User Consent for Data Processing: GDPR as a Paradigmatic Neoliberal Device

https://www.e-ir.info/2022/07/06/user-consent-for-data-processing-gdpr-as-a-paradigmatic-neoliberal-device/

IVAN MANOKHA, JUL 6 2022

Since its entry into force in May 2018, the General Data Protection Regulation (GDPR) of the European Union (EU) has acquired the status of a 'gold standard' for the protection of personal data, a view that is shared by a myriad of commentators (academics, journalists, IT specialists, civil society activists and think tanks, as well as numerous supervisory authorities). Some observers suggest that the GDPR constitutes the realisation of the idea of a 'new Magna Carta' for the web, while yet others argue that it launched a 'New Digital World Order' and thereby represents 'one of the greatest achievements' of the EU. Such dithyrambic assessments are regularly reinforced by announcements of large fines for non-compliance – at least 963 since 2018 – levied on various corporations, including the biggest tech companies, that are usually highly mediatized, which further bolsters the status of the GDPR as a model mechanism for data protection. In the light of such a widespread acclaim of the GDPR, it is not surprising that it has served as a model for similar legislation in Brazil, Japan, South Korea, Switzerland, Turkey, Mauritius, Chile, South Africa, Argentina, Kenya and others. Regulations that are seen as coming closest to the benchmark set by the GDPR are characteristically referred to as 'GDPR-light' (e.g. the California Consumer Privacy Act or the Swiss Federal Data Protection Act), thereby strengthening the status of the GDPR as an uncontested world standard.

The key stipulations of the Regulation concern the legal basis for gathering and processing personal data (Articles 5-11). Central here is the provision that "processing shall be lawful only if … *the data subject has given consent* to the processing of his or her personal data for one or more specific purposes" (Article 6). Concerning the nature of consent, Article 7 states that organisations seeking to gather personal data should formulate the request for consent "in an intelligible and easily accessible form", while individual consent itself, as explained in Recital 32, "should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data". It further stipulates that consent "could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data".

What this means is that the GDPR effectively places the responsibility for assessing and managing potential risks to their privacy on individual users. Such shifting of responsibility for their well-being on individuals themselves is one of the key aspects of neoliberal governance.

Neoliberalism: Enterprising and Self-Reliant Subjects

One of the central characteristics of neoliberalism is 'government at a distance' (Rose, 1999): first, the role of the state is confined to creating *a legal framework* for competitive markets to operate, without directly intervening into their functioning; second, the responsibility for their well-being and for managing various risks is devolved to individuals themselves. In particular, through the liberalization of the labour market, the neoliberal state compels more and more individuals to start behaving as 'enterprises' seeking to enhance their 'human capital' and competitiveness. As the philosopher Michel Foucault notes, here resides one of the key differences between classical liberalism of the nineteenth century and neoliberalism: "the classical liberal conception of homo

œconomicus as the partner of exchange is fundamentally transformed; homo œconomicus becomes "an entrepreneur of himself, …being for himself his own capital, … his own producer, … the source of [his] earnings" (Foucault, 2008, 226). At the same time, through reducing various social protections, the neoliberal state forces individual citizens to assume greater responsibility for managing risks related to physical and mental health, housing, education, retirement, and other fields that used to be predominantly collective responsibilities. As Zigmunt Bauman observed, those who fail to assume such responsibilities are only themselves to blame: "if they fall ill, it is because they were not resolute in following a health regime; if they stay unemployed, it is because they failed to learn the skills of winning an interview" (in Brown and Baker, 2012, 25). In short, neoliberal governance relies on indirectly shaping citizens' subjectivities to become more self-reliant and to align their self-regulating capacities to neoliberal norms.

In practice, user consent defined by the GDPR as a 'clear affirmative action' takes the form of a mechanical ticking of a box or clicking the 'Accept' button of various terms of service (TOS), cookies policies, privacy policies, etc. of service providers before users can access the service in question. As numerous studies have demonstrated, "no one has ever read a privacy notice who wasn't paid to do so" (Schwartz and Peifer, 2017, 150), and 99% of users accept these agreements without ever consulting them (ProPrivacy, 2020).

This is not a 'privacy paradox' – a concept often used (see Kokolakis, 2015) to describe the fact that while most individuals state that privacy is of paramount importance to them, virtually no one takes the necessary measures to protect it – but an outcome of structural power relations that characterize neoliberalism.

On the one hand, following neoliberal reforms, individual workers are compelled to work more intensely, and often to be available during irregular hours and even on a 24/7 basis, which, alongside increased responsibilities that they are forced to assume to manage their well-being, limits the time and resources that they could allocate to studying and trying to make sense of different TOS and privacy policies. In addition, many users – in particular 'gig' workers that depend on various platforms for their income – simply cannot afford to reject the TOS of these services.

On the other hand, the GDPR confers the right to draft these agreements on service providers themselves, and thereby enables them to dictate the conditions of their services – to 'stealthily' (Kim, 2013) grant themselves different rights and embed various practices – with respect to how and for what purposes they will collect user data. Indeed, these agreements constitute a variety of 'contracts of adhesion' (Patterson, 1919) – contracts that a user simply 'adheres' to because he or she has little choice as to its terms – that Kim refers to as 'clickwraps', defined as non-negotiable and 'take-it-or-leave-it' digital agreements where "one-sided legal terms are imposed upon non-drafting parties" (Kim, 2013, 39). To put it differently, various TOS and privacy policies embed and reproduce "a systemic lack of bargaining power" (Ibid, 204) that characterises the position of users. In addition, firms usually write these policies in a lengthy and complex manner, often with a lot of technical details and legalese, which requires a great deal of effort and time to read and understand. Coupled with the fact that users cannot amend or modify them in any way, this virtually eliminates any incentive to consult them. The practice of using such 'wrap' contracts obviously precedes the GDPR – it had been widely used, for example, in the insurance industry (Patterson, 1919), as well as in banking and in the consumer credit industry. When the digital revolution occurred, first in the software industry, and later in various online businesses, the firms adopted this form of agreement, which quickly became standardized and widespread. The GDPR now endorses and codifies this practice.

An Alternative – Collective Responsibility For User Privacy

To develop an alternative mechanism for personal data protection it seems necessary to begin by putting an end to its neoliberal 'outsourcing' to individuals, and by making it a *collective* responsibility, a solution that is advocated by critics of neoliberalism for other aspects of human life. Indeed, neoliberalism today is held responsible by a growing number of opponents for many different problems and failures – e.g. extensive exploitation and 'precarisation' of labour, unprecedented income inequality, poverty and social exclusion, the rise of populist ideologies, etc. – who increasingly call for a fundamental reform, for a 'New New Deal' or a 'Green New Deal', for a return of the state to regulate the economy and ensure social protection. Personal data protection clearly needs to be part of such a programme of fundamental transformations and reforms.

As regards more concrete measures, we may identify a potential way forward by building upon some of the existing initiatives and mechanisms. One of such initiatives is a Discussion Paper on Data Security released by the Australian Department of Home Affairs in April 2022. This paper has two dimensions that are worth emphasising, and that may potentially inspire the creation of alternative mechanisms for data protection. First, the paper speaks of 'collective responsibility' concerning the management of data. Although the emphasis is put on data security from cyberattacks and various malicious actors and not on user data collected by various service providers, it makes an important observation that individuals (as well private firms or public agencies), acting separately, cannot ensure data security. Instead, "data security is a *collective responsibility* where we, as a nation must remain joined up and connected on data security standards" (Australian Government: 11, emphasis added).

Second, rather than informing the public about the measures that the government intends to take in this respect, the paper has been released for public comment, that is, ordinary citizens and various stakeholders are invited to participate in the discussion concerning the measures to adopt. This is an important dimension because with a recent dramatic growth of state surveillance and the rise of a 'permanent state of exception' (Agamben, 2005) – the introduction of more and more exceptions to the exercise of different individual rights and liberties in the name of security – it seems essential not to leave it to the state alone to reform the system. Those who believe that an alternative mechanism for personal data protection is needed might borrow from this initiative: on the one hand, to extend the idea of collective responsibility for data security to the collection of user data by various platforms; on the other, to launch a public debate with the participation of policy-makers, civil society organisations, business firms and individual citizens on what would be the best solution to adopt.

In the meantime, the mandate of existing regulatory bodies and public oversight organisms to include as part of their mission the analysis and evaluation various TOS *before* they are submitted to individual users (as it is the case in other sectors, e.g. food supplements or medicines are approved before they commercialized). Another short-term improvement could consist in obliging service providers that share data with third-parties to state this in a short disclaimer which appears whenever an individual user connects to the service. Of course, such short-term solutions are cosmetic and still imply user consent and they do not constitute solutions at all as regards to 'gig' workers, who simply cannot afford not to 'consent'. However, before a fundamental overhaul of the current system of protection is implemented – ideally, as part of a more fundamental change in the world order – they might relieve individuals of at least some burden with respect to risk assessment. The starting point for such reforms, however, needs to be the understanding that the GDPR that so many commentators hail as the 'gold standard' of data protection is really not up to the task, and that it actually helps legitimize the use of private data for business purposes.

References

Agamben, Giorgio. 2005. *State of Exception*. Chicago: University of Chicago Press.

Australian Government. 2022. 'National Data Security Action Plan'. April. https://www.homeaffairs.gov.au/reports-and-pubs/files/data-security/nds-action-plan.pdf

Brown, Brian, and Sally Baker. 2012. *Responsible Citizens: Individuals, Health, and Policy Under Neoliberalism*. London: Anthem Press.

Foucault, Michel. 2008. *The Birth of Biopolitics: Lectures at the Collège De France, 1978-79* . Basingstoke: Palgrave Macmillan.

Kim, Nancy S. 2013. *Wrap Contracts: Foundations and Ramifications*. Oxford [England]: Oxford University Press.

Kokolakis. 2015. 'Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon'. *Computers & Security* 64: 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Patterson, Edwin. 1919. 'Delivery of a Life-Insurance Policy'. Harvard Law Review 33 (2): 198-222.

ProPrivacy. 2020. 'Privacy Complacency: The Hidden Dangers Lurking Beneath Today's Surface-Level Data Protection'. 28 January. https://proprivacy.com/privacy-news/privacy-complacency-ebook

Schwartz, Paul, and Karl-Nikolaus Peifer. 2017. 'Transatlantic Data Privacy Law'. *The Georgetown Law Journal* 106 (1): 115–79.

About the author:

Ivan Manokha is a Visiting Researcher at the Oxford Department of International Development. In his research, he has investigated the relationship between global capitalism and individual rights, and more recently has started working on the implications of new technologies of surveillance for different individual rights. His recent publications have focused on self-censorship and self-discipline in the context of surveillance and the rise of digital platforms and the commodification of user data.