TU Delft

Delft University of Technology

Document Version
Final published version

Licence
CC BY

Citation (APA)
Kempeneers, A. R., & Simonse, L. W. L. (in press). Relational consent: Redesigning the solution space for consent and disclosure. *Information Society*, *42*(5), 247-263. https://doi.org/10.1080/01972243.2026.2713455

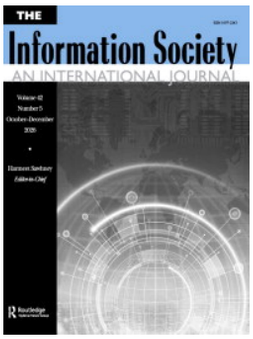
Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
In case the licence states “Dutch Copyright Act (Article 25fa)”, this publication was made available Green Open Access via the TU Delft Institutional Repository pursuant to Dutch Copyright Act (Article 25fa, the Taverne amendment). This provision does not affect copyright ownership.
Unless copyright is transferred by contract or statute, it remains with the copyright holder.

Sharing and reuse
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.



Routledge
Taylor & Francis Group

The Information Society
An International Journal

ISSN: 0197-2243 (Print) 1087-6537 (Online) Journal homepage: www.tandfonline.com/journals/utis20

Relational consent: Redesigning the solution space for consent and disclosure

Aniek R. Kempeneers & Lianne W. L. Simonse

To cite this article: Aniek R. Kempeneers & Lianne W. L. Simonse (2026) Relational consent: Redesigning the solution space for consent and disclosure, The Information Society, 42:5, 247-263, DOI: 10.1080/01972243.2026.2713455

To link to this article: https://doi.org/10.1080/01972243.2026.2713455

© 2026 The Author(s). Published with license by Taylor & Francis Group, LLC.

Published online: 27 Aug 2026.

Submit your article to this journal

Article views: 242

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=utis20

THE INFORMATION SOCIETY
2026, VOL. 42, NO. 5, 247–263
https://doi.org/10.1080/01972243.2026.2713455

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Relational consent: Redesigning the solution space for consent and disclosure

Aniek R. Kempeneers[a,b] and Lianne W. L. Simonse[a]

[a]Faculty of Industrial Design Engineering, Delft University of Technology, Delft, The Netherlands; [b]DCODE Network, Delft, The Netherlands

ABSTRACT

One of the grand challenges of the digital society is safeguarding data disclosure. Despite protective regulations, most end-users are unable to manage their individual consent properly due to the overwhelming complexity of disclosure interactions. Design research could help resolve these issues, but doing so requires a shift from siloed research perspectives and detailed recommendations on the design of consent notices toward consent models and relational design. In this article we deconstruct the solution space of consent and disclosure interactions by conducting a critical review on the literature at the intersection of ethics and society, policy management and legislation, and design and computer sciences. We synthesize existing models of consent (i.e., moral consent, protective consent, and human-centered consent) and deconstruct two critical barriers (i.e., regulatory noncompliance and consent malpractices) that need to be resolved to successfully redesign current consent practices and disclosure interactions. For undertaking new efforts of redesigning consent, we formulate a novel approach we term relational consent, along with accompanying design principles and guidance on how to redesign consent practices and disclosure interactions.

ARTICLE HISTORY
Received 25 May 2023
Accepted 30 July 2026

KEYWORDS
Consent; data disclosure; design principles; GDPR; informed consent; moral consent; relational consent; relational design

Introduction

Safeguarding data disclosure between end-users and organizations is one of the grand challenges in the digital society. Since end-users now serve as the main sources of data due to their user-generated content and digital interaction, platforms have become independent entities of data collection and analysis (Alaimo, Kallinikos, and Valderrama-Venegas 2020; Alaimo and Kallinikos 2017). However, the effectiveness of existing consent practices in protecting end-users' privacy (Mai 2016) and control over their personal data (Edenberg and Jones 2019) has been increasingly questioned. Contemporary regulations even appear to be counterproductive—end-users subjected to a constant stream of consent notices start accepting them blindly, which undermines their general goal of providing privacy protection (REFIT Platform Opinion 2016; Trevisan et al. 2019). While consent models were originally invented to enable end-users to practice their digital rights and manage their data disclosure. Current practices of consent and disclosure interactions leaves much to be desired. Most require end-users to possess highly complex technical and social skills to be able to consider their individual context and collective short- and long-term consequences of their data disclosure decisions. Furthermore, they require in-depth knowledge to comprehend the visual and textual elements present in the disclosure interaction (Human and Cech 2021). Consequently, end-users are "unlikely to understand the complexities of layered applications and their correlated, opaque data flows" (Richards and Hartzog 2019, 1482).

This has raised major concerns among scholars and practitioners regarding how failures in consent management impact society. Concerns include, on the one hand, increased data mining of people's everyday lives by organizations (Kallinikos and Constantiou 2015); and on the other hand, users' lack of knowledge and conceptual understanding of consent practices and disclosure interactions (Jones 2019). Consequently, scholars have called for new concepts of consent across all stages of end-user engagement as well as the specification of clear requirements for obtaining consent in each of these stages (Solove 2012; Utz et al. 2019).

CONTACT Lianne W. L. Simonse L.W.L.Simonse@tudelft.nl Department of Design, Organization, and Strategy, Faculty of Industrial Design Engineering, Delft University of Technology, Landbergstraat 15 Building 32 B-4-150, 2628 CE Delft, The Netherlands.

© 2026 The Author(s). Published with license by Taylor & Francis Group, LLC.
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

Design research into privacy control, consent practices, and requirements focuses on the resolution of regulatory issues regarding consent practices and disclosure interactions (Constantinides, Henfridsson, and Parker 2018). However, there is currently a lack of both a systematic overview and synthesis of the state of knowledge as well as an underlying conceptual understanding of consent practices and disclosure interactions. Therefore, in this article we investigate how different streams of literature—ethics and society, legislation and policy implementation, and design and computer science—have studied digital consent and then synthesize design recommendations on how digital consent can be improved. In addition, we uncover the critical barriers to its redesign and formulate a novel approach we term *Relational Consent*, along with accompanying design principles and guidance on how to redesign consent practices and disclosure interactions.

Our central research question is: How can we redesign consent and shift from siloed research perspectives and detailed recommendations on the design of consent notices toward new consent models? Our sub-questions are: (1) What models and recommendations have been suggested for the redesign of consent practices and disclosure interactions in the digital society? (2) Which critical barriers need to be resolved to successfully redesign current consent practices and disclosure interactions? To address these questions, we unpack the solution space for digital consent design and map the issues with current practices and interactions.

In the next section we provide a background to models of consent, including the definition and application in different fields. We follow this with a description of how contemporary consent practices are governed by European law and what types of data disclosure interactions are common practice. Subsequently, we offer recommendations on form and substance could be synthesized. We then deconstruct the issues raised by current consent practices and disclosure interactions, and identify two critical barriers that hinder efforts to redesign consent interactions. In the final section we discuss a novel approach, *Relational Consent* for overcoming the critical barriers and broadening the design space of future consent practices and disclosure interactions.

Models of consent

Consent is defined by the Cambridge Dictionary as: "To agree to do something, or to allow someone to do something" (Cambridge Dictionary n.d.a, Cambridge Dictionary n.d.b). The concept of consent is important in many fields including law, politics, healthcare, organizations, sociology, computer science, and those at their intersections. In the following section, we summarize three prevalent views on the concept of consent: society and ethics perspective, law and governance perspective, and design and application perspective.

Moral consent: Society and ethics perspective

Over the past decades, several conceptualizations of consent have been introduced and advocated, especially for ethical data management in, for instance, the medical (research) field: Presumed Consent (Bak et al. 2018; Fabre 2014; Karlsen, Solbakk, and Holm 2011), Informed Consent (Faden and Beauchamp 1986; Karlsen, Solbakk, and Holm 2011), Broad Consent (Bak et al. 2018; Hansson et al. 2026; Karlsen, Solbakk, and Holm 2011) and Open Consent (Karlsen, Solbakk, and Holm 2011; Lunshof et al. 2008). A selection is presented in Table 1.

Table 1. Different consent types.

Type	Description
Presumed (Bak et al. 2018; Fabre 2014; Karlsen, Solbakk, and Holm 2011)	A legal framework in which people must register to opt out, otherwise consent is presumed. Creates high participation rates and is less costly. Values utility and focuses on science and society
Streamlined (Bak et al. 2018; Faden, Beauchamp, and Kass 2014; Goldstein et al. 2018)	People are briefly and intuitively informed during conversation, but not asked for written consent. Provides maximum participation and is therefore the least costly approach
Tiered (Bak et al. 2018)	People choose from a list of purposes for which consent is provided. Promotes autonomy
Broad (Bak et al. 2018; Hansson et al. 2026; Karlsen, Solbakk, and Holm 2011)	Consent graduated on a scale ranging from strictly specified to blanket consent. It is generally provided for multiple purposes, all contributing to an overarching topic. Values confidentiality as technically manageable forms of risk, utility, and public trust
Blanket/future (Bak et al. 2018; Hansson et al. 2026)	Consent provided to something without limitations. Consent is for yet unspecified purposes
Open (Karlsen, Solbakk, and Holm 2011; Lunshof et al. 2008)	Consent provided to unrestricted redisclosure of personal data such as the unrestricted disclosure of information that emerges from future research/processing of data. No promises regarding anonymity, privacy or confidentiality can be made. Values veracity, which is argued to precede autonomy, and confidentiality as technically manageable forms of risk and utility
Informed (Faden and Beauchamp 1986; Karlsen, Solbakk, and Holm 2011)	People give permission to another party to do something after this other party has provided them with all the information about the potential effects and results. Values autonomy, right to confidentiality and individual trust

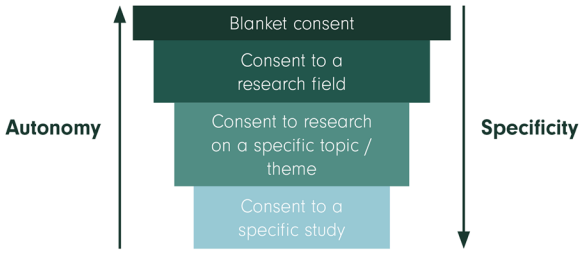


Figure 1. Consent types mapping on the continuums of autonomy and specificity. Adopted from Hansson et al. (2026).

Consent types are often delineated by their mapping on different dimensions: active vs. passive, expressed/explicit vs. implicit/implied, broad vs. specific, and collective vs. individual (Hansson et al. 2026). Figure 1 displays a model of consent along the two dimensions of autonomy and specificity.

The commonly practiced *Informed Consent* is defined as "agreement or permission to do something from someone who has been given full information about the possible effects or results" (Cambridge English Dictionary, n.d.). This specific concept can be interpreted from a moral perspective and is frequently used in patient-physician relations (Faden and Beauchamp 1986). It values autonomy, right to confidentiality, and individual trust (Karlsen, Solbakk, and Holm 2011). Its focus is on the individual. At its core, the moral values of informed consent are clear. Its ethical purpose, to enable end-users to practice their digital rights and manage their data disclosure, is clear (Edenberg and Jones 2019). Yet, today's consent practices are diluted by digital platform organizations (Alaimo, Kallinikos, and Valderrama-Venegas 2020; Kallinikos and Constantiou 2015).

Protective consent: Law and governance perspective

As far back as in the sixteenth century, the concept of consent was discussed by John Locke in his political theory. It distinguishes tacit consent from expressed consent (e.g. oath or written compact) and, how consent of the governed is a necessary condition for political legitimacy. Through *Tacit Consent*, the governed agree to obey the government simply by their presence in a specific territory (Dunn 1967; Tuckness 2020). Similarly, tacit consent has been inferred from users continued online presence rather than their explicit, informed agreement. This practice of an assumed yes, but unspoken, inferred agreement through the mere act of clicking around or staying logged has collapsed the boundary between an individual's private sphere and corporate control: Users can't meaningfully "opt-in" through tacit consent and therefore it should not count as consent (Nissenbaum 1999). To protect users from the underlying power asymmetry, the inherently exploitative data-harvesting and algorithmic governance (Gillespie 2018), and the illusion of agency of tacit consent in the absence of a meaningful choice (Boyd 2012), the GDPR has been created to regulate processing of individuals' personal data. Consent from an end-user in the digital sphere is defined as: "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"

(European Parliament and Council of the European Union 2018. Regulation (GDPR)—EU 2016/679, L119/34). The definition specifies several conditions for consent: it must be freely given, specific, informed, and unambiguous. Furthermore, the GDPR states that consent in the online environment is ruled invalid if any of these conditions are not met. Within the context of the digital society, these conditions have the following meaning. *Freely given* means the withdrawal or refusal of consent at any time without consequence. Correspondingly, the action of withdrawal should be just as easy as that of providing consent and the organizations must inform their customers of their right to do so. Specific and informed means that the organization's consent requests must include the identity of all involved organizations that rely on the consent, purpose of data processing, how activities are processed, and the notification of the right to withdraw. *Unambiguous* means the presence of proof of provided consent and a clear statement of the purposes for which consent is provided. An organization active in the digital society must be able to demonstrate that its customer has provided consent to personal data processing. If consent is requested in written form, it must be distinguishable from other terms and conditions presented in the declaration. Lastly, the consent request must be easily accessible and must use clear and plain language; for instance, it should employ oral or written statements such as check boxes. Silence, preticked boxes such as cookie walls or inactivity do not constitute consent (Information Commissioner's Office 2021b).

In comparison to Locke's consent theory, GDPR's data-protection regime places individual autonomy and voluntary agreement at the center of legitimate authority. It requires expressed consent as a "clear affirmative act" to signify consent and revocability, individuals have the right to withdraw consent at any time.

At the same time, consent in current practices has become a condition for organizational legitimacy. Compliant organizations benefit from greater customer trust (Publications Office and European Parliament 2020). However, simply being present in digital territory does not constitute consent in the online environment, as explained by the GDPR's definition and conditions for consent. The ePrivacy Directive supplements the GDPR in its conditions of consent by requiring organizations to request informed consent specifically for storage and access to information stored on customers' equipment (European Parliament and Council of the European Union 2009). In other words, organizations must request consent for data sent through cookies and other trackingmechanisms. The directive states in detail for which types of cookies consent (opt-in) must be obtained. Then the ePrivacy Regulation, an updated legal framework that supplements the GDPR and ePrivacy Directive, introduces simpler rules on cookies. It elaborates on consent practices by proposing consent management *via* browser settings and clarifies the regulation of the use of legitimate interest. However, such detailed regulations appear to be counterproductive, leading to even more detailed consent notices, which overwhelm the end-users, who then accept them blindly (Trevisan et al. 2019).

Human-centered consent: Design and application perspective

In the late nineties and early 2000s, Friedman proposed a model for informed consent on web-based applications (Friedman et al. 2000; Friedman, Kahn, et al. 2002). The original model consists of five components: *Disclosure*, *Comprehension*, *Voluntariness*, *Competence,* and *Agreement*. These components can be interpreted as conditions for informed consent in the digital society. A revision of the model includes the component of *Minimal Distraction* as an additional condition (Friedman, Kahn, and Borning 2013). The model was implemented in the Mozilla browser to test its application (Friedman, Howe, et al. 2002). The relation and definitions of the model's components are displayed in Figure 2.

In an article published almost two decades later, Human and Cech (2021) propose that consent should be conceptualized as a socio-cognitive action that includes cognitive, collective, and contextual dimensions. They argue that these three dimensions should be considered in the design and implementation of consent practices in the digital society. The cognitive dimension considers the complexity of current consent practices, which require end-users to have technical and social abilities to carefully deliberate on these issues with limited time, expertise, knowledge, and resources. The collective dimension considers the potential social impact of social data extracted from personal data (e.g., group photos) and individual privacy decisions. This also involves the end-users support from peers and experts throughout the consent practice and with personal data management due to the lack of expertise and/or end user ability, and the social consequences of privacy. The contextual dimension considers the need for control of end-users' needs and values within lived conditions and circumstances of consent practices. Despite the conceptual contribution of these dimensions to the solutions space,

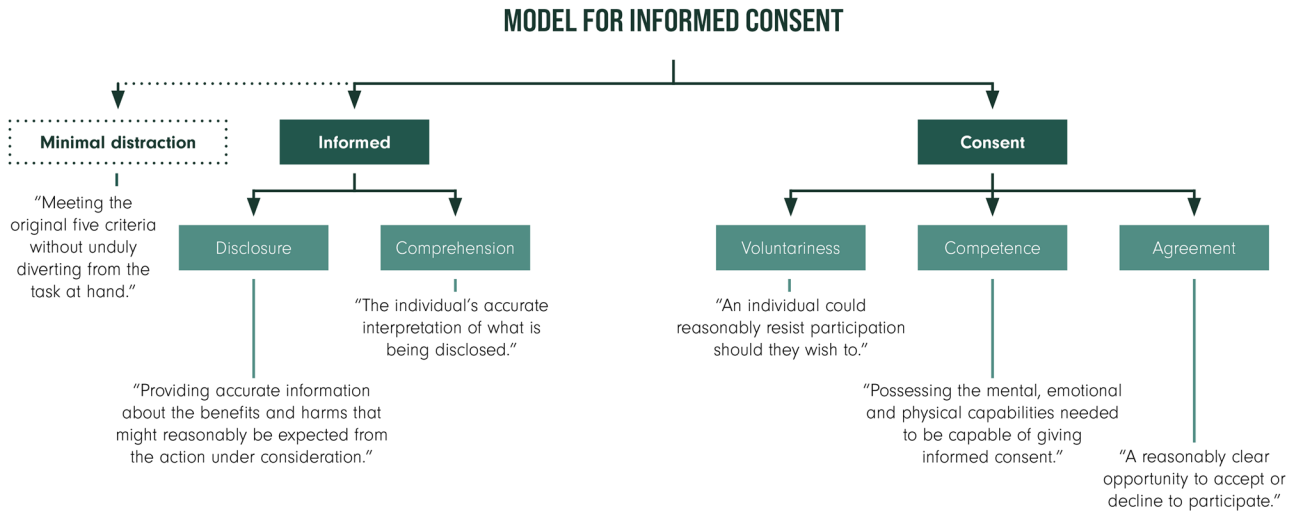


Figure 2. Model for informed consent from the field of design.
Note: Quotations from Friedman, Kahn, and Borning (2013, 62–63).

this overlooks the inherent adding of more complexity by requiring end-users to possess highly complex technical and social skills. Consequently, end-users are "unlikely to understand the complexities of layered applications and their correlated, opaque data flows" (Richards and Hartzog 2019, 1482), as they need to be able to consider the individual, contextual, and collective short- and long-term consequences of their data disclosure decisions.

To safeguard data disclosure in the digital society, we consider all three perspectives—*Society and Ethics*, *Law and Governance*, and *Design and Application*—as important lenses and essential approaches for redesigning the model of consent. That said, we do not suggest using each lens in isolation but rather argue for taking a multidimensional view while redesigning current consent and disclosure interactions. Moreover, we consider it important to include the underlying consent models in charting the design space of consent to create a comprehensive understanding of data disclosure. Hence, we synthesized the aforementioned practices into three models of consent: *Moral Consent*, *Protective Consent,* and *Human-centered Consent*. Table 2 provides an overview of the essential conditions of these consent models with different emphasis on essential conditions of each consent model is highlighted. It is important to note that these conditions are not mutually exclusive.

Contemporary practices of consent

In addition to these models of consent, a deconstruction of contemporary consent practices is important to gain the thorough understanding necessary to chart the current design space of consent and disclosure.

Types of consent practices and disclosure interactions

In Table 3, we describe different types of consent practices and disclosure interactions in the digital society. The first column displays the types of data governance practices that involve consent between organizations and their end-users. Digital platform organizations with their socio-technical data infrastructures, especially social media platforms, shape user-platform involvement and participation practices (Alaimo, Kallinikos, and Valderrama-Venegas 2020; Alaimo and Kallinikos 2017). The second column elaborates on the design practices of disclosure interactions. The governance and design practices of consent (left) and disclosure interactions (right) affect

Table 2. Overview of essential conditions of consent models.

	Informed			Consent						Expressed-explicit			
	Specific	Disclosure statement	Comprehension	Autonomy	Right to confidentiality	Individual trust	Freely given/ voluntariness	Agreement	Competence	Clear affirmative action	Unambigious meaningful choice	Easy accessable	Minimal distraction
Moral consent model	x	x		xxx	xxx	xxx	x	x					
Protective consent model	xx	x		xx	x		xxx	xxx		xxx	xxx	xxx	
Human-centered consent model	xxx	xxx	xxx	x	x		xxx	xx	xxx	x	x	xxx	xxx

xxx = core condition xx = moderate emphasis on this condition x = some emphasis on this condition.

Table 3. Types of consent practices (left) and disclosure interaction practices (right).

Data governance practices (with consent)	Designed disclosure interaction practices
Terms and Conditions, Terms of Service, and Terms of Use are all different names for the same kind of legally binding agreement. There is no legal difference between these. Organizations are not obligated to provide such terms of agreements. Although, they do so to protect the organization's interests, as the terms describes the agreements rules and limits (iubenda n.d.)	*Long contracts (with checkmarks)* are common practice for Terms and Conditions and Privacy Policy agreements. It is often mandatory to select checkmarks to be able to use an organization's service for the first time or after receiving revised terms. This is then referred to as a *Consent Wall*. Sometimes organizations apply consent provided for these contracts to multiple sub-organizations at once. An example of this is Meta with both Facebook and Instagram
Disclaimers are sometimes provided in addition to Terms and Conditions. They state what the organization is not responsible for, thereby protecting it against legal liability. In essence, organizations use disclaimers to give up legal claims, obligations or rights (Wex Definitions Team 2021)	*Consent Banners and Popups* often mediate the interaction between end-users and organizations in the case of consent requests for cookies. They come in many shapes, sizes, and positions. They generally offer the option to manage cookie settings to allow end-users to customize their consent preferences on different levels. For example, consent can be specified per stakeholder, per purpose (e.g., personalization, marketing) or per processing activity (e.g., linking devices, location data)
Privacy policies are generally perceived to improve end-user trust and reduce privacy concerns. However, organizations are legally required to provide this agreement. It explains how personal data is used and informs end-users about security tools and protection systems (Wu et al. 2012). It can be defined as a description of "a system's data practices including all relevant parameters, namely what data is being collected about users (and why), how this information is being used (and why), whether it is shared with third parties and for what purposes, how long information is retained, as well as available choice and access mechanisms." (Schaub et al. 2015)	*Implied consent* is often presented in the form of automatic cookie acceptance by scrolling through an organization's service
Cookies are trackers that enable the collection and storage of information on online activity and device specifications (Autoriteit Persoonsgegevens n.d.). They are necessary for performing crucial functions on digital platforms but also have the potential to identify end-users without their consent due to the large amount of data they store (Koch 2019). Therefore, consent must be obtained	*Cookie walls* look like banners or pop-ups and notifies end-users of cookies which they cannot refuse *N.B*: Cookie Walls and Implied Consent are both practices that are not allowed in many European countries
Legitimate interest is a lawful foundation for processing personal data. It is appropriate for expected data practices and has a minimal impact on privacy (Information Commissioner's Office 2021a). The first- or third-party interest can be individual and/or societal. Examples of this legal foundation provided by the European Commission include processing within a client relationship, processing for direct marketing purposes, preventing fraud, and securing the network and information security of IT systems	*Consent as part of subscriptions* is a practice that links information about data disclosure and consent to paid subscription plans for services provided by an organization. As an example, selecting a free subscription means that an end-user is consenting to the use of cookies and tracking by the organization and third parties to provide personalized advertising

each other reciprocally. On the one hand, agreements, even those not requiring consent, as in the case of strictly necessary and functional cookies, affect the disclosure interaction (Europa.eu 2021). On the other hand, the design of consent notices affects end-users' disclosure decisions and interaction rates, as shown by several studies (Koch 2019; Schaub et al. 2015; Wu et al. 2012).

Within the design literature, studies have found that properties of consent notices such as position, visibility of choices, service blocking, use of nudging, links to policy documents and specific mentions in text all have significant effects (e.g. Utz et al. 2019). Research has also provided insights into user behavior such as default conditions and coping, and the effect of threat appraisal on acceptance rates were found as well (Van Bavel and Rodríguez-Priego 2016). Based on this comprehensive evidence, we argue that the interplay between consent practices and disclosure interactions is a key element in the redesign effort for their improvement.

Form and substance (re-)design recommendations

The aforementioned types of consent practices and disclosure interactions have become a key element in international privacy disputes and transnational innovation of digital platforms. (Inter)national supervisory authorities and courts are increasingly taking legal action against organizations in the digital society that do not comply with consent regulation and legislation (Edenberg and Jones 2019). Consequently, it is crucial to improve consent practices and disclosure interactions, as they are currently the main mechanism for end-users to regulate data disclosure and control their privacy. As discussed above, studies in multiple literature streams propose many suggestions and specific recommendations for improvement from different perspectives. In this section, we categorized the currently suggested guidance and specific recommendations for the design of consent notices and agreements such as the Terms and Conditions (T&C). We thereby make a distinction between consent notices and

agreements when presenting suggested general guidance for their design. In addition, we make the same distinction for our description of specific design recommendations.

(Re-)design guidance: Consent notices

Schaub et al. (2015) propose providing overall guidance on design aspects of consent notices that can impact their effectiveness, instead of proposing standalone requirements. This overall guidance is provided by mapping the design space for privacy notice design. Their framework is meant to indicate the dimensions along which consent practices can be innovated: timing, channel, modality, and control (Schaub et al. 2015) (Figure 3).

Timing refers to when notices are presented. The design space illustrates different options: at setup during first-time use, at the time when a specific data practice is active (i.e., just in time), when it is relevant to show additional notices for context (i.e., context-dependent), at a specific number of times in a specified frequency (i.e., periodic), during an ongoing data practice (i.e., persistent) or when end-users actively seek information for themselves (i.e., on demand). *Channel* refers to how notices are delivered and includes primary, secondary, and public options. Primary means that the notice is provided on the same platform. Secondary refers to notice provision on other channels. Both primary and secondary channels are directed toward a specific group of end-users. If the identity of the end-user is broad or unspecified, public channels may be used (e.g., signs to indicate camera surveillance). *Modality* refers to what interaction modes are used: visual, auditory, haptic or machine-readable means. Visual includes text, images, icons or a combination thereof, which are frequently used in contemporary consent requests. Auditory means include spoken words or sounds. Haptic feedback can be provided through vibrations. Neither are commonly used in the context of digital platforms. A machine-readable format involves encoding data practices and communicating them to other systems and devices. *Control* refers to how choices are provided: *via* blocking, non-blocking or decoupled. Blocking means that end-users should make a choice on what to provide consent for based on the information in the notice. Non-blocking does not require end-user engagement and involves, for instance, settings replicated for multiple interactions. Decoupled means that the choices may be separate from the privacy notice; for instance, this is the case with privacy settings pages or reviews when necessary. Based on the same line of reasoning Feng, Yao, and Sadeh (2021) proposed to unpack this control dimension into the two separate sub-dimensions of notice functionality (presentation, enforcement and feedback) and type of choice (binary, multiple, contextualized, and privacy right based).

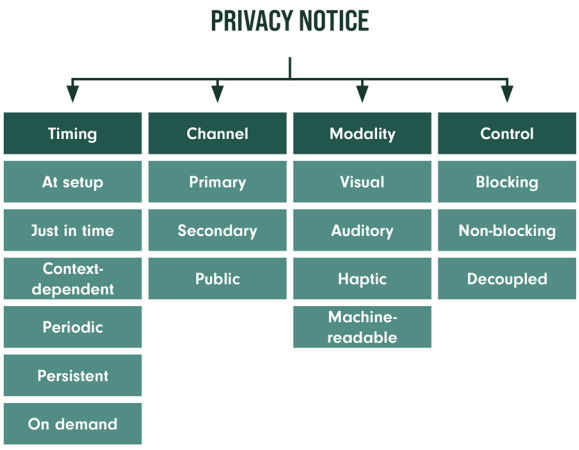


Figure 3. A framework for the design space of consent notices. Adopted from Schaub et al. (2015).

(Re-)design recommendations: Consent notices

In addition to general design guidance, specific recommendations are also provided for designing consent notices. For instance, Utz et al. (2019) recommend, based on their study findings, that consent notices should be placed in the lower left corner on a desktop and in the lower part of the screen on a cellphone, as this placement significantly increases the chances of end-users interacting with them. In addition, Nouwens et al. (2020) conclude that end-users effectively ignore any information and control after the first page of a consent notice. Therefore, they propose providing granular controls on the first interface of a consent notice to further stimulate interaction rates and control over personal privacy and data practices. Their research shows that this intervention decreased consent acceptance rates by 8 to 20%. Other recommendations suggest a layering of Just-in-Time notices that break consent into bite-sized choices at the moment they matter. A prior study by Harkous et al. (2016) proposed the use of chatbots as a more intuitive and natural interface to delivering privacy notice and choice through a two-way dialogue between the user and chatbot. In a field study such a personalized privacy assistant was evaluated by users to have a high adoption rate –78.7% and the recommendations made by this assistant were perceived as usable. Although, in terms of useful outcomes, participants

only changed 5.1% of their settings despite substantial engagement with daily "privacy nudges" (Liu et al. 2016). Concerning the consent interface designs. Habib et al. (2022) assessed the usability impact of seven design parameters of 12 variants of cookie consent interfaces and concluded that that a fully-blocking consent interface with in-line cookie options accompanied by a persistent button enabling users to later change their consent decision best meets several design objectives. The latest study from Bouma-Sims et al. (2023) evaluated the usability of cookie consent interface design of 14 One-Trust consent management platform interfaces and found that the initial set of options displayed in the cookie banner had the largest effect on user behavior although other significant effects concerned lower comprehension of interface information among mobile users and negative sentiment among UK vs US participants. Once again, providing evidence of the inadequacy of current cookie consent processes and the notice-and-choice framework for cookie consent banners.

(Re-)design guidance: Consent agreements (T&C)

Similarly to Schaub et al. (2015) guidance for consent notices, Kinch (2021) and Kinch and Mytka (n.d.) have developed the Better Disclosure Toolkit and the Better Disclosure Canvas respectively, which aim to improve the design of Terms and Conditions agreements. The Canvas features nine steps and can be used as a guideline and supportive tool in the design process: (1) Lead with values, (2) Break components down and utilize layering techniques, (3) Diversify the form factor, (4) Offer contextual guidance, (5) Give visibility of tangible progress, (6) Clarify the consequences (both negative and positive), (7) Delay the core action, (8) Give people a receipt of the agreement they entered into (enable review at any time), and (9) Define action items and ownership.

(Re-)design recommendations: Consent agreements (T&C)

In addition to general design guidance, specific recommendations are also provided for designing consent agreements such as Terms and Conditions. For example, a study from the European Commission proposes several standalone requirements to improve the form and substance of Terms and Conditions agreements (European Commission 2016). The study argues that these agreements should be made simpler and more user-friendly, which can be achieved by shortening and simplifying the text and indicating how long it takes to read, which makes people more likely to read (parts) and understand them. In addition, default exposure to agreements seems to increase readership. Furthermore, added quality cues (e.g., "These Terms and Conditions are fair") influence end-users' attitudes and behaviors regarding trust in the organization and the agreements themselves. Specifically, endorsements by national or European Union consumer organizations have a positive effect. The last proposition is to stimulate end-users to gain awareness of their digital rights from other sources—such as the frequently asked questions section—to reduce the need to include such matters in the agreements. Consequently, they would only contain service-relevant information.

Critical barriers to the redesign of consent

The purpose of notifying end-users regarding a digital platform organization's data practice is to enable them to make informed decisions about their personal privacy. However, from our comprehensive literature review, we learned that organizations in our digital society in fact impose barriers and thresholds instead. As shown in Figure 4, the first major barrier posed by contemporary consent practices is that they are often useless (Schaub et al. 2015) due to *Regulatory Noncompliance* (Carpineto, Lo Re, and Romano 2016; Leenes and Kosta 2015; Nouwens et al. 2020; Trevisan et al. 2019) and additionally suffer from being overcomplicated and unclear due to differences in national legislations (Edenberg and Jones 2019). This barrier discourages end-user access to their data and prevents them from proactively managing their data disclosure.

A second major barrier concerns *Consent Malpractices,* which cause unusable consent practices and disclosure interactions (Schaub et al. 2015) following Richards and Hartzog (2019) taxonomy of unwitting consent, coerced consent, and incapacitated consent practices. Therefore, end-users generally ignore consent notices and pay little consideration to the disclosure decisions to be made (Graßl et al. 2021; Obar and Oeldorf-Hirsch 2020; Schaub et al. 2015).

Critical barrier 1: Regulatory noncompliance

Contemporary consent practices are often not compliant with current regulations and legislation. Consent obtained through non-compliant practices has been ruled to be invalid (Autoriteit Persoonsgegevens 2019; Carpineto, Lo Re, and Romano 2016; Leenes and Kosta 2015; Nouwens et al. 2020; Trevisan et al. 2019).

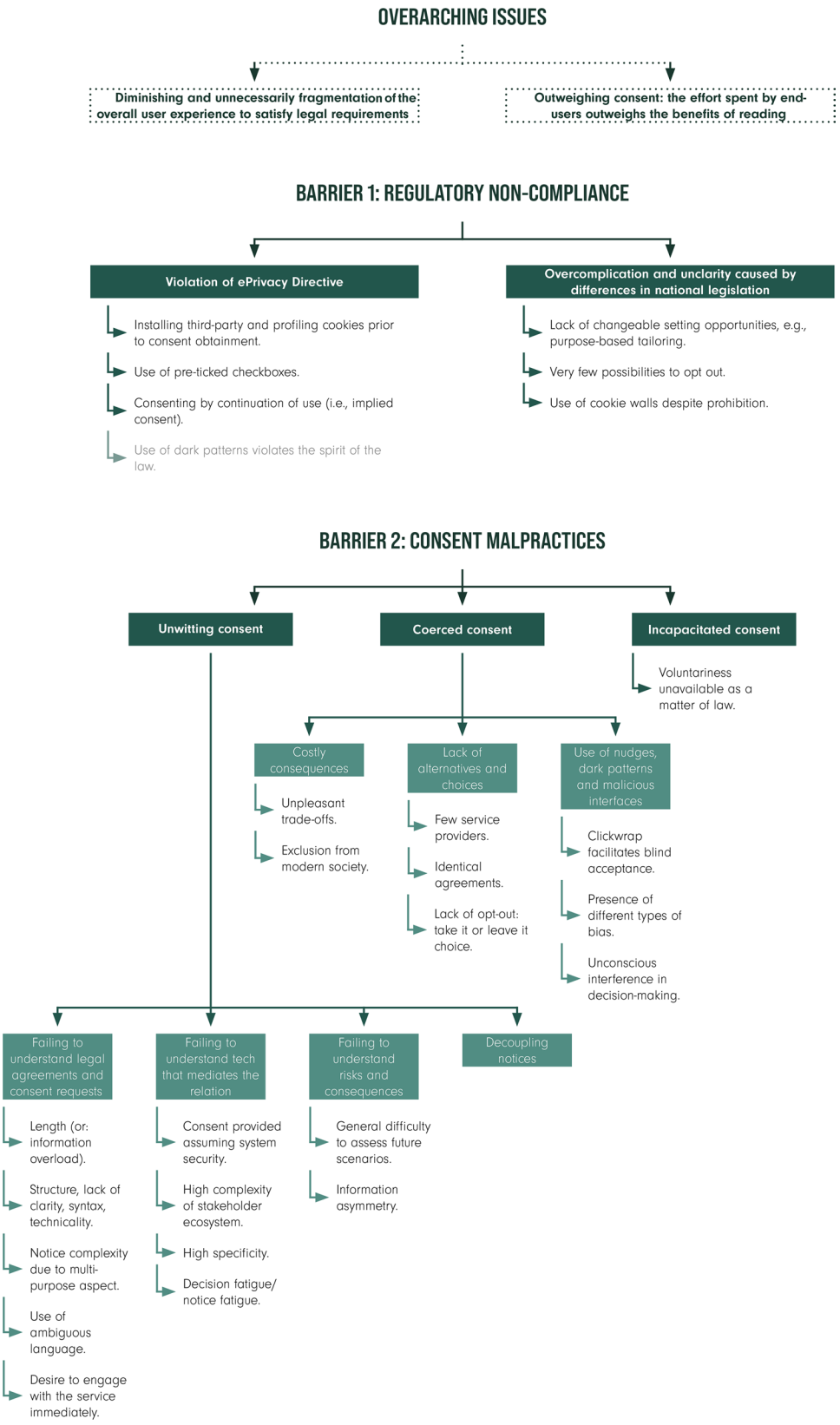


Figure 4. Diagram specifying the factors influencing critical barriers.

Violation of the ePrivacy Directive

The first identified cause of regulatory noncompliance is *direct violation of the ePrivacy Directive*. An example of this violation is an organization that installs third-party cookies and profiling cookies prior to receiving end-user consent (Trevisan et al.

2019). Other common violations include the use of pre-ticked boxes and consenting by continuation of digital platform use (i.e., Implied Consent) as concluded by the Dutch Data Protection Authority (Autoriteit Persoonsgegevens 2019). Furthermore, Nouwens et al. (2020) found that, in addition to implied consent, dark patterns in consent notices are ubiquitous. A dark pattern that "tricks users into doing something is likely to achieve more conversions than one that allows users to make an informed decision" (Brignull 2011).

Despite the absence of an explicit ban on dark patterns in the GDPR, their implementation goes against the spirit of the law. Overall, violation of the ePrivacy Directive has remained constant between 2015 and 2018 (Trevisan et al. 2019). Consent management organizations are particularly negligent, as only 11.8% of the investigated digital platforms meet minimal legal requirements (Nouwens et al. 2020).

Overcomplicated and unclear terms caused by differences in national legislation

The second identified cause of regulatory noncompliance is the presence of *overcomplicated and unclear terms caused by differences in national legislation* (Edenberg and Jones 2019), which might further increase noncompliance. Consent practices differ significantly across Europe because of differences in national legislation. For instance, more than half of the digital platforms researched in the EU lack the option to change settings, such as purpose-based tailoring of cookies, thereby preventing end-users from proactively managing their data disclosure. Furthermore, some countries provide very few possibilities to opt out. Sometimes even cookie walls are used, even though they are prohibited.

Critical barrier 2: Consent malpractices

Contemporary consent practices are often unusable due to the way they are currently implemented by organizations in the digital society, here referred to as *Consent Malpractices*. Richards and Hartzog (2019) have developed a taxonomy to refer to different types of problems with current consent practices. They identified unwitting consent, coerced consent and incapacitated consent, to which we add several additional identified issues. This section is based on European norms that represent the highest level of data protection and information privacy.

Unwitting consent

Unwitting Consent is malpractice in which end-users are unaware and deliberately left ignorant during disclosure interactions (Richards and Hartzog 2019).

First, end-users may fail to understand the legal agreements and consent requests (European Commission 2016; Graßl et al. 2021; Reidenberg et al. 2015; Schaub et al. 2015), due to their length [termed "information overload" by Obar and Oeldorf-Hirsch (2020)], language, structure, technicality, lack of clarity and/or syntax, for instance (Richards and Hartzog 2019). In addition, Schaub et al. (2015) identified notice complexity as a cause due to its multipurpose aspect (i.e., the need to inform end-users, demonstrate compliance, and limit organizational liability simultaneously) and vague use of language to prevent limitation of future uses of collected end-user data (Gray et al. 2021; Schaub et al. 2015). Moreover, Graßl et al. (2021) state that the use of ambiguous language causes uncertainty in the decision-making process, thereby making it even more difficult for end-users to understand consent practices. Lastly, all these factors are diminished by end-users' desire to engage with the provided service immediately without being slowed down by explanatory text or discussion about the means (Obar and Oeldorf-Hirsch 2020).

Second, end-users may *fail to understand the technology that mediates the relation between end-users and digital platforms*. As a consequence, consent is provided with the *assumption that organizations' systems will protect end-users and are secure* (Richards and Hartzog 2019). However, the Cambridge Analytica scandal has shown that dubious data practices that do not protect end-users occur on an international scale. In addition, systems *lack security* regarding, for instance, session cookies, as currently the majority of data is left unprotected in several industries. Another example in which end-users may fail to understand the technology involves advertising on digital platforms. Advertising technology employs *highly complex* advertising networks and servers to manage, run, and report on ad campaigns. However, simplifying and streamlining compliance for this data practice does not justify the real complexity of these processes. On the contrary, *high specificity* may cause end-users to suffer from *decision-fatigue/notice fatigue*, thereby reducing their ability to process information regarding data practices in relation to consent (Richards and Hartzog 2019; Schaub et al. 2015; Van Bavel and Rodríguez-Priego 2016).

Third, end-users may *fail to understand the consequences and/or risks of their informational relationship*

with organizations in the digital environment (Richards and Hartzog 2019). People generally have difficulty assessing future uses and concerns associated with data disclosure (Obar and Oeldorf-Hirsch 2020), yet they are *repeatedly asked to construct future scenarios* in which provided consent might or might not harm them (Richards and Hartzog 2019). In addition, end-users may fail to assess consequences due to the presence of *information asymmetry* between them and organizations regarding the purpose of data collection and future application of collected end-user data (Acquisti et al. 2017; Graßl et al. 2021).

Fourth, we identify the malpractice of *decoupling notices*, as introduced by Schaub et al. (2015), as another reason why end-users are deliberately left in the dark during disclosure interactions. Decoupled notices are privacy notices that are presented separately from the actual system or device. For instance, privacy policies are provided on organizations' websites, while an Internet of Things product (e.g., a smartwatch) does not provide any notices itself. This causes a gap between end-users' knowledge of the data practices and the actual data practices (Schaub et al. 2015).

Coerced consent

Coerced Consent occurs as a malpractice when data disclosure is (partially) involuntary (Richards and Hartzog 2019).

First, sometimes there is no choice other than to accept, which may have *costly consequences* (European Commission 2016). Similarly, a choice can become an *unpleasant tradeoff* when either consent is provided or an important asset is lost (Graßl et al. 2021; Richards and Hartzog 2019). For instance, choosing not to use digital platforms is in practice akin to choosing not to participate in modern society (Hill 2019).

Second, there is a *lack of alternative service providers,* which highly limits options for consent and even less for bargaining. Even if there is sufficient market competition, organizations might still offer identical Terms and Conditions agreements (Richards and Hartzog 2019). Furthermore, often end-users are informed about data practices, but *are not provided with opportunities to opt out* (i.e., a take-it-or-leave-it choice). In these instances, end-users almost always provide consent if it means getting access to the digital platform they want to use (Schaub et al. 2015).

Third, contemporary disclosure interactions suffer from *dark patterns and malicious interfaces* that significantly affect consent provision rates (Richards and Hartzog 2019; Utz et al. 2019). For example, applying clickwrap (i.e., quickly bypassing agreements with one click) contributes to end-users' ignorance behavior toward presented agreements and/or notices, thereby facilitating fast lanes to monetized sections of the service and maintenance of the status quo (Obar and Oeldorf-Hirsch 2020). Consequently, different *types of bias* are present in consent requests such as status-quo bias (e.g., preference for the default) and salience bias (e.g., focus on prominent features) that influence people's privacy decisions (Graßl et al. 2021). These manipulative techniques and corresponding biases favor organizational profits over end-user values. Dark patterns may therefore lead to undesirable interference in end-users' decision-making processes and degree of control over their personal privacy and data practices (Forbrukerrådet 2018; Graßl et al. 2021; Nouwens et al. 2020; Schubert 2015). In addition, these malpractices obstruct the creation of a trustworthy relation between end-users and organizations.

Incapacitated consent

Incapacitated Consent occurs as a malpractice when decision-making on data disclosure is legally unavailable. For example, children are legally incapable of providing consent (Richards and Hartzog 2019).

Overarching issues

To conclude, we need to tackle two critical overarching issues. One, the practice of *diminishing and unnecessarily fragmentation of the overall user experience* of consent practices and disclosure interactions to satisfy legal requirements (Gray et al. 2021). Two, *outweighing consent* –the effort spent by end-users on reading policies, terms, and notices outweighs the benefits of reading them (European Commission 2016), especially considering that organizations' policies may change at any time and that effort may be spent in vain (Schaub et al. 2015).

The mapping of the overarching issues and the two critical barriers shows that redesign efforts by, and centered on, these separate fields (law and governance, computer sciences, organizations, design sciences, and others) are insufficient to overcome the two critical barriers. Their resolution requires inputs from a number of different, sometimes overlapping, fields. Therefore, we recommend engaging in transdisciplinary redesign efforts rather than pursuing a disciplinary perspective.

Redesigning consent

Resolving critical barriers to (re-)designing consent

To redesign consent, our principal finding in this deconstruction study is the identification of the two critical barriers namely, *Regulatory Noncompliance* and *Consent Malpractices*—that digital platform organizations currently practice. In addition to the identified overarching issues (Figure 4), these barriers bring into focus the presence and interplay of specific issues and relational dynamics between digital platform organizations and end-users that need to be resolved with transdisciplinary cooperation for successful consent practice and disclosure interaction redesign efforts. Our detailed mapping of the barriers might be used as guidance for redesigning throughout the innovation process, although we prefer to consider this overview as evidence of the overwhelming complexity of disclosure interactions. In effect, this work once more confirms that current organizational practices make it impossible to properly manage consent by end-users across their digital journey.

Furthermore, in this study we extend the current understanding of contemporary consent practices and disclosure interactions. We provide insight into the (re-)design recommendations by categorizing these into *form and substance* and *general guidance* on design aspects of consent notices (e.g., cookies) and agreements (e.g., Terms and Conditions)—laying out areas of opportunity to further define the design space of consent practices and disclosure interactions.

From the f*orm and substance* recommendations, we unpacked detailed design elements such as position, length, structure, technicality, clarity, and syntax influence interaction rates, decision-making processes, and acceptance rates (Forbrukerrådet 2018; Graßl et al. 2021; Nouwens et al. 2020; Schubert 2015; Utz et al. 2019; Van Bavel and Rodríguez-Priego 2016). However, these types of design interventions are found to only have a minor impact on individual decisions and seem not to affect the societal-level consequences (European Commission 2016; Nouwens et al. 2020; Utz et al. 2019; Van Bavel and Rodríguez-Priego 2016).

Safeguarding data disclosure remains a grand societal challenge. Consequently, the suggested recommendations at the level of *form and substance* seem only fit to tackle individual detailed issues as specified in the barriers overview. From this, we conclude that detailing the issues and recommendations in greater depth leads to an insignificant impact on improvement, and that redesigning consent practices and disclosure interactions of consent models is required instead. Accordingly, the design space needs to open toward new model suggestions.

Therefore, our recommendation for future research is to focus efforts to redesign the consent model rather than the consent *form and substance.* We suggest shifting from siloed research perspectives and detailed recommendations of consent related to characteristics of consent notices and agreements toward models of consent and relational thinking. In addition to existing models of consent (i.e., moral, protected and human-centered), we propose considering a novel model: *Relational Consent*.

Conceptual redesign: Relational consent

In line with our initial synthesis of three models of consent (i.e., moral consent, protective consent and human-centered consent), we take a multidimensional view in the conceptual redesign of consent and disclosure interactions. We propose to apply relational design to consent: *Relational Consent*.

In essence, the central focus of *Relational Consent* is on the relation between two main actors: end-users and digital platform organizations. We conceptualize that both are engaged in the dynamic relation of data transformation (see Figure 5). Different from the existing models of moral- , protective- , and human-centered consent, the endeavor is to view consent not as a one-off exchange focused on single interactions (see for instance Graßl et al. 2021), but as a transformation of the relationship based on the autonomous willingness of one party to allow the action of the other party. By pursuing this *Relational Consent* model, we extend the conceptual work of Solove (2012), who suggested viewing consent as the foundation of end-users' relationships with digitally mediated organizations by providing an empirical and methodological translation into design practice. This novel model, which positions the relationship of end-users and organizations in a central role in consent, also corresponds with the recent suggestions of Richards and Hartzog (2019), to be more sensitive to relationships and power disparities, and Edenberg and Jones (2019), to consider consent as a relational concept that functions to transform the relation between two parties.

We introduce the *Relational Consent* model (see Figure 5) with at its core the idea of an evolving relation in a process of gradual data disclosure and multiple conversations about consent between end-users and platform organizations, developing a data exchange relation over a longer period of time. This resonates with Martin and Shilton (2016) proposal to consider

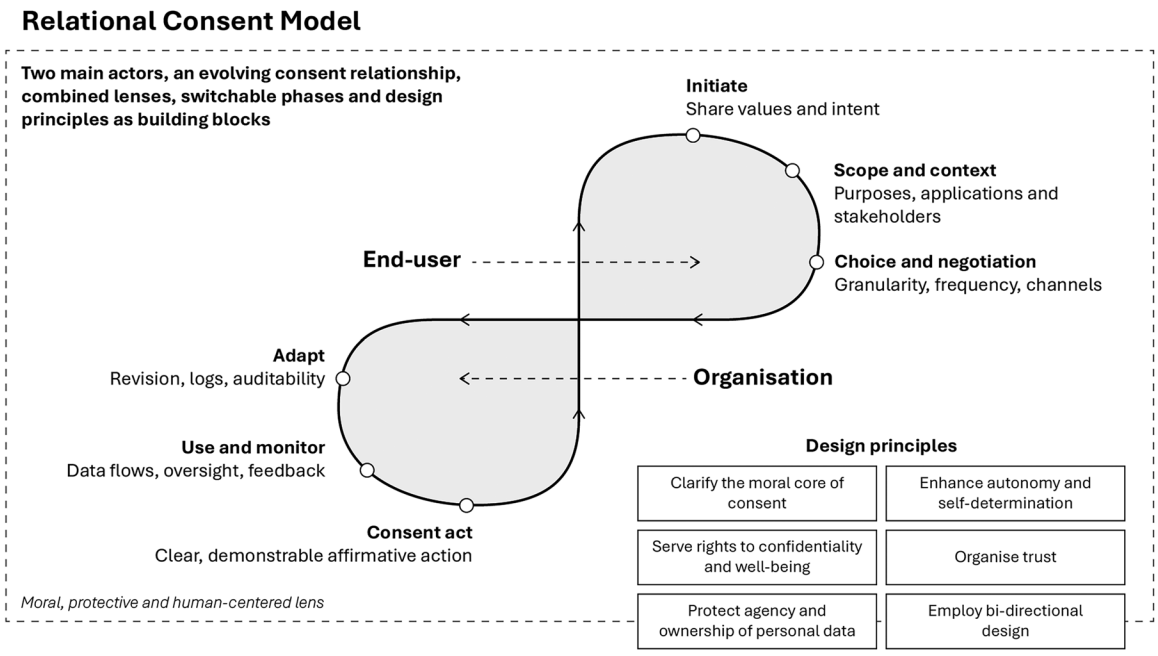


Figure 5. Relational consent model.

flow granularity and temporal context to capture the subtleties of real-world user experiences and dynamic norm shifts. They proposed this as an extension to the contextual integrity model of Nissenbaum (2004, 2019). Considering that this model brought nuance to disparate framings of both FAIR information practice and control-based definitions of privacy; by providing the alternative concept of appropriate flows, the underlying philosophy of relational consent is to some extend similar. Different, however, are the focal point of attention on the evolvement of the relation, rather than the changing contexts and its violations. Relational consent isn't about violations and protecting users from violations, nor is it about taking a moral stance, and designing from a one-directional point of view, either an end-user or an organization, relational consent is about a bi-directional relation and shared decision making over a longer period of time. Our model of taking the relation central extends prior design studies which have either addressed multiple perspectives (Gray et al. 2021) but did not consider the organization's view or focused on how one actor's view is affected by the other instead of focusing on their interaction (see for instance Graßl et al. 2021).

Besides going beyond resolving organizational malpractices, the *Relational Consent* model proposes going beyond an end-user centric focus. This fundamental shift in thinking discards the conceptualization of how end-users are—often negatively—affected by practices. In contrast, *Relational Consent* considers their active connection to, and dynamic relation with, digital platform organizations as being central to redesigning consent practices and disclosure interactions.

Design principles for consent

In addition, we provided several redesign recommendations of a conceptual nature that we synthesized and termed as "*Six principles for the redesign of consent practices and disclosure interactions.*"

1. *Clarify the moral core of consent.* Considering the evolving nature of relational consent, clarifying the moral core of informed consent brings it back to its essentials. As concluded above, the values of moral consent—autonomy, right to confidentiality and individual trust—are clear. Its ethical objective is to enable end-users to practice their digital rights and manage their data disclosure. To clarify this moral core upfront is a good start for (re-) building an ethical relationship. According to Edenberg and Jones (2019), this can provide a way forward to cooperative online jurisdictions in the digital society. For its redesign, five conditions are key: fairness condition—end-users should be treated fairly and should not be required to sacrifice other important rights; voluntariness condition—freedom to choose from among a set of viable options; scope condition—mutual understanding of a clearly defined scope of action; knowledge condition—relevant information provided to the end-user,

including what consent is given to and how that information will be processed and used; background condition—clear delineation of the background conditions for permissible and impermissible uses of end-users' data.

2. *Enhance autonomy and self-determination.* Richards and Hartzog (2019) conclude that the core problem with consent for data practices is not the form or substance of the interaction itself and instead argue for consent practices that meaningfully enhance the autonomy and self-determination of end-users. They propose three principal requirements that effective consent practices must have: (1) Consent requests must be infrequent to prevent decision fatigue, (2) Risks of consent must be vivid and easy to envision, and (3) End-users need an incentive to understand the decisions' significance and motivate them to take each request seriously.
3. *Serve rights to confidentiality and well-being.* In addition to enhancing autonomy, consent should serve the well-being of the end-user or, in other words, the agent's interest. However, these values may sometimes conflict. Focusing on the context in which consent takes place may provide a solution to this conflict. The conditions should ensure fair treatment of users, as described in the Fair Transaction Model. In essence, the model states that an entity seeking consent is morally permitted to proceed on the basis of a consent transaction if it has treated the entity that is requesting consent from fairly and responds in a reasonable manner to its own expression of consent (Miller and Wertheimer 2010).
4. *Organize trust.* The influence and relevance of improving consent practices at organizations is characterized by enhanced trust. This can be achieved by improving the perception of fairness of the agreements that end-users are providing consent to European Commission (2016). Improving trust is important not only because researchers identify it as the key ingredient toward a better future (Richards and Hartzog 2019), but also because organizations may gain competitive advantages and unique selling points by employing user-centric methods for consent management in combination with implementation of sophisticated supportive tools.
5. *Protect agency and ownership of personal data.* Relational consent is about protecting users from r*egulatory noncompliance* and *consent malpractices*, through a gradual evolving data disclosure instead of an all in once agreement. If performed meaningfully, relational consent practices have the potential to enable both end-users' and organizations agency regarding ownership and management of their own personal data. Designing relational consent includes cognitive, collective, and contextual dimensions. As currently the consent practices of Google, Amazon, Facebook, Apple and Microsoft (i.e., GAFAM) are particularly lacking in the collective and contextual aspects (Human and Cech 2021), end-users should be empowered in their right to consent through interdisciplinary and multidimensional sociotechnical means and approaches. To further increase relevance for both end users and organizations is to redesign consent practices in such a way to achieve higher customer satisfaction by reducing end-user frustration. In addition, organizations should ensure that end-users will consider building a data exchange relation worth their time.
6. *Employ bi-directional design.* Relational consent isn't about designing from a one-directional point of view, either a user or an organization, relational consent it is about a bi-directional relation and shared decision making over a longer period. Our model includes the organization's view in addition to Gray et al. (2021) who argued for employing bidirectional design in the innovation of consent practices. They describe this type of design as: "the opportunities to evaluate and interrogate design experiences using the language of law and policy (legal → design), while also using a user experience or user interface as a means of addressing gaps or opportunities for more precision in existing legal or policy frameworks (design → legal)" (Gray et al. 2021, 13). Relational consent extends these prior multiple perspective studies by adding the society and ethics perspective (design ↔ society) and the values of the moral core and concern for end-users' well-being in the digital society. Moreover, relational consent adds the organization's point of view and conceptualizes the relation between users and the platform organizations as an evolving relation with multiple interactions instead of focusing on a single interaction. Over a longer period, the consent relation develops in which one actor's view is affected by the other.

For undertaking new efforts to redesign consent, we propose considering these design principles as guidance. To conclude, in considering the practical implications that shed light on how to resolve the critical barriers to consent described in this study, we propose shifting toward a conceptual redesign of new consent practices and disclosure interactions by designing dynamic and process-based future practices and interactions that are grounded on the *Relational Consent* model.

Designers, digital platform organizations and policymakers could consider applying the relational consent model to the development of new consent practices and disclosure interactions. In addition, they can consult the model for the development of policies, regulations and specific organizational requirements. In response, managers and designers could adopt the relational consent model by designing evolving future consent practices and disclosure interactions.

In considering the limitations and future research, we recognize that the proposed model of relational consent and its guiding design principles represent an emerging theory that does not yet conform to the development stages of mutual exclusivity or collective exhaustiveness. Accordingly, future research should consider conducting research on designing relational consent.

Acknowledgments

For providing their valuable advice and support we gratefully acknowledge Dr. Heather Wiltse from Umeå Institute of Design and Prof. Dr. Elisa Giaccardi formerly from Delft University of Technology, faculty of Industrial Design Engineering now affiliated with Politecnico Dipartimento di Design.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

ORCID

Aniek R. Kempeneers http://orcid.org/0000-0001-5540-1686

Lianne W. L. Simonse http://orcid.org/0000-0001-8860-6522

References

Acquisti, A., I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh. F. Schaub, M. Sleeper, Y. Wang, and S. Wilson. 2017. "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online." *ACM Computing Surveys* 50 (3): 1–41. https://dl.acm.org/doi/10.1145/3054926.

Alaimo, C., and J. Kallinikos. 2017. "Computing the Everyday: Social Media as Data Platforms." *The Information Society* 33 (4): 175–191. https://doi.org/10.1080/01972243.2017.1318327.

Alaimo, C., J. Kallinikos, and E. Valderrama-Venegas. 2020. "Platform Evolution: A Study of TripAdvisor." Proceedings of the 53rd Hawaii International Conference on System Sciences, 5462–5471. https://doi.org/10.24251/HICSS.2020.672.

Autoriteit Persoonsgegevens. 2019. "AP: Veel Websites Vragen op Onjuiste Wijze Toestemming Voor Plaatsen Tracking Cookies." https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-veel-websites-vragen-op-onjuiste-wijze-toestemming-voor-plaatsen-tracking-cookies.

Autoriteit Persoonsgegevens. n.d. "Cookies." https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies.

Bak, M. A. R., M. T. Blom, H. L. Tan, and D. L. Willems. 2018. "Ethical Aspects of Sudden Cardiac Arrest Research Using Observational Data: A Narrative Review." *Critical Care* 22 (1): 212. https://doi.org/10.1186/s13054-018-2153-3.

Bouma-Sims, E. R., M. Li, Y. Lin, A. Sakura-Lemessy, A. Nisenoff, E. Young, E. Birrell, L. F. Cranor, and H. Habib. 2023. "A US-UK Usability Evaluation of Consent Management Platform Cookie Consent Interface Design on Desktop and Mobile." CHI'23: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, 1–36.

Boyd, D. 2012. "Taken out of Context: American Teen Sociality in Networked Publics." *The Information Society* 28 (3): 180–187.

Brignull, H. 2011. "Dark Patterns: Deception vs. Honesty in UI Design." *A List Apart* Issue No. 338. https://alistapart.com/issue/338/

Cambridge Dictionary. n.d.a. "Consent." *Cambridge Advanced Learner's Dictionary & Thesaurus*. https://dictionary.cambridge.org/dictionary/english/consent.

Cambridge Dictionary. n.d.b. "Informed Consent." In *Cambridge Advanced Learner's Dictionary & Thesaurus*. Cambridge, UK: Cambridge University Press & Assessment. https://dictionary.cambridge.org/dictionary/english/consent.

Carpineto, C., D. Lo Re, and G. Romano. 2016. "Automatic Assessment of Website Compliance to the European Cookie Law with CooLCheck." WPES'16: Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society, 135–138.

Constantinides, P., O. Henfridsson, and G. G. Parker. 2018. "Introduction: Platforms and Infrastructures in the Digital

Age." *Information Systems Research* 29 (2): 381–400. https://doi.org/10.1287/isre.2018.0794.
Dunn, J. 1967. "Consent in the Political Theory of John Locke." *The Historical Journal* 10 (02): 153–182. https://doi.org/10.1017/S0018246X6700001X.
Edenberg, E., and M. L. Jones. 2019. "Analyzing the Legal Roots and Moral Core of Digital Consent." *New Media & Society* 21 (8): 1804–1823. https://doi.org/10.1177/1461444819831321.
Europa.eu. 2021. "Online Privacy." https://europa.eu/youreurope/business/dealing-with-customers/data-protection/online-privacy/index_nl.htm.
European Commission. 2016. "Study on Consumers' Attitudes to Terms and Conditions (T&Cs)." https://ec.europa.eu/info/publications/consumers-attitudes-terms-and-conditions-tcs_en.
European Parliament and Council of the European Union. 2009. "Directive 2009/136/EC Amending Directive 2002/22/EC on Universal Service and Users." Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws. EU. Vol. 2009/136/EC.
European Parliament and Council of the European Union. 2018. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27." April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC. (General Data Protection Regulation) 4.5.2016 Official Journal of the European Union, Vol. 2016/679: L 119/1-88.
Fabre, J. 2014. "Presumed Consent for Organ Donation: A Clinically Unnecessary and Corrupting Influence in Medicine and Politics." *Clinical Medicine* 14 (6): 567–571. https://doi.org/10.7861/clinmedicine.14-6-567.
Faden, R. R., and T. L. Beauchamp. 1986. *A History and Theory of Informed Consent*. Oxford: Oxford University Press.
Faden, R. R., T. L. Beauchamp, and N. E. Kass. 2014. "Informed Consent, Comparative Effectiveness, and Learning Health Care." *The New England Journal of Medicine* 370 (8): 766–768. https://doi.org/10.1056/NEJMhle1313674.
Feng, Y., Y. Yao, and N. Sadeh. 2021. "A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things." CHI'21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 1–16.
Forbrukerrådet. 2018. "Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy." https://www.slideshare.net/slideshow/deceived-by-design-how-tech-companies-use-dark-patterns-to-discourage-us-from-exercising-our-rights-to-privacy/104616308
Friedman, B., D. C. Howe, and E. Felten. 2002. "Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design." Proceedings of the 35th Annual Hawaii International Conference on System Sciences, 1–10. Honolulu, HI: University of Hawai'i Press.
Friedman, B., E. Felten, and L. I. Millett. 2000. "Informed Consent Online: A Conceptual Model and Design Principles." (University of Washington Computer Science & Engineering Technical Report 8). https://old.vsdesign.org/publications/pdf/UW-CSE-00-12-02_informed_consent_design_principles.pdf
Friedman, B., P. H. Kahn, and A. Borning. 2002. Value Sensitive Design: Theory and Methods." (UW CSE Technical Report 02-12-01). Seattle: Department of Computer Science and Engineering University of Washington.
Friedman, B., P. H. Kahn, and A. Borning. 2013. "Value Sensitive Design and Information Systems." In *Early Engagement and New Technologies: Opening up the Laboratory*, edited by Doorn N, Schuurbiers D, van de Poel I, and Gorman ME, 55–95. Dordrecht: Springer. https://doi.org/10.1007/978-94-007-7844-3_4.
Gillespie, T. 2018. "Consent by Design." *The Information Society* 25 (2): 99–112.
Goldstein, C. E., C. Weijer, J. C. Brehaut, D. A. Fergusson, J. M. Grimshaw, A. R. Horn, and M. Taljaard. 2018. "Ethical Issues in Pragmatic Randomized Controlled Trials: A Review of the Recent Literature Identifies Gaps in Ethical Argumentation." *BMC Medical Ethics* 19 (1) Article: 14. https://doi.org/10.1186/s12910-018-0253-x.
Graßl, P., H. Schraffenberger, F. Zuiderveen Borgesius, and M. Buijzen. 2021. "Dark and Bright Patterns in Cookie Consent Requests." *Journal of Digital Social Research* 3 (1): 1–38. https://doi.org/10.33621/jdsr.v3i1.54.
Gray, C. M., C. Santos, N. Bielova, M. Toth, and D. Clifford. 2021. "Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective." CHI'21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 1–18. 172.
Habib, H., M. Li, E. Young, and L. Cranor. 2022. "Okay, Whatever': An Evaluation of Cookie Consent Interfaces." CHI'22: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, 1–27.
Hansson, M. G., J. Dillner, C. R. Bartram, J. A. Carlson, and G. Helgesson. 2026. "Should Donors be Allowed to Give Broad Consent to Future Biobank Research?" *The Lancet Oncology* 7 (3): 266–269. https://doi.org/10.1016/S1470-2045(06)70618-0.
Harkous, H., K. Fawaz, K. G. Shin, and K. Aberer. 2016. "PriBots: Conversational Privacy with Chatbots." https://www.usenix.org/system/files/conference/soups2016/wfpn16-paper-harkous.pdf
Hill, K. 2019. "Goodbye Big Five." https://gizmodo.com/tag/goodbye-big-five
Human, S., and F. Cech. 2021. "A Human-Centric Perspective on Digital Consenting: The Case of GAFAM." In *Human Centred Intelligent Systems*, edited by A. Zimmermann, R. J. Howlett, and L. C. Jain, 139–159. Singapore: Springer. https://doi.org/10.1007/978-981-15-5784-2_12.
Information Commissioner's Office. 2021a. "What Is Valid Consent?" https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/.
Information Commissioner's Office. 2021b. "Legitimate Interests." https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-

regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.
iubenda. n.d. "What Are the Terms and Conditions and When Are They Needed?" https://www.iubenda.com/en/help/2859-terms-and-conditions-when-are-they-needed.
Jones, M. L. 2019. "The Development of Consent to Computing." *IEEE Annals of the History of Computing* 41 (4): 34–47. https://doi.org/10.1109/MAHC.2019.2896282.
Kallinikos, J., and I. D. Constantiou. 2015. "Big Data Revisited: A Rejoinder." *Journal of Information Technology* 30 (1): 70–74. https://doi.org/10.1057/jit.2014.36.
Karlsen, J. R., J. H. Solbakk, and S. Holm. 2011. "Ethical Endgames: Broad Consent for Narrow Interests; Open Consent for Closed Minds." *Cambridge Quarterly of Healthcare Ethics* 20 (4): 572–583. https://doi.org/10.1017/S0963180111000314.
Kinch, N. 2021. "The Better Disclosure Toolkit." https://greaterthanlearning.online/core-stream-better-disclosure/.
Kinch, N., and M. Mytka. n.d. "Better Disclosure Canvas—v0.2." https://ethos.tethix.co/tools/better-disclosure-canvas/
Koch, R. 2019. "Cookies, the GDPR, and the EPrivacy Directive." https://gdpr.eu/cookies/.
Leenes, R., and E. Kosta. 2015. "Taming the Cookie Monster with Dutch Law: A Tale of Regulatory Failure." *Computer Law & Security Review* 31 (3): 317–335. https://doi.org/10.1016/j.clsr.2015.01.004.
Liu, B., M. S. Andersen, F. Schaub, H. Almuhimedi, S. Zhang, N. Sadeh, A. Acquisti, and Y. Agarwal. 2016. "Follow my Recommendations: A Personalized Privacy Assistant for Mobile App Permissions." https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-liu.pdf
Lunshof, J. E., R. Chadwick, D. B. Vorhaus, and G. M. Church. 2008. "From Genetic Privacy to Open Consent." *Nature Reviews. Genetics* 9 (5): 406–411. https://doi.org/10.1038/nrg2360.
Mai, J.-E. 2016. "Big Data Privacy: The Datafication of Personal Information." *The Information Society* 32 (3): 192–199. https://doi.org/10.1080/01972243.2016.1153010.
Martin, K., and K. Shilton. 2016. "Why Experience Matters to Privacy: How Context-Based Experience Shapes Consumer Privacy Expectations for Mobile Applications." *The Information Society* 32 (3): 179–189.
Miller, F. G., and A. Wertheimer. 2010. *The Ethics of Consent: Theory and Practice*. New York: Oxford University Press.
Nissenbaum, H. 1999. "The Meaning of Anonymity in an Information Age." *The Information Society* 15 (2): 141–144. https://doi.org/10.1080/019722499128592.
Nissenbaum, H. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79 (1): 119–157.
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., I. Liccardi, M. Veale, D. Karger, and L. Kagal. 2020. "Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence." CHI'20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 1–13.
Obar, J. A., and A. Oeldorf-Hirsch. 2020. "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services." *Information, Communication & Society* 23 (1): 128–147. https://doi.org/10.1080/1369118X.2018.1486870.
Publications Office and European Parliament. 2020. "Protection of Personal Data (from 2018)." https://eur-lex.europa.eu/legal content/EN/LSU/?uri=CELEX%3A32016R0679.
REFIT Platform Opinion. 2016. "REFIT Platform Opinion on the Submission by the Danish Business Forum on the E Privacy Directive and the Current Rules Related to Cookies." https://ec.europa.eu/info/sites/default/files/opinion_comm_net.pdf.
Reidenberg, J. R., T. Breaux, L. F. Cranor, B. French, A. Grannis, J. T. Graves, F. Liu, et al. 2015. "Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding." *Berkeley Technology Law Journal* 30 (1): 39–88.
Richards, N., and W. Hartzog. 2019. "The Pathologies of Digital Consent." *Washington University Law Review* 96 (6): 1461–1503.
Schaub, F., R. Balebako, A. L. Durity, and L. F. Cranor. 2015. "A Design Space for Effective Privacy Notices." https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf
Schubert, C. 2015. "On the Ethics of Public Nudging: Autonomy and Agency." https://doi.org/10.2139/ssrn.2672970.
Solove, D. J. 2012. "Introduction: Privacy Self-Management and the Consent Dilemma." *Harvard Law Review* 126: 1880–1903.
Trevisan, M., S. Traverso, E. Bassi, and M. Mellia. 2019. "4 Years of EU Cookie Law: Results and Lessons Learned." https://petsymposium.org/popets/2019/popets-2019-0023.php
Tuckness, A. 2020. "Locke's Political Philosophy." The Stanford Encyclopedia of Philosophy Archive, edited by E. N. Zalta. https://plato.stanford.edu/archives/win2020/entries/locke-political/
Utz, C., M. Degeling, S. Fahl, F. Schaub, and T. Holz. 2019. "("Un)Informed Consent: Studying GDPR Consent Notices in the Field." CCS'19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 973–990.
Van Bavel, R., and N. Rodríguez-Priego. 2016. *Testing the Effect of Cookie Banners on Behaviour* (Joint Research Center Technical Report JRC103997). Luxembourg: Publications Office of the European Union.
Wex Definitions Team. 2021. "Disclaim." https://www.law.cornell.edu/wex/disclaim.
Wu, K.-W., S. Y. Huang, D. C. Yen, and I. Popova. 2012. "The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust." *Computers in Human Behavior* 28 (3): 889–897. https://doi.org/10.1016/j.chb.2011.12.008.