internet democracy project

DGN Policy Brief 11

March 2021

Data Governance Network
Anchored by IDFC Institute

Informed Consent - Said Who? A Feminist Perspective on Principles of Consent in the Age of Embodied Data

Anja Kovacs and Tripti Jain

Consent continues to be a crucial element of data protection regimes around the world. However, as a tool to promote and protect individuals' autonomy, it has been diagnosed with numerable weaknesses. While there have been suggestions that it is therefore time to move away from consent altogether, we propose a different approach. Data protection regimes first need to reconceptualise the nature of data, by recognising the need to centre bodies in debates on data governance. Once the entanglement between bodies and data has been acknowledged, data governance regimes can, then, adopt feminist principles of consent that build on insights developed in numerous offline contexts and which allow us to imagine data relations that enable people to actually move closer to the ideal of meaningful consent.

Context

Despite the centrality of consent in data protection regimes, criticisms of consent regimes are on the rise. Weaknesses of current consent regimes are believed to vary from cognitive or perception problems, to systemic or structural problems that individuals can do little to address (Solove, 2013), and include inadequate notices, consent fatigue, “take it or leave it” contracts, unclear data sharing arrangements with third parties, and consent's function as an enabler of purely data driven business models, among others.

Common to all these weaknesses is the construction of data as a resource. Not altogether different from any material resource that can be traded, this construction has made it possible for data to be reduced to merely a means of exchange, enabled in contract by consent. If data-driven entities are able to engage with impunity in the appropriation of our data (Zuboff, 2019), the portrayal of our data as a fair consideration for the services or products that these companies (and, increasingly, governments) supposedly provide to individual users has been essential to the proliferation of these practices.

Consent can be rescued from this quagmire, however, by putting bodies back into the data debate. After all, as - with the datafication of even the most intimate aspects of our lives - more and more decisions that affect our physical bodies are taken on the basis of our data bodies, the distinction between our physical bodies and virtual bodies is becoming irrelevant (van der Ploeg, 2012). As a consequence, we increasingly experience data as an extension of our bodies, and even an integral part. Once we recognise this close entanglement between our bodies and our data, we can turn to existing areas of research in which questions of consent and the body have figured strongly, for guidance on how to strengthen consent regimes.

One particularly rich area of such discussions has been that of sexual consent in feminism. It is to this that we turn our attention next.

Strengthening Consent: A Feminist Perspective

In their explorations of consent in the context of sexual relations, feminists have highlighted that, rather than an expression of the will of autonomous and equal individuals, consent in practice is fundamentally embedded in power relations that, legally and/or socially, construct some as free and equal, and others as less so. The consent of the latter is then irrelevant or always already assumed. Against this background, feminists have suggested a number of central ways over the years to strengthen consent. Of particular relevance here are the following:

- **Consent must be embedded in a notion of relational, rather than individual, autonomy:** to be meaningful, consent needs to be conceptualised in far broader terms which include, among other things, an assumption of responsibility between individuals and mutuality of relationships.
- **Consent must be given proactively, communicated in the affirmative,** i.e. the partner initiating the act will be required to prove beyond a doubt that they have sought consent and to demonstrate that consent was expressed.

- **Consent must be specific, continuous and ongoing:** it cannot be assumed to be a blanket "yes" for the whole act; it is to be sought for different acts and at different stages, it is required to be built.
- **Consent is a process:** it opens up a conversation, rather than entailing merely a yes/no decision.
- **Consent allows for negotiation by all parties involved:** each party shall have the ability to say no as well as to provide input on the terms of agreement.
- **Conditions must be created so that consent can be given freely:** to be able to give consent freely, the person should be free from any fear or experience of oppression or violence of any kind in the context in which consent is sought.

Lessons from Feminist Perspectives on Consent for Data Protection

At first sight, it may appear that some of these feminist principles are already integrated in data protection regimes - in particular those that specify that consent should be free, informed, specific, easy to withdraw and affirmative. However, while paying lip-service to them, current data protection regimes do not translate these principles into practice in a substantive manner. This is both because these frameworks continue to conceptualise data as a resource, rather than as an extension of our bodies, and because they are, at least in part as a consequence, oblivious to the relational nature of the autonomy of those whose consent is sought and the structural obstacles that they face. To strengthen the quality of consent, the consent qualifiers in data governance, thus, need to undergo a sea change.

Recommendations

At least three different types of changes need to be made. While it may not be possible to present in detail all that would be required, it is possible to propose a number of changes that should be made immediately for each type:

1. Changes required at the time when data is collected

At present data protection regimes often contain the principles of data minimisation and purpose limitation. However, such purposes have been decided by the data controller, either state actors or non-state actors, rather than the individual seeking to buy a product or use a service, and in the age of surveillance capitalism, their purposes are rarely aligned with those that the user has in mind (Zuboff, 2019). Thus, the following changes are among those that are essential:

- An end should be put to deceptive and opaque practices that disable people from understanding the discrepancy between the data controller's purposes and their own as a user when their consent is being sought, and that thus result in the specificity of that consent being undermined.
- Data controllers should not be allowed to process the personal data of individuals for "certain reasonable purposes" not explicitly mentioned in their privacy policies.
- State and non-state actors should not be allowed to change privacy policies unilaterally, with users only provided with the option to agree or stop using the service.
- The State should provide notice to users for all essential purposes other than security of the State (thus including for the provision of essential services and in emergencies), because notice can be a tool to improve transparency and ask for accountability concerning governments' data collection efforts. For non-essential purposes, such as research, consent should be sought separately, and these purposes should be clearly and narrowly defined.
- Users should be able to deny consent to any practice that doesn't relate narrowly to the service being provided, without being forced to stop using the service. This includes when consent for non-essential purposes is being sought by the State.
- In general, data governance policies need to demarcate more narrowly situations in which the requirement to provide notices and seek consent can be done away with in the first place.
- Users should have the right to access and correct their data.

2. Changes required to what are permissible uses of collected data

Where mechanisms to negotiate exist, they currently seem to focus squarely on the data that the user shares with the data controller; negotiation in terms of what the data controller does with this data for the moment is impossible. Thus, a second set of changes are required to ensure that we will never even be asked to consent to currently prevalent malpractices. The following practices should no longer be legal:

- Business and governance models that seek profit or to boost surveillance capacity from analysing behavioural surplus, including for welfare purposes. The only exception can be where there is public debate, subsequently translated into law, that this serves the public good.
- Practices which deny users the possibility to object to third party data sharing, yet refuse to take up any responsibility for harms that may accrue to the user following such data sharing or, equally damaging, simply presume that consent implies consent to the terms and conditions of all these third parties as well.
- Practices of selling citizens' raw and aggregated data, including behavioural surplus, by governments and the private sector, and whether to private or public entities.
- Data sharing by government, including *among* government departments, for any purposes other than essential ones, such as the provision of the service requested and to which this data relates.

3. Changes required to especially protect people who are particularly vulnerable

While the above are changes that are required to protect all of us, for some people, in some situations, additional protections may be required. For example, where data is collected as part of the employer-employee relationship, people might be in a situation of decisional vulnerability as there is a clear power imbalance between themselves and those collecting the data (Jain et al., 2020).

Luna (2019) proposes that we pay attention to two factors when assessing vulnerability and determining whether additional protections might be required: the likelihood of risks and the harmfulness of effects. Where consent is concerned, this may lead to additional protections for these vulnerable individuals and groups both where the collection of data and the use of data are concerned - as is currently already being done for children.

References

Jain, Tripti, Kovacs, Anja & Ranjit, Tanisha (2020). *Submission to the Joint Parliamentary Committee on the Personal Data Protection Bill 2019.* Internet Democracy Project.

Luna, Florencia (2019). Identifying and evaluating layers of vulnerability: A way forward. *Developing World Bioethics,* 19(2), 86-95. DOI: 10.1111/dewb.12206

Solove, Daniel J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review,* 126(7), 1880-1903. https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf

van der Ploeg, Irma (2012). The body as data in the age of information. In Kirstie Ball, Kevin Haggerty, & David Lyon (Eds.), *Routledge Handbook of Surveillance Studies* (pp. 176-185). Routledge.

Zuboff, Shoshana (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* Profile Books

Data Governance Network

The Data Governance Network is developing a multi-disciplinary community of researchers tackling India's next policy frontiers: data-enabled policymaking and the digital economy. At DGN, we work to cultivate and communicate research stemming from diverse viewpoints on market regulation, information privacy and digital rights. Our hope is to generate balanced and networked perspectives on data governance - thereby helping governments make smart policy choices which advance the empowerment and protection of individuals in today's data-rich environment.

About Us

The Internet Democracy Project works towards realising feminist visions of the digital in society, by exploring and addressing power imbalances in the areas of norms, governance and infrastructure in India and beyond.

About the Authors

Dr. Anja Kovacs directs the Internet Democracy Project. Her current research focuses on questions regarding data governance, surveillance and cyber security, and regarding freedom of expression - including work on gender, bodies, surveillance, and dataveillance, and gender and online abuse. She has also conducted extensive research on the architecture of Internet governance. Anja has lectured in the UK, India and Brazil and has worked as an international consultant on Internet issues, including for the United Nations Development Programme in Asia and the Pacific. Having previously been a Fellow at the Centre for Internet and Society in Bangalore, she is currently a CyberBRICS Non-Resident Fellow at the Fundação Getulio Vargas (FGV), Rio de Janeiro. She obtained her PhD in Development Studies from the University of East Anglia in the UK, and has conducted extensive fieldwork across South Asia.

Tripti Jain is a researcher at the Internet Democracy Project for the Bodies and Data Governance Project. Her responsibilities include planning, conducting, and presenting research. Prior to joining the Internet Democracy Project, Tripti was a counsel at Sflc.in. She was managing their Internet Shutdowns project and was involved in various projects that included research and advocacy on issues such as privacy, snd civil rights on the Internet. Tripti is a lawyer by education.

Acknowledgments

This policy brief draws on a paper with the same title by Anja Kovacs and Tripti Jain. The policy brief was prepared by Tripti Jain and Anja Kovacs.

Disclaimer and Terms of Use

The views and opinions expressed in this paper are those of the authors and do not necessarily represent those of the Internet Democracy Project.

IDFC Institute

301, 3rd Floor, Construction House 'A', 24th Road, Off Linking Road,
Khar West, Mumbai 400052

/idfcinstitute @idfcinstitute /IDFCInstitute