

REGULATORY

The myth of consent: Big tech meets (big) data protection

1 March 2023 8 min read

Data Privacy & Cybercrime

Consumers rely on digital platforms such as Google, Amazon and Takealot to gain wider and more convenient access to a variety of goods and/or services. Unfortunately, part-n-parcel of such convenience seems to include the little-to-no-control that consumers experience over the use of their personal information.[1] In light of the aforementioned tension between technological innovation and privacy protection, an ever-increasing number of human-rights interest groups, digital platform users and government officials have called for a more comprehensive data privacy regulatory regime.[2]

In acknowledging the need for further privacy and data management policies (and support for same), various leaders in the Information Technology and Communications (“ITC”) industry[3] have stated their desire for more comprehensive data protection regulations.[4]

For example, one of the highlights of the 2020 World Economic Forum’s 50th anniversary (held in Davos, Switzerland) was the call by Big Tech[5] executives for increased regulation in the realm, *inter alia*, of artificial intelligence and data management regimes.[6] To this end, the likes of Apple’s Chief Executive (Tim Cook) and Meta’s CEO (Mark Zuckerberg) called for laws that expand on consumers’ rights over their data; and while emphasised the need for regulators to set clearer rules regarding, *inter alia*, the dissemination of online content, data portability and privacy rights.[7]

Since the advent of governments’ increased focus on privacy rights,[8] digital platforms, in general; and Big Tech in particular, have come under fire for their data collection practices, their use of targeted advertising on young users[9] and other (allegedly) anti-competitive business practices.[10]

Background

A digital platform is a website, mobile application (colloquially referred to as an “app”) or digital venue that interacts commercially with users or groups of users.[11] Popular digital platforms include Youtube, Uber, TikTok and Spotify; most of which are owned and operated by a handful of prolific technology companies that operate in the ITC marketplace.[12]

The types/categories of data collected by digital platforms[13] may include a user’s location, search and purchase history, IP address’, emails received and dispatched etc. – depending on the nature of the digital platform.[14] One of the more relevant (and controversial) features of digital platforms’ data collection and/or management practices involves the selling of user data to third parties – including credit agencies, marketers and other similar service providers.[15]

Indeed, the concept of ‘**Fair Information Practices**’ (i.e. a prelude to the OECD’s[16] Guidelines on the Protection of Privacy)[17] speaks to the global standard for privacy and data protection.[18] However, the OECD’s initial ‘notice and consent’ model is no longer relevant to a 4IR world in which technological developments have reduced consumers’ ability to understand what they are consenting to in privacy policies. [19] Generally speaking, internet users who click ‘agree’ to such ‘click-wrap’ agreements are often consenting to the lowest denominator of existing privacy protections; and in turn, unknowingly permitting the disclosure of their personal information to third parties.[20]

The European Union's ("EU") attempts to regulate the ITC industry have led to unintended consequences.[21] For example, the [General Data Protection Regulation](#) ("GDPR") is aimed at protecting consumer privacy. Unfortunately, Tech Giants have obtained increased access to personal data – with fewer restrictions – by pushing the consent requirements of the GDPR onto digital publishers; and labelling themselves as 'a controller of personal data'; thus allowing Tech Giants to cement themselves, *inter alia*, as leading advertising partners.[22]

From a competition law perspective, one of the solutions tabled to circumvent the possible anticompetitive conduct of Big Tech firms and other digital platforms is the concept of interoperability – which would require the tech platforms to exchange information by operating in conjunction with each other, as opposed to the norm of monopolising information in order to entrench dominance in the market.[23] Although this strategy may alleviate competition concerns relating to abuse of dominance, one of its biggest (and most important) pitfalls lies in the nature and extent to which such data-sharing may raise data protection concerns!

Further, while the potential abuse of dominance may be alleviated by interoperability; the concept appears to lend itself to cartel conduct. The reality of this pitfall is demonstrated by the merger of *Sanlam Emerging Markets Proprietary Limited and Allianz Europe B.V./SAN JV (RF) Proprietary Limited*, wherein the CCSA recommended the approval of the merger, subject to conditions that mitigate the exchange of competitively sensitive information between the impugned joint-venture partners.[24] Thus, inasmuch as interoperability may lend itself to the levelling of the proverbial 'playing field' from a competition perspective, it should not be achieved at the expense of Data Subjects' right to privacy and data privacy legislation.[25]

POPIA[26] provide for the legal processing of personal information in the absence of consent. In terms of POPIA, consent may be a prerequisite for the processing of certain types of personal information (i.e. special personal information or the personal information of minors), as well as the further processing of personal information. However POPIA **is not** a consent-driven legislation. In other words, a Responsible Party (or controller) does not necessarily need to obtain the consent of a data subject before processing the personal information of the data subject, provided that such processing occurs on a lawful basis. This approach demonstrates the South African competition law regulator's awareness of how the myth of consent in so-called 'click-wrap' agreements can ultimately endanger the security, accuracy and integrity of users' personal information.[27]

Conclusion

Indeed, the recent wave of competition investigations – accompanied by a growing backlash over privacy, encryption, artificial intelligence and content monitoring concerns – has pressured persons (both natural and juristic) into implementing self-regulatory schemes relating to data management.[28] After all, who can forget the **big rush** (and confusion) into privacy policy formation following the commencement of POPIA.[29]

Be that as it may, it remains important to evaluate the global data governance regime(s) – particularly in the context of Big Tech and digital platforms – with the awareness that building new technologies means more than creating new (virtual) realities; it also includes developing mechanisms that ensure the appropriate application of such new technologies.

In the words of Jim Henson, "*There is not a word yet for old friends who've just met.*" Similarly, there is yet to be a word invented for the ever-present congruency that exists between digital ecosystems, big business (i.e. Big Tech), and (big) data (protection and management).

What is clear, however, is that there can be no denying the intrinsic link between digital platform regulation and consumer data privacy/protection.[30]

[Cybercrimes Act: South Africa Finally Joins The Big Boy Table](#)

Footnotes

[1] [The Regulatory Review "Data Privacy Through the Lens of Big Tech"](#) accessed 16 February 2023.

[2] [The Regulatory Review "Data Privacy Through the Lens of Big Tech"](#) accessed 16 February 2023.

[3] [The Regulatory Review "Data Privacy Through the Lens of Big Tech"](#) accessed 16 February 2023. Big Tech includes Meta (Facebook); Amazon, Microsoft, Apple and Alphabet (i.e. Google parent company).

[4] [The Regulatory Review "Data Privacy Through the Lens of Big Tech"](#) accessed 16 February 2023.

[5] [The Regulatory Review "Data Privacy Through the Lens of Big Tech"](#) accessed 16 February 2023. The largest and most dominant digital platforms in the world are Meta (Facebook), Amazon, Microsoft, Apple and Alphabet (i.e. Google's parent company).

[6] Forbes “Davos 2020 Hacked: Tech And Innovation Dominate” accessed 26 February 2023.

[7] The Wall Street Journal “Tech Giants’ New Appeal to Governments. Please Regulate Us” accessed 20 February 2023.

[8] The Constitution of the Republic of South Africa, 1996, section 14.

[9] Competition Policy International “Biden Calls For Antitrust Push to Rein In Tech Giants” accessed 8 February 2023.

[10] Competition Policy International “Biden calls for Antitrust Push To Rein in Tech Giants” accessed 20 February 2023. Self-preferencing has been identified as one of the potentially anti-competitive business practices in which digital platforms engage.

[11] The Regulatory Review “Data Privacy Through the Lens of Big Tech” accessed 16 February 2023.

[12] The Regulatory Review “Data Privacy Through the Lens of Big Tech” accessed 16 February 2023.

[13] The Regulatory Review “Data Privacy Through the Lens of Big Tech” accessed 16 February 2023.

[14] The Regulatory Review “Data Privacy Through the Lens of Big Tech” accessed 16 February 2023.

[15] The Regulatory Review “Data Privacy Through the Lens of Big Tech” accessed 16 February 2023.

[16] Organisation for Economic Co-operation and Development.

[17] OECD “Privacy” accessed 26 February 2023.

[18] OECD “Privacy” accessed 26 February 2023.

[19] The Regulatory Review “Data Privacy Through the Lens of Big Tech” accessed 20 February 2023.

[20] The Regulatory Review “Data Privacy Through the Lens of Big Tech” accessed 20 February 2023.

[21] The Regulatory Review “Data Privacy Through the Lens of Big Tech” accessed 20 February 2023.

[22] The Regulatory Review “Data Privacy Through the Lens of Big Tech” accessed 20 February 2023.

[23] The Regulatory Review “Data Privacy Through the Lens of Big Tech” accessed 20 February 2023.

[24] Competition Commission “Media Releases” accessed 27 February 2023.

[25] The Regulatory Review “Data Privacy Through the Lens of Big Tech” accessed 20 February 2023.

[26] Protection of Personal Information Act 4 of 2013.

[27] The Wall Street Journal “Tech Giants’ New Appeal to Governments. Please Regulate Us” accessed 20 February 2023.

[28] The Regulatory Review “Data Privacy Through the Lens of Big Tech” accessed 20 February 2023.

[29] The Wall Street Journal “Tech Giants’ New Appeal to Governments. Please Regulate Us” accessed 20 February 2023.

[30] The Regulatory Review “Data Privacy Through the Lens of Big Tech” accessed 20 February 2023.



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)