International Journal of Communication 19(2025), Forum 1814–1820 1932–8036/2025FRM0002

When User Consent Fails: How Platforms Undermine Data Governance

ROHAN GROVER[1]
University of Southern California, USA

Consent is a powerful moral force that features centrally in data governance today, often imposed as a condition for companies to collect users' personal data. In response, an industry of consent management platforms (CMPs) has developed to administer user consent on behalf of companies complying with data privacy laws such as the General Data Protection Regulation. But CMPs do not always work as expected: technical audits reveal that CMPs often violate the conditions of legally valid consent, leading to calls for strengthening user consent. This article reinterprets such audits by applying a sociotechnical perspective to reject the facile solution of bolstering consent. Instead, I characterize CMPs as mediators that obfuscate moral relations, producing *relationship errors* that undermine users' relational autonomy. This reinterpretation points to solutions that repudiate data-as-property and instead reckon with the social nature of datafication.

Keywords: consent, data governance, privacy, relational autonomy, mediation

Consent holds an ambivalent yet persistent position in data governance today. The dominant paradigm treats data like property over which individuals can claim ownership. Beginning with the Fair Information Privacy practices in the 1970s, regulations have demanded that companies request user consent in order to collect and process user data—a requirement that has been largely unsuccessful in curtailing datafication practices (Hartzog, 2017). But today, privacy scholars have all but abandoned consent as a primary basis for data governance, calling it a "dirty word" (Jones & Kaminski, 2020) and an untenable conceptualization "indebted to property thinking" (Cohen, 2021, para. 4). Despite these critiques, consent persists in data governance today through data protection and information privacy laws that follow a regime of "notice and consent" under which data practices are sanctioned by notifying users about data practices and requesting their consent. For example, the European Union's General Data Protection Regulation (GDPR) strengthens requirements for valid consent by stipulating that it must be freely given, informed, specific, and unambiguous.

These stringent requirements for valid user consent have precipitated the commodification of consent. Companies responsible for complying with the GDPR—that is, organizations across the world that collect personal information from EU residents—have had to ensure that their personal data collection and

[1] Thanks to Mike Ananny, Simogne Hudson, Megan Finn, Noah D'Mello, and USC MASTS for their feedback and thoughtful engagement with the ideas reflected here.

Copyright © 2025 (Rohan Grover, rohan.grover@usc.edu). Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://ijoc.org.

processing practices satisfy one of the GDPR's lawful bases.[2] In response, a *privacy tech industry* has emerged to offer data governance solutions, offering compliance-as-a-service by selling software and advisory services. Consent management platforms (CMP) are an example of privacy tech software, developed by companies such as OneTrust, Quantcast, and Osano, that help their clients inform users about their data practices, collect and store user consent records, and recall each user's consent preferences when summoned by an application or enforcement authority.

In this article, I argue that CMPs are not simply neutral intermediaries but rather mediators that compromise the moral power of user consent. I apply a sociotechnical lens to technical audits of CMPs that reveal widespread violations of the conditions for morally valid consent. While some conclude that these *consent errors* can be rectified by strengthening and standardizing user consent, I argue instead that CMPs obfuscate moral relations between users and companies that collect their personal data, thus producing *relationship errors*. I draw on feminist philosophy to describe how these relationship errors undermine users' relational autonomy, which I argue is valuable for repudiating the property basis inherent in the consent paradigm and for reckoning with data as a social relation.

Defining Invalid Consent

Consent is a powerful moral force. It represents a boundary of individual autonomy that forbids certain actions unless one has been granted consent. Legal philosopher Heidi Hurd (1996) describes this as the "moral magic of consent" (p. 121): the presence or absence of consent can distinguish a guest attending a dinner party from trespassing on private property, borrowing from stealing a car, or a handshake from battery. In other words, granting consent creates new rights and obligations for others; it can make something permissible that would otherwise be forbidden. Valid consent commands several criteria in order to uphold a liberal right to individual autonomy, which is achieved in two ways (Hurd, 1996). First, it recognizes that the individual has autonomy as a natural attribute, requiring consent for certain actions. Second, it recognizes that an individual's choice to alter their relationship with another actor by granting consent must be made in an autonomous manner. Thus, consent is a powerful moral force insofar as it upholds individual autonomy by satisfying these two conditions.

In moral philosophy, consent is a transaction between two actors that must meet three criteria and be communicated to be morally valid. Specifically, the consent decision must meet the criteria of competence, voluntariness, and knowledge (Beauchamp & Faden, 1986). *Competence* refers to the ability to make a free choice, which is often measured by age or maturity. *Voluntariness* refers to the absence of coercion, including not only force but also incentives that impose substantial pressure. *Knowledge* refers to both comprehending the scope of the action and understanding its circumstances and consequences. For example, before a medical procedure, a patient should be told not only what the procedure entails but also the alternatives and the relative risks and side effects of each. In addition to these three criteria, the valid consent decision must be communicated. Although some philosophers disagree on the necessary

[2] Article 6 of the GDPR enumerates six lawful bases for processing personal data, only one of which requires valid user consent. Nevertheless, many companies rely on the consent basis to justify collecting and processing personal data, so it still features prominently under the GDPR (see Jones and Kaminski, 2020).

form, I follow Tom Dougherty's (2015) expectation that valid consent must be activated through a *communicative act* that conveys consent while also fostering mutual recognition and accountability between the two actors. Collectively, these conditions provide criteria by which a consent transaction can be evaluated for moral validity—and thus whether it upholds individual autonomy.

Invalidating User Consent

These criteria for morally valid consent serve as a rubric for evaluating consent in practice. In other words, if an actor intends to collect morally valid consent but fails to do so according to the criteria above, this can be considered a *consent error*. In medical practice, consent error often refers to material issues with consent forms, such as illegible handwriting, inaccurate information, or missing signatures, which may lead to malpractice claims. In the context of data governance, computer scientists have conducted technical audits to evaluate whether cookie consent interfaces collect legally valid consent under the GDPR and the EU's ePrivacy Directive, which is also known as the "cookie law" for triggering the proliferation of cookie consent pop-ups.

In this section, I review four such studies of user consent in the field—by Bollinger, Kubicek, Cotrini, and Basin (2022); Bouhoula, Kubicek, Zac, Cotrini, and Basin (2024); Matte, Bielova, and Santos (2020); and Nouwens, Liccardi, Veale, Karger, and Kagal (2020)—to identify how *consent error* is mobilized to diagnose problems with valid consent under the GDPR. These studies employ algorithmic Web crawlers to audit how companies implement the EU's requirements for valid consent when setting website cookies. They are collectively interested in identifying legally invalid (or dubious) consent errors that are otherwise indiscernible to lay users. Notably, each study was conducted during a different time period, between September 2019 and March 2023, and employs a different methodology to sample websites likely subject to the GDPR, classify each website's cookies, test the consent interface, and evaluate potential regulatory violations (see Bouhoula and colleagues [2024] for a comparison). These differences result in some discrepancies in the frequency of each type of error. Nevertheless, I am more interested in the broader question of how user consent—an ambivalent yet persistent feature of data governance—is consistently undermined. Below, I synthesize findings from the four audits using the criteria of morally valid consent described above: competence, voluntariness, knowledge, and a communicative act.

Competence is not addressed directly by the audits of user consent. This is unsurprising since the GDPR does not prescribe specific criteria for competence; instead, it upholds data protection and privacy as fundamental rights. Nevertheless, dark patterns—which are manipulative, deceptive, or coercive interface designs—can undermine competence by impairing agency, independence, freedom, and control (Ahuja & Kumar, 2022). Nouwens and colleagues (2020) found that 87% of websites forced users to follow a longer clickstream to "reject all" cookies compared to "accept all," exhibiting the *obstruction* dark pattern, and Bouhoula and associates (2024) found that 68% of websites presented "positive" and "negative" consent response buttons in different colors, exhibiting the *interface interference* dark pattern that may influence user behavior. These examples undermine one's capacity for rational free choice to make a valid consent decision.

Voluntariness, or the absence of coercion, is compromised more directly. The audits found that some websites—ranging from 7% (Matte, Bielova, & Santos, 2020) to 32% (Bouhoula et al., 2024)—gave

users no choice to decline optional cookie tracking. Even among websites that offered the choice to opt out, many—ranging from 10% (Matte, Bielova, & Santos, 2020) to 33% (Nouwens et al., 2020) to 78% (Bouhoula et al., 2024)—presumed user consent to set cookies even though they had not communicated a consent decision. Additionally, many websites—ranging from 47% (Matte, Bielova, & Santos, 2020) to 56% (Nouwens et al., 2020) to 73% (Bouhoula et al., 2024)—pressured users into granting consent by preselecting checkboxes, which constitutes coercion not only morally but also under the GDPR. These findings illustrate how widely user consent is undermined by forcing or pressuring users into granting consent.

Knowledge, or comprehending the scope, circumstances, and consequences of the action being consented to, is also compromised through incomplete or inaccurate information. Bollinger and colleagues (2022) found widespread problems, including 83% of websites setting undeclared cookies, 9% listing inaccurate expiration times, and 8% describing cookie purposes inaccurately. Bouhoula and associates (2024) also found that 21% of websites were missing purpose declarations for some cookies. These discrepancies undermine the moral validity of user consent because users were not accurately informed about the scope and extent of the data collection that was being requested.

Finally, the *communicative* act of consent is not always respected. Several audits evaluated this by rejecting all nonessential cookies and then identifying which rejected cookies were still set. Recent studies found that 65% of websites set cookies despite a negative consent decision (Bollinger et al., 2022; Bouhoula et al., 2024). In these cases, even if users conveyed a morally valid consent decision, it was not respected by the website.

Mediating Consent, Muddling Accountability

Altogether, these consent errors demonstrate that user consent, in practice, often fails the conditions of moral validity. Moreover, they illustrate how CMPs bear some responsibility for many of the errors by reconfiguring the consent transaction described previously. For example, many CMPs provide templates to client companies that feature dark patterns (Stöver et al., 2022), and CMPs feature violations of valid consent at different rates—sometimes in 100% of cases (Matte, Bielova, & Santos, 2020). Thus, consent in practice diverges from the ideal consent transaction described earlier by splintering consent into a series of translations mediated by a third actor: CMPs.

Mediating consent undermines its capacity to perform moral magic. Recall that consent has the capacity to alter moral relations between two actors, and that the communicative act of granting consent can strengthen their relationship by fostering mutual recognition and accountability. Who is accountable when consent is invalidated in the course of being mediated across a network of actors? Moral philosophers have argued that an action can be morally defensible even without valid consent if an actor genuinely and reasonably presumed they had received consent. This implies that even if a CMP improperly collects user consent, companies may still be morally (but not legally) justified in collecting user data.

It is more complicated when it is difficult or impossible to locate a single source of error. For example, if dark patterns compromise individual competence, websites likely bear legal responsibility, but CMPs also bear some moral responsibility for propagating design standards that undermine user consent.

This draws attention to sociotechnical interactions—such as developing design templates, training clients, auditing implementation—in which a CMP's mediating role is central and accountability is less clear. In such interactions, CMPs heighten the risk of invalidating consent by obfuscating moral relations between the two original actors in the consent transaction: users and companies. Thus, despite CMPs insisting on moral and legal neutrality as "platforms" that merely connect companies and users, they can, in fact, encode political values. In other words, CMPs are not neutral "intermediaries" that transport meaning but rather *mediators* whose "input is never a good predictor of their output" (Latour, 2005, p. 39).

This attention to mediated relations invites a different perspective through which consent error can be better understood as *relationship error*. This approach draws on feminist reinterpretations of autonomy as a relational construct rather than an atomistic property (Mackenzie & Stoljar, 2000). In other words, individual autonomy is not a natural property to protect *from* relationships; it is instead developed *through* relationships and thus must be cultivated through social relations. This perspective shifts attention from consent as an object to be audited and upheld through the *absence* of relational interference—to users as subjects to be evaluated through the relationships that *constitute* their capacity to choose. Thus, centering users means examining how CMPs implicate users' relational autonomy rather than just the validity of their consent. From this perspective, CMPs undermine users' relational autonomy by obfuscating moral relations in the course of mediating user consent.

Reinterpreting consent error as relationship error suggests a different path forward. *Consent error* draws attention to the ways in which consent is invalidated, implying that it can and should be rescued by preserving the conditions for autonomous consent. On the other hand, *relationship error* suggests that improving the integrity of users' social relations is necessary to cultivate relational autonomy. This calls for elucidating how moral responsibility is distributed between CMPs and companies that collect user data—which requires, at a minimum, highlighting the crucial role that CMPs play and their potential for improving conditions for valid consent—but this also includes abandoning the data-as-property paradigm. Data may be definitionally "personal" under the GDPR, but even personal data are employed by artificial intelligence models that deploy the logic of homophily to develop inferences about others (Chun, 2021). Thus, personal data effectively construct new relations that also affect relational autonomy of more than one individual at a time, supporting calls for social data governance (Viljoen, 2021).

In sum, CMPs can be understood to produce two types of error. On one level, CMPs produce *consent errors* by failing to uphold the conditions of valid consent. On another level, CMPs produce *relationship errors* by undermining the integrity of users' relationships. These perspectives operationalize different conceptualizations of autonomy: the former fails to *respect* autonomy as an individual attribute as presumed by liberal philosophy, whereas the latter fails to *cultivate* autonomy as a relational construct as defined in feminist philosophy. I have argued that the latter approach—centering relational analysis—is analytically and functionally valuable because it repudiates property thinking while pointing to solutions that lean into rather than abandon the social nature of both autonomy and datafication. Reconceptualizing consent error as relationship error is thus a crucial step for developing data governance strategies that account for—and respect—the social relations mediated by datafication.

References

Ahuja, S., & Kumar, J. (2022). Conceptualizations of user autonomy within the normative evaluation of dark patterns. *Ethics and Information Technology*, *24*(4), 52. doi:10.1007/s10676-022-09672-9

Beauchamp, T. L., & Faden, R. R. (1986). *A history and theory of informed consent*. Oxford, UK: Oxford University Press.

Bollinger, D., Kubicek, K., Cotrini, C., & Basin, D. (2022). Automating cookie consent and GDPR violation detection. *Proceedings of the 31st USENIX Security Symposium*. Retrieved from https://www.usenix.org/conference/usenixsecurity22/presentation/bollinger

Bouhoula, A., Kubicek, K., Zac, A., Cotrini, C., & Basin, D. (2024). Automated large-scale analysis of cookie notice compliance. *Proceedings of the 33rd USENIX Security Symposium*. Retrieved from https://www.usenix.org/conference/usenixsecurity24/presentation/bouhoula

Chun, W. H. K. (2021). *Discriminating data: Correlation, neighborhoods, and the new politics of recognition*. Cambridge, MA: MIT Press.

Cohen, J. E. (2021, March 23). *How (not) to write a privacy law*. Retrieved from https://knightcolumbia.org/content/how-not-to-write-a-privacy-law

Dougherty, T. (2015). Yes means yes: Consent as communication. *Philosophy & Public Affairs*, *43*(3), 224–253. doi:10.1111/papa.12059

Hartzog, W. (2017). The inadequate, invaluable Fair Information Practices. *Maryland Law Review*, *76*(4), 952–983.

Hurd, H. (1996). The moral magic of consent. *Legal Theory*, *2*(2), 121–146. doi:10.1017/S1352325200000434

Jones, M. L., & Kaminski, M. E. (2020). An American's guide to the GDPR. *Denver Law Review*, *98*(1), 93–128.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network theory*. Oxford, UK: Oxford University Press.

Mackenzie, C., & Stoljar, N. (2000). Introduction: Autonomy reconfigured. In C. Mackenzie & N. Stoljar (Eds.), *Relational autonomy: Feminist perspectives on autonomy, agency, and the social self* (pp. 3–31). Oxford, UK: Oxford University Press.

Matte, C., Bielova, N., & Santos, C. (2020). Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB Europe's transparency and consent framework. *2020 IEEE Symposium on Security and Privacy*, 791–809. doi:10.1109/SP40000.2020.00076

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 1–13. doi:10.1145/3313831.3376321

Stöver, A., Gerber, N., Cornel, C., Henz, M., Marky, K., Zimmermann, V., & Vogt, J. (2022). Website operators are not the enemy either—Analyzing options for creating cookie consent notices without dark patterns. *Mensch und Computer 2022—Workshopband*. doi:10.18420/muc2022-mci-ws01-458

Viljoen, S. (2021). A relational theory of data governance. *Yale Law Journal, 131*(2), 573–654.