal systems frame the role of consent as a *pro forma* requirement in data protection. The article illustrates that while the criticism on consent mechanisms persists - especially in algorithmic processing of data, current proposals are looking for a way out of the existing dilemma between the modalities of individual or institutional control. Efficient data protection in the context of an algorithmically driven society cannot rely on an absolute dual approach. The legitimising role of consent in data processing is only as valid as the design surrounding it and the accountability measures reinforcing it.

Despite the development of various consent mechanisms so that they match the technological leaps of a data driven society, it is truism to repeat how reliance on consent - with its fallacies and fragmented application - results in devaluing the substantiality of the legal and ethical underpinnings of the concept. We have traced the efforts in creating a more efficient consent system based on reforms on the normative, governance, or overall design level. Bridging the gap

between the consent inconsistencies could require out-of-the-(tool)box solutions; ones that provide a techno-legal mechanism of empowerment. Thus, pressure can be added to the current technological status quo both on the level of architectural market constraints and on the collective administration of personal data through governance and technological choices.

REFERENCES

Arnold, R., Hillebrand, A., & Waldburger, M. (2015). Informed Consent in Theorie und Praxis: Warum Lesen, Verstehen und Handeln auseinanderfallen [Informed consent in theory and practice: why reading, understanding, and action diverge]. *Datenschutz und Datensicherheit*, *39*(11), 730–734. https://doi.org/10.1007/s11623-015-0509-2

Article 29 Data Protection Working Party. (2011). *Opinion 15/2011 on the definition of consent, 01197/11/EN WP 187.*

Article 29 Data Protection Working Party. (2014). *Opinion /2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC, WP 217.*

Article 29 Data Protection Working Party. (2018). *Guidelines on consent under Regulation 2016/679, 17/EN WP259 rev.01.*

Allen, A. (2011). *Unpopular privacy. What must we hide?* Oxford University Press. https://doi.org/10.1093/acprof:oso/9780195141375.001.0001

Allen, C. (2016, April 25), The Path to Self Sovereign Identity, http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Ausloos, J. (2018). *The Right to Erasure: Safeguard for Informational Self-Determination in a Digital Society*? [PhD Thesis, KU Leuven]. https://lirias.kuleuven.be/retrieve/517438

Barocas, S., & Nissenbaum, H. (2014). Big Data's End Run around Anonymity and Consent. In J. I. Lane, V. Stuodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, big data, and the public good: Frameworks for engagement* (pp. 44–75). Cambridge University Press.

Bernal, P. (2014), *Internet Privacy Rights: Rights to Protect Autonomy*, Cambridge University Press.

Bietti E. (2020). Consent as a free pass: platform power and the limits of the informational turn. *Pace Law Review*, *40*(1), 310–398. https://digitalcommons.pace.edu/plr/vol40/iss1/7

Calo, R. (2013). Against Notice Skepticism in Privacy (and Elsewhere). *Notre Dame Law Review*, *87*(3), 1027–1072. http://ndlawreview.org/wp-content/uploads/2013/06/Calo.pdf

Cohen, J. (2013). What Privacy Is For. *Harvard Law Review*, *126*(7), 1904-1933. https://harvardlawreview.org/2013/05/what-privacy-is-for/

Cohen, J. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press. https://doi.org/10.1093/oso/9780190246693.001.0001

Cohen, J. (2020). Turning Privacy Inside Out, *Theoretical Inquiries in Law*, *20*(1), 1–32. https://doi.org/10.1515/til-2019-0002

Delacroix, S., & Lawrence, N.D.(2019), Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance, *International Data Privacy Law*, *9*(4), 236–252. https://doi.org/10.1093/idpl/ipz014

Ducato, R., & Strowel, A. (2018). *Limitations to Text and Data Mining and Consumer Empowerment: Making the Case for a Right to "Machine Legibility"* [Working Paper No.

1/2018]. Centre de recherche Interdisciplinaire Droit, Entreprise et Société.

Edenberg, E., & Leta Jones, M. (2019). Analyzing the legal roots and moral core of digital consent. *New Media and Society*, *2*(8), 1804–1823. https://doi.org/10.1177/1461444819831321

Edwards, L., & Veale, M. (2018), Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'? *IEEE Security & Privacy*, *16*(3), 46–54. https://doi.org/10.1109/MSP.2018.2701152

Efroni, Z., Metzger, J., Mischau, L., & Schirmbeck M. (2019), Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing, *European Data Protection Law Review*, *5*(3), 352–366. https://doi.rog/10.21552/edpl/2019/3/9

Gal, M. S. (2018). Algorithmic Challenges to Autonomous Choice, *Michigan Telecommunications and Technology Law Review*, *25*(1), 59–104. https://repository.law.umich.edu/mtlr/vol25/iss1/3/

Gürses, S., & Van Hoboken, J. (2018). Privacy after the Agile Turn. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), *Cambridge Handbook of Consumer Privacy* (pp. 579–601), Cambridge University Press.

Hansen, M. (2009). Putting Privacy Pictograms into Practice - a European Perspective. *GI Jahrestagung*.

Hartzog, W. (2018). The case against idealizing control. *European Data Protection Review*, *4*(4), 423–432. https://doi.org/10.21552/edpl/2018/4/5

Hoofnagle, C. (2018). Designing for consent, *Journal of European Consumer and Market Law*, *7*(2), 162–171.

Hull, G. (2015). Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data, *Ethics and Information Technology*, 17(2), 89–101. https://doi.org/10.1007/s10676-015-9363-z

Jones, M.L., Edenberg, E., & Kaufman, E. (2018). AI and the Ethics of Automating Consent. *IEEE Security & Privacy*, *16*(3), 64–72. https://doi.org/10.1109/msp.2018.2701155

Kamara I., & de Hert P. (2018). *Understanding the balancing act behind the legitimate interst of the controller ground: A pragmatic approach* [Working Paper No. 12]. Brussels Privacy Hub. https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf

Kamarinou, D., Millard C., & Singh J. (2016). *Machine learning with personal data* [Research Paper No. 247/2016]. Queen Mary School of Law Legal Studies Research Paper No 247/2016. https://ssrn.com/abstract=2865811

Koops, B.-J., & Leenes, R. (2005). 'Code' and the Slow Erosion of Privacy. *Michigan Telecommunications and Technology Law Review*, *12*(1), 115–188. https://repository.law.umich.edu/mttlr/vol12/iss1/3/

Koops, B.-J. (2014). The Trouble with European Data Protection Law, *International Data Privacy Law*, *4*(4), 250–261.

Kosta, E. (2013). *Consent in European Data Protection Law*. Nijhoff Publishers.

Kosta, E., & Cuijpers, C. (2014). The Draft Data Protection Regulation and the Development of Data Processing Applications. In M. Hansen, J.-H. Hoepman, R. Leenes. & D. Whitehouse. (Eds) *Privacy and Identity Management for Emerging Services and Technologies. Privacy and Identity 2013. IFIP Advances in Information and Communication Technology* (pp. 12–32). Springer. https://doi.org/10.1007/978-3-642-55137-6_2

Mahieu, R., Van Hoboken, J., & Asghari, H. (2019). Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, *10*(1), 85–105. https://doi.org/10.2139/ssrn.3256743 https://hdl.handle.net/11245.1/5c40ae82-dedb-4550-8412-44428653031a

Mayer- Schönberger, V., & Cukier, K. (2013). *Big Data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

Mayer-Schönberger, V., & Padova, Y. (2016). Regime Change? Enabling Big Data through Europe's New Data Protection Regulation, *Columbia Science & Technology Law Review*, *17*(2), 315–335. https://journals.library.columbia.edu/index.php/stlr/article/view/4007

Moerel, L., & Prins, C. (2016). *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things*. https://doi.org/10.2139/ssrn.2784123.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Nissenbaum, H. (2019), Contextual Integrity Up and Down the Data Food Chain. *Theoretical Inquiries in Law*, 20(1), 221–256. https://doi.org/10.1515/til-2019-0008

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence*. arXiv. https://arxiv.org/abs/2001.02479v1

Ohm, P. & Frankle, J., (2018). Desirable inefficiency. *Florida Law Review*, *70*(4), 777-838. http://www.floridalawreview.com/2019/desirable-inefficiency/

Oostveen, M. (2018). *Protecting individuals against the negative impact of big data: Potential and limitations of the privacy and data protection law approach*. Wolters Kluwer.

Perlis, A. (1967). The Synthesis of Algorithmic Systems. *Journal of the ACM*, *14*(1), 1-9, https://doi.org/10.1145/321371.321372

Purtova, N. (2018) The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40–81. 10.1080/17579961.2018.1452176

Reidenberg, J .R., Breaux, T., Cranor, L. F., & French, B. M. (2015). Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding, *Berkeley Technology Law Journal*, *30*(1), 39–88. https://btlj.org/2015/10/disagreeable-privacy-policies/

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. https://doi.org/10.1007/s10676-014-9343-8

Simmons J. A. (2010). Political obligation and consent. In F. Miller & A. Wertheimer (Eds.), *The Ethics of Consent: Theory and Practice* (pp. 305–306). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780195335149.003.0012

Solove, D. (2013). Privacy Self-Management and the Consent Dilemma, *Harvard Law Review*, *126*(7), 1880–1903. https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/

Tene, O., & Polonetsky, J. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property*, *11*(5), 258–273. https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1

Vaidhyanathan, S. (2011). *The Googlization of Everything: (And Why We Should Worry)*. University of California Press.

Van Hoboken, J. (2019). *The privacy disconnect*. In R.F. Jørgensen (Ed.), *Human Rights in the Age of Platforms* (pp. 255–284). The MIT Press. https://doi.org/10.7551/mitpress/11304.003.0017

Vertesi, J. (2014). Seamful Spaces: Heterogeneous Infrastructures in Interaction, *Science, Technology, & Human Values*, *39*(2), 264–284. https://doi.org/10.1177/0162243913516012

Wang, F., & De Filippi, P. (2020). Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion Frontiers in Blockchain. *Frontiers in Blockchain*, *2*. https://doi.org/10.3389/fbloc.2019.00028

Westin, A. (1967). *Privacy and Freedom*. Atheneum.

Yin Soh, S. (2019). Privacy Nudges: An Alternative Regulatory Mechanism to 'Informed Consent' for Online Data Protection Behaviour. *European Data Protection Law Review*, *5*(1), 65–74, https://doi.org/10.21552/edpl/2019/1/10

Zuiderveen Borgesius, F. J. (2014). *Improving privacy protection in the area of behavioural targeting* [PhD Thesis, University of Amsterdam]. https://hdl.handle.net/11245/1.434236

FOOTNOTES

1. It is worth noting that the term “algorithmic systems” was first employed by Alan Perlis in 1967 in his speech entitled “The Synthesis of Algorithmic Systems”.

2. The sales of voice assistants like Amazon’s Alexa and Google’s Home are rising globally, with already millions of devices installed in European homes.

3. The argument of lack of control in this context is used to illustrate the power asymmetries between individual and private companies. The lack of control involving the relationship between state surveillance and citizens is left outside of the scope of the current contribution.

4. See for example, the case law involving Max Schrems and Facebook: Maximillian Schrems v Data Protection Commissioner (2015) Court of Justice of the European Union C-362/14. The revelation of the involvement of the data analytics company Cambridge Analytica and Facebook

in psychologically manipulating users by algorithmic processing of their personal data brought significant attention to the impact of framing the consent requirement as a legal ground for personal data processing.

5. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, updated in 2013.

6. 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. Hereinafter Directive 95/46/EC.

7. See also for example European Commission (2018), It's Your Data—Take Control. May 4. https://ec.europa.eu/info/sites/info/files/data-protection-overview-citizens_en_0.pdf

8. According to the European Data Protection Regulation (GDPR), which entered into force on 25 May 2018 replacing Directive 95/46/EC, "natural persons should have control of their own personal data".

9. Control is thus both freedom to make informed choices about the exercise of data protection within current regulatory frameworks and the assurance that safeguards will ensure the preservation of this autonomy against actors that could limit it.

10. According to Bernal (2014), autonomy refers to individuals' ability to make free and meaningful choices.

11. In the age of big data, the US model has been qualified as a "successful failure" because of the continuous degradation of consent-obtaining mechanisms by big platforms (Hull, 2015). In the current context of sensory overload of data, current consent reliance is criticised for placing an excessive burden on the individual without leading to true individual empowerment (Solove, 2013).

12. In that sense, control remains among the guiding principles of the Regulation but in its positive and negative form: positive, as an expression of individual autonomy and negative, as a protection against the consequences of the subversion of that autonomy.

13. Similar formulation exists in the GDPR: According to article 4(11) of the GDPR, "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

14. For example, according to Recital 32, "consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided". Similarly, per the validity of consent see

recitals 33, 38, 42, 43 etc.

15. Council of Europe (2018), Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, para 42.

16. Council of Europe (2018), Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (CM/Inf(2018)15-final)

17. For example, purpose specification can be found both as a principle in the Fair Information Principles applicable in the USA and as an obligation for data controllers in the GDPR.

18. Technology can have an "eroding effect" on privacy. According to Bert-Jaap Koops and Ronald Leenes, "there is no precise stage at which one can stab a finger at technology to accuse it of unreasonably tilting the balance of privacy. Exactly because of the flexible, fluid nature of privacy, society gradually adapts to new technologies and the privacy expectations that go with them" (Koops & Leenes, 2005).

19. This is certainly not a new affirmation, as for years, scholars point out how problematic it is to achieve valid consent (Mayer-Schönberger & Padova, 2016).The growing disconnection from the original legal underpinnings surrounding consent in data protection is described by Bert-Jaap Koops as the 'mythology of consent' (Koops, 2014).

20. We refer to the otherwise called "transparency paradox" describing the conundrum of either providing detailed explanations which may not be understood (even read) or simplified ones that will gloss over important details.

21. European Court cases have highlighted that consent should be informed and a positive separate action. See for example: Court of Justice of the European Union, Case C-673/17 Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. ECLI:EU:C:2019:801. (2019). Design practices in seeking consent have been under scrutiny for failing to comply with the established normative framework (Nouwens et al 2020).

22. See also Recitals 58 and 60 of the GDPR: "The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising".

23. EDPB, Guidelines on Transparency under Regulation 2016/679.

24. An interesting methodology to answer the challenges of GDPR's icons has been developed within the research project run by the Cirsfid group at the University of Bologna: http://gdprbydesign.cirsfid.unibo.it/(Ducato and Strowel, 2018)The development of risk-based privacy signaling is the focus of the "Daten als Zahlungsmittel" research group at the Weizenbaum Institut in Berlin. (Efroni et al., 2019).

25. The legal notion of consent in the digital age has been subject to adaptations in order to accommodate the demands of a digital informed consent (concerning data protection or

contracts). For example, the Creative Commons licenses have developed pictograms, "human readable licenses" and "legal deeds" demonstrating the dissonance in expressing informed consent on contractual copyright management.

26. Admittedly none of the projects has achieved widespread recognition nor success that would lead to transnational standardisation such as the one that Creative Commons achieved. These efforts cannot be treated as a universal *passepartout* for improving digital consent.

27. Helen Nissenbaum uses the term data primitives to underline the multi-layered data collection processes designed within our technological realities : "Before we have text, a photo, a place, a shoe order, or a social network, we have mouse clicks registered as digital (electric) pulses, environmental phenomena (temperature, airborne chemicals, etc.) and biological features rendered as sensor signals, as mathematical templates, and metrics, flowing via digital networks to software platforms. We have electrical signals passing from transmitters to transceivers, activated pixels producing digital images, and geospatial coordinates communicated from satellite to GPS-enabled devices. These event imprints, the base-layer of the informational universe, are what I am calling, data primitives." (Nissenbaum 2019).

28. As the author of the theory admits, "choosing is not mere picking but requires that the subject understand that to which he or she is consenting, which is lacking in our interactions with data primitives, defined so precisely because they are absent of meaning" (Nissenbaum, 2019).

29. However, the empowerment of privacy choices through more rigid regulation could be considered too paternalistic according to parts of academic scholarship: "Regulation that sidesteps consent denies people the freedom to make choices," Daniel Solove argues (Solove, 2013). This holds true for specific legal privacy rationales tending to rely more on a pure cost-benefit analysis.

30. In the same spirit, Siva Vaidhyanathan also criticizes the illusion of freedom of choice on consent in favour of a more paternalistic approach. "We are conditioned to believe that having more choices–empty though they may be–is the very essence of human freedom. But meaningful freedom implies real control over the conditions of one's life." (Vaidhyanathan 2011).

31. Lowering the threshold of consent requirements can be part of a "fair use" application of personal data processing according to some scholars (Schermer et al, 2014). However, relying solely on the limitation of the impact of consent and consequently on the limitation of individual autonomy and user control without the appropriate regulatory safeguards is a flagrant shortcoming for individuals' privacy.

32. For example, the relationship of the principles of data minimization and of purpose limitation with big data business models can be seen as "antithetical" (Tene & Polonetsky, 2013).

33. The proposal for the creation of data trusts exists for quite some time in not exclusively bottom-up approaches. Despite its admittedly multiple merits, it leaves the civil law system quite perplexed because of the lack of a specific legal fiction or instrument equivalent to that of the common law trust mechanism. The concept of "community-based data sharing agreements" is used more broadly, in order to escape the legal implications that the trust carries in common law.

34. According to Cohen's previous work, "privacy is shorthand for breathing room to engage in the processes of boundary management that enable and constitute self-development" (2019).

35. As Cohen points out, "there is an intractable tension between the regulatory goal of specific, explicit consent to data collection and processing and the marketplace drift toward convenience. Formally, European data protection law imposes a strict definition of consent and forbids processing personal data in ways incompatible with the purpose for which the data was initially collected. Renewed consent can justify later processing for a new, incompatible purpose, but rolling consent is not supposed to become a mechanism for evading purpose limitations entirely" (2020, p. 263).