A View From Somewhere: Shifting Expertise in Identifying and Evaluating Dark Patterns

Rohan Grover

University of Southern California, Los Angeles, California, United States

Abstract

Regulatory responses to dark patterns often rely on expert assessments of design interfaces to evaluate whether users are being subjected to manipulation or deception. In this article, I unpack expert assessments of dark patterns used to solicit user consent and argue that regulatory action should explicitly reckon with questions about whose expertise is consulted. I conclude by discussing how deliberative mechanisms can be valuable for expanding the range of both experts and modes of expertise in identifying, evaluating, and ultimately regulating dark patterns.

Keywords

consent, dark patterns, data privacy, expertise, feminist theory

1. Introduction

You click on a link to a news article. A new tab opens in your browser and a web page renders. You begin reading the headline when a pop-up module appears, obscuring the text. The module confronts you with a menu of toggle switches about various types of cookies. Strictly necessary: on or off? Analytics: on or off? Functional? Personalization? Performance? Some are selected by default, others are not. Reading all the fine print on this module would be onerous. You glimpse a line that says, "blocking some types of cookies may impact your experience on the site…." It seems necessary to agree with everything in order to move on and read the article—just like agreeing to privacy policies or terms of service—and you don't want a subpar experience, so you click "accept all" and move on.

Or perhaps you don't. Perhaps you recognize that this is a case of obstruction—a kind of dark pattern—because these cookies are truly optional. Perhaps you are aware of the right to make an independent decision about your consent and that your decision cannot be used to diminish your website experience, as stipulated by your local data protection law.

Prior research has demonstrated that socioeconomic factors may correlated with the likelihood that you fall into one category or the other. For example, scholars have conducted surveys to find that age, education, income, and race may predict digital literacy and privacy behavior in some contexts [1, 2]. These are important findings that can be used to prioritize marginalized

Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practices Workshop at CHI Conference on Human Factors in Computing Systems, May 12, 2024, Honolulu, HI (Hybrid Workshop)

rohan.grover@usc.edu (R. Grover)

https://www.rohangrover.org/ (R. Grover)

0000-0002-9042-8259 (R. Grover)

perspectives and experiences in identifying and curbing manipulative and deceptive design practices.

One explanation for disparate outcomes is that individuals lack access to information and skills to develop informed decisions about online privacy—in other words, they lack privacy literacy [3]. According to this framework, based on the knowledge gap hypothesis, increasing individuals' knowledge of online privacy will improve their privacy behaviors and outcomes [4]. Some examples of categories of knowledge that contribute to online privacy literacy include awareness of technical aspects of data collection, about laws related to data protection, and about user strategies for exercising privacy [3].

This framework is premised on a rational model of privacy behavior: new, relevant knowledge will lead to better informed decisions. However, empirical evidence also suggests that a sufficient level of privacy literacy may never be attainable because it simply may not exist given the rapid development of new technologies and design practices. For example, a nationally representative survey in the US demonstrated that individuals lacked the knowledge to meaningfully consent to data collection, raising the question of whether consent can and should continue to serve as a legally valid basis for companies to collect personal data [5]. In other words, privacy literacy may be so deficient that there is little hope that the public can ever catch up.

The framework is also premised on a contested understanding of privacy as an individual value. Instead, privacy scholars have advocated for recognizing privacy as a fundamentally social phenomenon–especially in the case of information privacy [6, 7, 8, 9, 10]. Indeed, scholars have argued that individualizing privacy—both as a right and as a behavioral prescription—capitulates to the depoliticizing impulse of "digital resignation" [11, 12] cultivated by the architecture of contemporary "platform societies" [13, 14, 15]. These critiques suggest that solutions should not necessarily be found in training or empowering individuals but rather in addressing structural conditions.

These latent values and assumptions are embedded in how the opening anecdote was framed–as a case of individual responsibility and deficient literacy. But this interpretation is not inevitable. What might an alternative reading look like?

In this article, I argue that evaluating and explicitly accounting for expertise can help address the contested premises of the privacy literacy model in identifying, evaluating, and ultimately regulating dark patterns. This intervention responds to regulatory models that often rely on expert assessments of design interfaces to evaluate whether users are being subjected to manipulation or deception. Specifically, I examine and unpack expert assessments of user consent by drawing on two bodies of scholarship—evaluating technical expertise and feminist analysis of consent—and then I outline an emergent model for governing dark patterns based on deliberative mechanisms. I conclude by arguing that regulatory action should explicitly reckon with questions of *whose* expertise-and in what form-is consulted and included by HCI scholarship and policy advice.

2. The Relevance of Expertise

Expertise is a complex analytic developed largely by sociologists and science and technology studies (STS) scholars to account for various experiences and controversies over claims to

(especially scientific) knowledge. An intuitive understanding—which largely aligns with the definition of privacy literacy above—may interpret expertise to be specialized knowledge, skills, or abilities in a particular domain possessed by an individual. However, this definition has been scrutinized and subjected to symmetrical analysis by also understanding expertise as a social construction. The latter conceptualization has helped scholars consider how and whether expertise can and should be democratized and deconstructed by, for example, evaluating scientific knowledge on the same terms as other forms of knowledge. Altogether, however, prior literature does not agree on a single definition that captures what expertise is as much as it has demonstrated various ways in which expertise is a valuable tool to expand and refine analysis. These debates have also opened up distinct but related normative questions about what the role of expertise should be. In this section, I identify key elements of this debate and demonstrate how they can be applied to privacy literacy and governing dark patterns.

One key distinction in understanding expertise is identifying it as either an attribute or an attribution. As an *attribute*, expertise refers to knowledge, skills, or abilities (henceforth, "capabilities") in a specific domain that can be possessed by an individual or community, similar to the definition of privacy literacy described previously. Meanwhile, as an *attribution*, expertise refers to a qualification recognized by others; it is thus a fundamentally relational dynamic that depends on social recognition rather than objective or abstract truth [16]. In other words, these approaches differ by locating expertise either "inside" or "outside" individuals [17].

In the case of dark patterns, both definitions help to understand how expertise has been operationalized in prior research, albeit implicitly. On one hand, content analyses of interfaces often rely on credentialed researcher teams who draw on their domain knowledge to identify whether design patterns qualify as manipulate or deceptive or not [18, 19, 20, 21, 22, 23]. On the other hand, user studies and experimental research identify dark patterns based on participants' experiences and behaviors [24, 25, 26, 27, 28, 29, 30]. Thus, it appears that both kinds of expertise–an as attribute organically possessed by all people and as an attribution earned through recognition for relevant experience–are valued in empirical research on dark patterns.

However, the question of which of these sources of expertise should be solicited, included, and prioritized in research, governance, and policy is a key decision for HCI and policy communities. On one level, it may be consequential in terms of leading to different outcomes: do users' and experts' assessments align? Which users, specifically? Can users' experiences be automated through algorithmic or AI systems at scale?

In addition, distinguishing between the two approaches to expertise can be consequential for how and whether the public(s) is included. This is especially true when non-expert communities disagree with expert assessments by asserting different forms of knowledge that are not recognized as credentialed expertise [31]. A classic example is from the 1980s when AIDS activists asserted their "lay expertise"–such as their familiarity with norms and practices among patient communities that deviated from researchers' expectations–to influence clinical trials, ultimately working together with research teams to develop more robust and efficacious trials [32]. In that case, patients had to invest in acquiring cultural competence by developing interactional practices, learning new vocabulary, and accessing conferences so that credentialed medical practitioners would take seriously their experiences and perspectives. Thus, "lay expertise" can be a key source of local, embodied, subjective, or experiential knowledge, and either including or excluding lay expertise carries epistemic and political implications.

One way to address the potential value of lay expertise is to measure expertise not by an individual's credentials but rather according to the content of their knowledge. Harry Collins and Robert Evans's framework distinguishes expertise based on different forms of knowledge—without referring to lay people or experts but rather to ubiquitous and specialist knowledge and expertise [16]. In the first level, they distinguished ubiquitous expertise from specialist expertise. Ubiquitous expertise refers to capabilities possessed by all members of a society, such as natural language communication. Specialist expertise is further divided into the categories of ubiquitous knowledge, interactional expertise, and contributory expertise. Ubiquitous knowledge refers to "low levels" of knowledge that is ascertainable through activities such as reading or memorizing but don't require immersive experience. This includes information that could be studied and evaluated in a game of trivia or the ability to recite facts about theoretical physics after reading an article in the popular press. Interactional expertise, on the other hand, is "the ability to master the language of a specialist domain in the absence of practical competence" (p. 14). For example, a scholar may be able to peer review a journal manuscript even if it is only adjacent to their area of specialty but not overlapping. Finally, contributory expertise is "what you need to do an activity with competence" (p. 14) that is accepted by a mutually recognized community of experts.

Collins and Evans's framework can serve as a rubric to evaluate privacy literacy as it relates to detecting dark patterns. Privacy literacy is generally not a low-level form of ubiquitous expertise or ubiquitous knowledge because, by definition, it is not an intuitive capability naturally available to all people. Instead, it requires some education and training. This likely qualifies as a form of interactional expertise, which is developed and assessed by meeting standards and expectations. However, these expectations are not created in a vacuum; they are "developed through socialization into a collectivity of expert practitioners, with the performance judged by, and held accountable to, the standards of the relevant peer community" (p. 767) [16]. Thus, while privacy literacy in general has already been developed through specific mechanisms such as survey questions [3, 5], it is still being developed in the specific domain of regulating dark patterns, where a peer community is currently in formation through efforts such as the present workshop.

3. Toward "A View From Somewhere"

The contemporary moment–developing institutional structures such as standard definitions and a formalized community–is a crucial moment for intentionally defining what forms of expertise are centered in identifying, evaluating, and regulating dark patterns. After all, the definitions and standards developed in this space will implicitly set inclusion and exclusion criteria which may create barriers for particular categories of "lay" people–especially those with marginalized identities. This includes marginalized identities that are often protected by statutory law, such as age and physical ability in some jurisdictions, but also forms of marginalization such as neurodiversity, caste, and class. To be clear, in developing this analysis the intent is not to take away from the well-intentioned, analytically rigorous, and generous work pursued in the dark patterns scholarly community. Instead, the goal is to step back and call attention to questions relevant to any project or scholarly community–but especially when the opportunity and the

urgency for regulatory intervention is so imminent and broadly supported.

In addition, these questions index a broader normative question about what the role of different forms of expertise *should* be–in other words, *whose* expertise should count toward identifying, evaluating, and regulating dark patterns (and technology policy more broadly)? This question alludes to a public, political dilemma about whether expertise should be defined and used to drive technocracy–in which decisions are made by experts entrusted to exercise their unique technical knowledge–or participatory democracy–in which citizens are empowered to scrutinize authority and contribute their (lay) expertise to public debates [17].

A key concern about upholding professionalized technical expertise–and the technocracy model in general–is that standards and definitions may be devitalized by structural power dynamics such as corporate incentives for data accumulation. For example, when liable companies translate data privacy laws into specific compliance procedures, the labor of interpreting ambiguous requirements is often entrusted to software developers because of their presumed technical expertise [33]. However, developers are often uncertain about how to proceed, and thus rely on standards and managerial practices set by large institutions such as platform companies that promote a vacuous interpretation of privacy to avoid disrupting their business models that rely on nearly indiscriminate data collection [34]. For example, Alice Marwick has identified the International Association of Privacy Professionals (IAPP) as an institutional actor that has professionalized privacy work by developing norms, standards, and accreditation resources that transform complex values about privacy into managerial procedures and project management practices [35]. Marwick identities this perspective as a "view from nowhere" that perpetuates existing power dynamics that favor corporate, institutional actors over shifting structural relations.

In this article, I take up this claim as a charge to uphold a situated analysis–a *view from somewhere*–with explicit, intentional sensitivity to expertise and, by extension, power and public participation. I argue that such an approach is crucial for defining whose expertise, and in what form, will guide the identification and evaluation of dark patterns. Of course, *where* that "somewhere" is located can originate from various theoretical perspectives with different implications. Thus, in the following section, I discuss how feminist analysis of consent draws attention to embodied subjectivity as a source of expertise.

4. Feminist Analysis of Consent

Soliciting individuals for valid consent is a key, commonly used mechanism for collecting personal data that is permitted by data privacy laws such as the General Data Protection Regulation (GDPR). In response, scholars have pursued empirical evaluations through algorithmic audits and user studies of consent interfaces to determine whether the consent they collect is "valid" and what are the resulting implications for user outcomes [25, 36, 37]. Collectively, these studies illustrate a specific kind of expertise about what constitutes valid consent: an abstract, formalized, often binary condition that can be evaluated at scale and through automated means. Such studies have been instrumental for helping regulators identify targets for enforcement action, but they represent a limited analysis of consent.

Feminist scholars have long explored and unpacked consent as an analytic and argued that

consent is not a stable, discrete, binary, individual choice but rather a structural relation rooted in subjectivity [6, 38, 39, 40, 41, 42, 43, 44, 45]. For example, this has been applied to develop a model of affirmative consent, such as the FRIES model, which was developed by Planned Parenthood and defines "affirmative consent" according to five criteria: freely given, reversible, informed, enthusiastic, and specific. Scholars and practitioners alike have advocated for adopting the FRIES model to build and design *consentful* technologies and policy [44, 46].

This conceptualization of consent shifts the nature of expertise from a rational abstraction to an embodied subjectivity. For example, algorithmic methods evaluating consent interfaces at scale and through automated means cannot meaningfully assess whether a design interface solicits consent that is enthusiastic. This exemplary criterion of the FRIES model illustrates how the impulse to evaluate consent at scale displaces embodied, subjectively affective experiences of consent. In other words, algorithmic audits foreclose user subjectivity by focusing exclusively on the accuracy of transmission and generally disregarding how consent traverses contexts and mediates relations beyond users and their data–in other words, privacy as a social phenomenon, as discussed previously. By emphasizing invalid consent at scale, then, algorithmic audits of data privacy laws privilege institutional actors over users and their subjective, contextual, embodied relationships to personal data.

Some may argue that a "higher" standard of valid consent imposes excessive burden on regulatory possibilities. However, the FRIES model is not necessarily a higher standard but rather a model of consent founded on an altogether different premise. This can be seen through each model's relationship to expertise. A model of valid consent based on formal rules and algorithmic evaluation understands consent as an explicit, abstract phenomenon, whereas the FRIES model understands consent to be fundamentally tacit and practical; in other words, consent is experiential, relational, and social. Another fundamental difference is that the FRIES model is uniquely sensitive to structural conditions. Algorithmic audits and studies at scale address structural inequalities by evaluating differential outcomes across socioeconomic demographic categories, especially protected categories such as race, age, or gender. However, the FRIES model seeks to address structural injustice by holistically evaluating the quality of consent according to its embodied integrity rather than simply the efficiency of its outcomes.

5. Conclusion

In this article, I have argued that the social construction of expertise is a relevant question that merits scrutiny and debate among the professional community(ies) advocating for regulatory action about dark patterns. I discussed several dimensions of expertise, including whether it is an attribute or attribution, whether expertise is assigned according to mutual recognition from an expert community or if it can be found within individuals, including "lay" people, and whether the nature of relevant expertise is best represented through formal logic amenable to algorithmic detection or as an experiential, relational, social phenomenon. I argued that the stakes for defining expertise thoughtfully and intentionally are made clear by the open question of whether standards and governance frameworks will perpetuate or reconfigure power relations–in other words, whether they constitute "a view from nowhere" [35] or, alternatively, a view from somewhere–and if so, *where*?

To answer this question, I drew on feminist analysis of consent to advocate for considering what the governance of dark patterns may look if it is based on alternative sites of expertise. In particular, I argued that the FRIES model demonstrates how expertise can be found in embodied subjectivity and affective experience in the context of sexual consent. Notably, the model is applicable to individual interpersonal relationships and is not easily scalable. To some extent, refusing scalability is part of the point of foregrounding the FRIES model. It is necessarily contingent, relational, and dynamic.

But on a practical level, in terms of regulatory governance, this argument points to opportunities beyond standards for automated detection. For example, under the FRIES model, consent is reversible and enthusiastic. In practice, these criteria necessitate a continuous, relational dialogue among the involved actors. Consent is not a binary variable that can be switched on in perpetuity. Instead, it is a contingent condition of the relationship among actors. Thus, identifying violations of consent cannot be reduced to tracing the decision point and assessing the validity of the initial consent decision. Instead, its continuous legitimacy must be agreed upon through discovery.

What might this look like for the regulation of dark patterns? Rather than developing universal standards, a feminist analysis of expertise and consent may suggest a deliberative approach to identification and evaluation. For example, dark patterns could be identified by juries constituted by the public and/or civil society organizations that represent different marginalized perspectives. Such a model would locate expertise in the experiences of various public(s) rather than the privacy literacy or technical proficiency of individual technocrats. Such a model would constitute "a view from somewhere"–and would locate the "somewhere" in the experiences of marginalized identities to contest structural power relations in technology companies and interfaces.

References

[1] M. Madden, M. Gilman, K. Levy, A. Marwick, Privacy, poverty, and big data: A matrix of vulnerabilities for poor americans, Washington University Law Review 95 (2017) 53.

[2] Y. J. Park, Digital literacy and privacy behavior online, Communication Research 40 (2013) 215–236.

[3] S. Trepte, D. Teutsch, P. K. Masur, C. Eicher, M. Fischer, A. Hennhöfer, F. Lind, Do people know about privacy and data protection strategies? towards the "online privacy literacy scale" (OPLIS), in: S. Gutwirth, R. Leenes, P. de Hert (Eds.), Reforming European Data Protection Law, Springer, 2015, pp. 333–365.

[4] P. K. Masur, How online privacy literacy supports self-data protection and self-determination in the age of information, Media and Communication 8 (2020) 258–269. doi:10.17645/mac.v8i2.2855.

[5] J. Turow, Y. Lelkes, N. A. Draper, A. E. Waldman, Americans can't consent to companies' use of their data, International Journal of Communication 17 (2023) 4796–4817.

[6] J. E. Cohen, Configuring the Networked Self: Law, Code, and the Play of Everyday Practice, Yale University Press, 2012.

[7] H. Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford University Press, 2009.
[8] A. E. Waldman, Privacy as Trust: Information Privacy for an Information Age, Cambridge University Press, 2018.
[9] D. J. Solove, Understanding Privacy, Harvard University Press, 2010.
[10] H. Nissenbaum, Privacy as contextual integrity, Washington Law Review 79 (2004) 119–158.
[11] N. A. Draper, J. Turow, The corporate cultivation of digital resignation, New Media & Society 21 (2019) 1824–1839. doi:10.1177/1461444819833331.
[12] S. Gürses, A. Kundnani, J. Van Hoboken, Crypto and empire: The contradictions of counter-surveillance advocacy, Media, Culture & Society 38 (2016) 576–590. doi:10.1177/0163443716643006.
[13] P. Helm, S. Seubert, Normative paradoxes of privacy: Literacy and choice in platform societies, Surveillance & Society 18 (2020) 185–198. doi:10.24908/ss.v18i2.13356.
[14] N. Srnicek, Platform Capitalism, John Wiley & Sons, 2017.
[15] D. J. Solove, The myth of the privacy paradox, The Geoge Washington Law Review 89 (2021) 1–51.
[16] H. Collins, R. Evans, Rethinking Expertise, University of Chicago Press, 2019.
[17] G. Eyal, The Crisis of Expertise, John Wiley & Sons, 2019.
[18] H. Habib, Y. Zou, A. Jannu, N. Sridhar, C. Swoopes, A. Acquisti, L. F. Cranor, N. Sadeh, F. Schaub, An empirical analysis of data deletion and {Opt-Out} choices on 150 websites, in: Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security, SOUPS'19, 2019, pp. 387–406. doi:10.5555/3361476.3361505.
[19] A. Mathur, G. Acar, M. J. Friedman, E. Lucherini, J. Mayer, M. Chetty, A. Narayanan, Dark patterns at scale: Findings from a crawl of 11k shopping websites, Proceedings of the ACM on Human-Computer Interaction 3 (2019). doi:10.1145/3359183.
[20] I. Sanchez-Rola, M. Dell'Amico, P. Kotzias, D. Balzarotti, L. Bilge, P.-A. Vervier, I. Santos, Can I opt out yet? GDPR and the global illusion of cookie control, in: Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, Asia CCS '19, 2019, pp. 340–351. doi:10.1145/3321705.3329806.
[21] T. H. Soe, O. E. Nordberg, F. Guribye, M. Slavkovik, Circumvention by design-dark patterns in cookie consent for online news outlets, in: Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society, NordiCHI '20, 2020. doi:10.1145/3419249.3420132.
[22] C. M. Gray, C. Santos, N. Bielova, M. Toth, D. Clifford, Dark patterns and the legal requirements of consent banners: An interaction criticism perspective, in: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, CHI '21, 2021. doi:10.1145/3411764.3445779.
[23] C. Matte, N. Bielova, C. Santos, Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB Europe's Transparency and Consent Framework, in: 2020 IEEE Symposium on Security and Privacy, 2020, pp. 791–809. doi:10.1109/SP40000.2020.00076.
[24] H. Habib, S. Pearman, J. Wang, Y. Zou, A. Acquisti, L. F. Cranor, N. Sadeh, F. Schaub, "It's a scavenger hunt": Usability of websites' opt-out and data deletion choices, in: Proceedings

of the 2020 CHI Conference on Human Factors in Computing Systems, CHI '20, 2020. doi:10.1145/3313831.3376511.

[25] C. Utz, M. Degeling, S. Fahl, F. Schaub, T. Holz, (Un)informed consent: Studying GDPR consent notices in the field, in: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS '19, 2019, pp. 973–990. doi:10.1145/3319535.3354212.

[26] D. Machuletz, R. Böhme, Multiple purposes, multiple problems: A user study of consent dialogs after GDPR, in: Proceedings on Privacy Enhancing Technologies, PETS '20, 2020, pp. 481–498. doi:10.2478/popets-2020-0037.

[27] P. Graßl, H. Schraffenberger, F. Zuiderveen Borgesius, M. Buijzen, Dark and bright patterns in cookie consent requests, Journal of Digital Social Research 3 (2021). doi:10.33621/jdsr.v3i1.54.

[28] C. M. Gray, J. Chen, S. S. Chivukula, L. Qu, End user accounts of dark patterns as felt manipulation, Proceedings of the ACM on Human-Computer Interaction 5 (2021). doi:10.1145/3479516.

[29] A. M. Bhoot, M. A. Shinde, W. P. Mishra, Towards the identification of dark patterns: An analysis based on end-user reactions, in: Proceedings of the 11th Indian Conference on Human-Computer Interaction, IndiaHCI '20, 2020, pp. 24–33. doi:10.1145/3429290.3429293.

[30] K. Bongard-Blanchy, A. Rossi, S. Rivas, S. Doublet, V. Koenig, G. Lenzini, "I am definitely manipulated, even when I am aware of it. It's ridiculous!" - Dark patterns from the end-user perspective, in: Proceedings of the 2021 ACM Designing Interactive Systems Conference, DIS '21, 2021, pp. 763–776. doi:10.1145/3461778.3462086.

[31] B. Wynne, May the sheep safely graze? a reflexive view of the expert-lay knowledge divide, in: S. Lash, B. Szerszynski, B. Wynne (Eds.), Risk, Environment and Modernity: Towards a New Ecology, Sage, 1996, pp. 44–83.

[32] S. Epstein, The construction of lay expertise: AIDS activism and the forging of credibility in the reform of clinical trials, Science, Technology, & Human values 20 (1995) 408–437. doi:10.1177/016224399502000402.

[33] R. Grover, Encoding privacy: Sociotechnical dynamics of data protection compliance work, in: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, CHI '24, 2024. doi:10.1145/3613904.3642872.

[34] A. E. Waldman, Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power, Cambridge University Press, Cambridge, UK, 2021.

[35] A. Marwick, Privacy without power: What privacy research can learn from surveillance studies, Surveillance & Society 20 (2022) 397–405. doi:10.24908/ss.v20i4.16009.

[36] H. Habib, M. Li, E. Young, L. Cranor, "Okay, whatever": An evaluation of cookie consent interfaces, in: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, CHI '22, 2022. doi:10.1145/3491102.3501985.

[37] M. Nouwens, I. Liccardi, M. Veale, D. Karger, L. Kagal, Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence, in: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, CHI '20, 2020. doi:10.1145/3313831.3376321.

[38] R. Bauer, Queer BDSM Intimacies: Critical Consent and Pushing Boundaries, Springer,

2014.
[39] J. E. Cohen, What privacy is for, Harvard Law Review 126 (2012) 1904.
[40] A. Fanghanel, Asking for it: BDSM sexual practice and the trouble of consent, Sexualities 23 (2020) 269–286. doi:10.1177/1363460719828933.
[41] J. Friedman, J. Valenti, Yes Means Yes!: Visions of Female Sexual Power and a World Without Rape, Seal Press, 2019.
[42] J. Im, J. Dimond, M. Berton, U. Lee, K. Mustelier, M. S. Ackerman, E. Gilbert, Yes: Affirmative consent as a theoretical framework for understanding and imagining social platforms, in: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, CHI '21, 2021. doi:10.1145/3411764.3445778.
[43] A. Kovacs, T. Jain, Informed Consent-Said Who? A Feminist Perspective on Principles of Consent in the Age of Embodied Data, Report, Data Governance Network, 2020.
[44] Y. Strengers, J. Sadowski, Z. Li, A. Shimshak, F. 'Floyd'Mueller, What can HCI learn from sexual consent? A feminist process of embodied consent for interactions with emerging technologies, in: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, CHI '21, 2021. doi:10.1145/3411764.3445107.
[45] J. T. Theilen, A. Baur-Ahrens, F. Bieker, R. Ammicht Quinn, M. Hansen, G. González Fuster, Feminist data protection: An introduction, Internet Policy Review 10 (2021) 1–26. doi:10.14763/2021.4.1609.
[46] U. Lee, D. Tolliver, Building Consentful Tech, Report, Allied Media Projects, 2017.