Corporate digital responsibility: Dealing with ethical, privacy and fairness challenges of AI

Received: 16th May, 2022

Professor Jochen Wirtz
Vice Dean, National University of Singapore, Singapore
E-mail: jochen@nus.edu.sg

James ‘Jimmy’ Tarbit
PhD Candidate, University of Queensland, Australia
E-mail: j.tarbit@business.uq.edu.au

Associate Professor Nicole Hartley
Associate Professor, MBA Director at University of Queensland, Australia
E-mail: n.hartley@business.uq.edu.au

Professor Werner Kunz
Professor (of Marketing), University of Massachusetts, USA
E-mail: werner.kunz@umb.edu

KEYWORDS: corporate digital responsibility, artificial intelligence, data, ethics, privacy, fairness

Artificial intelligence (AI) has made, and will continue to make, significant improvements to service companies with respect to workforce automation, market offerings, service quality and productivity.¹⁻⁵ However, these applications of AI can pose serious and disproportionate risks to service customers as a result of ethical trade-offs made by companies in the design and operation of AI.⁶ For instance, autonomous decision-making processes have been shown to display biases and discrimination against certain vulnerable consumers in the provision of important services;⁷,⁸ the use of AI in data-driven
business models that operates without oversight or accountability while covertly harvesting consumer data *en masse*; and the application of AI generated consumer data and insights to prompt addictive or coercive service interactions. These exemplars of ethical business trade-offs can inflict negative outcomes onto service consumers, including dehumanisation, loss of autonomy and dignity, financial liability and marginalisation within society, to name but a few.

Although AI practices may be implemented and governed by service companies with the best intentions toward mitigating these ethical concerns, AI models can become malleable and create unintended outcomes (or ‘algorithmic fallout’) through ‘poisoned’ input data, method biases, and historical biases.

As service companies increasingly migrate their offerings to digital platforms and implement progressively advanced AI systems, the degree of potential harm to consumers, scope of unintended outcomes and opportunity costs inherent within ethical trade-offs can only escalate. In the context of AI applications within digitally-focused service business models, these ethical concerns are difficult to manage given the opacity, complexity, ubiquity and unobservability of AI systems. Accordingly, service academics and practitioners are progressively utilising the concept of corporate digital responsibility (CDR) to assist in identifying, managing and mitigating the ethical trade-offs attributed to AI.

At the society level, CDR can be defined as a ‘set of shared values and norms guiding an organisation’s operations concerning the creation and operation of digital technology and data’. From a service perspective, CDR involves the shared values, social norms, organisational artifacts, governance procedures and operational practices utilised by service companies in addressing the ethical trade-offs involved with managing AI systems within their business models and value chains. While internally managed, a company’s CDR practices are informed by external regulation (eg General Data Protection Regulation [GDPR]), consumer expectations and willingness of the company to absorb opportunity costs imposed by managing ethical trade-offs (eg shutting down external revenue streams derived from selling consumer data to unaffiliated third parties).

In ensuring ethical operation of AI in service companies, CDR practices respond to specific ethical risks that arise from different stages of the service technology and data lifecycle. Each lifecycle stage involves distinct activities and processes pertaining to the ethical usage of AI technology and data. First, the creation lifecycle stage focuses on ethical risks involved with the capture of data to be processed by AI systems (eg observation and surveillance, biometric identification, integrating data from third parties, designing variables representative of the target population and training data, disclosure of data collection practices). Second, the operation stage refers to the functioning of AI systems to execute service processes (eg analysing consumer information to enact service decisions with transparency, validity and all stakeholder interests accounted for). Third, the refinement stage of AI systems and trained data sets involves optimisation, inspection and financial/social impact assessment of operating AI systems (eg detecting biases, unforeseen consequences and bad actors through performance auditing and formal governance procedures). Fourth, the retainment stage refers to practices involving the secure storage or retirement of data and AI systems (eg ensuring security of sensitive consumer information such as banking details, biometric data permanently destroyed after a mandated time interval has passed). At each stage of a service company’s service technology and data lifecycle, ethical trade-offs are apparent in relation to the use of AI systems both internal to service companies and also in response to how other service companies embed their AI practices across
these lifecycles, both up and down service value chains (ie supply chain partners, data aggregators and data base providers).

But why are service companies making ethical trade-offs and needing to engage in CDR in the first instance? In identifying motivations behind these trade-offs, the CDR calculus is proposed to assess the value of good CDR to a service company. As depicted in Figure 1, the benefits and costs of implementing good CDR practices are proposed to determine the likelihood of a company engaging in ethical trade-offs involving AI systems. The CDR calculus asserts that service companies will engage in positive CDR practices if the calculus is positive or neutral (with respect to financial and reputational costs), whereas negative ethical trade-offs are more likely to occur if the calculus is negative unless external regulation stipulates otherwise.

As the ethical risks, unintended consequences and trade-offs involved with the operation of increasingly powerful AI systems will escalate in future, service companies should ensure that robust and effective CDR practices are in place to manage these risks. A strong CDR culture provides service firms a means to mitigate CDR concerns and pursue the ethical operation of AI systems within digital business models and service offerings.

References
12. Belk, ref. 6 above.
16. Akter et al., ref. 7 above.


22. Lobschat et al., ref. 20 above, p. 876.

23. Elliot et al., ref. 10 above.

24. Lobschat et al., ref. 20 above.


26. Elliot et al., ref. 10 above.

27. Breidbach and Maglio, ref. 9 above.


31. Belk, ref. 6 above.

32. Elliot et al., ref. 10 above.


35. Rai, ref. 28 above.


38. Lobschat et al., ref. 20 above.


40. Wirtz et al., ref. 21 above.