ORGDYN 53 (2024) 101044

Contents lists available at ScienceDirect

Organizational Dynamics

journal homepage: www.elsevier.com/locate/orgdyn

Assessing digital responsibility in a digital-first world: Revisiting the U-commerce framework

Jeandri Robertson [a,b,*,1], Caitlin Ferreira [c,2], Richard T. Watson [d,3], Ian McCarthy [e,f,4], Jan Kietzmann [g,5], Leyland Pitt [e,6]

[a] Industrial Marketing, Luleå University of Technology, Luleå, Sweden
[b] School of Management Studies, Marketing Section, University of Cape Town, Cape Town, South Africa
[c] Graduate School of Business, University of Cape Town, Cape Town, South Africa
[d] Digital Frontier Partners, Melbourne, Australia
[e] Beedie School of Business, Simon Fraser University, Vancouver, Canada
[f] Luiss, Rome, Italy
[g] Gustavson School of Business at the University of Victoria, Canada

"Those who rule data will rule the entire world"

Masayoshi Son

Introduction

In our contemporary digital-first world, data has emerged as more than just a piece of information – it has become an invaluable and prized commodity. Our online interactions, big and small, carve our digital footprints and leave behind trails of bits and bytes that are collected, analyzed, and often commoditized. As our lives entwine even more with the digital realm, collecting and using this data has raised critical questions about individuals' privacy and organizations' responsibilities. Unfortunately, the transparency of data usage remains opaque at best. Consumers are often left in the dark about how their information is gathered, who it is shared with, and how it contributes to organizations' bottom line. This lack of clarity has led to a widening trust gap between consumers and organizations, where the latter is seen more as exploiters of personal data than protectors. The ongoing privacy concerns stemming from current data practices suggest that embracing responsible corporate citizenship, through active engagement in corporate responsibility initiatives, provides both individuals and organizations a clear way forward.

Corporate social responsibility has traditionally focused on societal and environmental impacts. However, with digitization now ubiquitous, organizations must also prioritize corporate digital responsibility, which means upholding ethical data interactions, responsible artificial intelligence (AI) development, and fair digital trade to restore consumers' trust in the growing role of technology in their lives. This perspective mirrors the changing landscape of organizational operations and highlights the need for organizations to foster positive influences on consumer communities' overall health and well-being. When handled conscientiously, technology need not come at the expense of privacy but can empower communities through shared progress. However, achieving an equilibrium between growth and protecting consumers' digital interests requires transparency and stewardship of personal information.

Rapid technological advancements have broadened the scope of responsibility for both organizations and individuals, introducing a range of ethical, legal, and social challenges. However, the clear definition and allocation of these responsibilities have not evolved as quickly as technology, leaving behind a persistent gray area of uncertainty. This ambiguity, highlighted by ethical dilemmas facing consumers and regulators, underscores the urgent need for contemporary frameworks to navigate today's dynamic ethical landscapes and offer clear guidance. Over two decades ago, Richard Watson and colleagues introduced the concept of ubiquitous commerce (U-commerce), envisioning a new marketing era enabled by pervasive digital networks through four core

* Corresponding author at: Industrial Marketing, Luleå University of Technology, Luleå, Sweden.
E-mail address: jeandri.robertson@ltu.se (J. Robertson).
[1] ORCID: 0000-0002-3486-8292
[2] ORCID: 0000-0001-9575-6676
[3] ORCID: 0000-0003-0664-8337
[4] ORCID: 0000-0003-3330-0977
[5] ORCID: 0000-0002-3576-994X
[6] ORCID: 0000-0002-3089-9184

https://doi.org/10.1016/j.orgdyn.2024.101044
Received 30 September 2023; Accepted 21 February 2024
Available online 29 March 2024

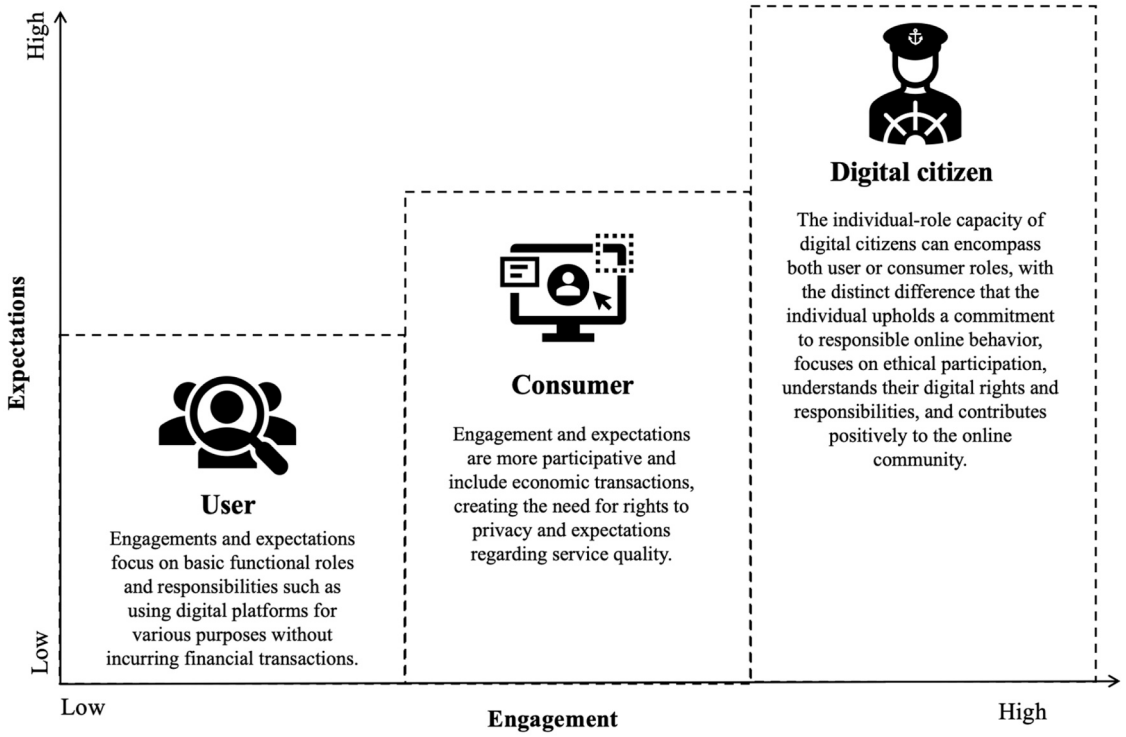

Fig. 1. Individual-role capacities regarding digital responsibilities and data rights.

dimensions – *unique* customization, *universal* access, *ubiquitous* networks, and *unison* in interactions – all elements that have become increasingly relevant in today's digitally interconnected world. We propose revisiting the U-commerce framework to better understand digital responsibilities for individuals and organizations, with the aim to offer managers, practitioners, and citizens of this digital world a refined perspective on their roles within the digital ecosystem, informed by expectations, engagement levels, and responsibility focus.

We begin by considering the challenges and consequences of U-commerce in a digital-first world. This is followed by a discussion on mapping digital responsibilities across stakeholders implicated in these challenges, including consumers (and their data), as well as the broader digital citizenry, which catalyzed the emergence of corporate digital responsibility. Following this, we revisit the dimensions of the U-commerce framework to demonstrate how the transition from ubiquitous networks to participatory accountabilities leads to a more defined view on digital responsibility. This transition emphasizes both the focal point of responsibility and the type of data interaction, culminating in the UP framework. The UP framework offers a clearer separation, aiming to resolve the increasing uncertainty surrounding data rights and responsibilities. Finally, we explore digital social contracts which build upon the UP framework, as a way to define ethical data governance.

The challenges and consequences of U-commerce in a digital-first world: Setting boundary lines

The digital landscape's evolution, highlighted by the growth of U-commerce, has undoubtedly presented individuals with unprecedented convenience, connectivity, and personalized experiences. Simultaneously, it has armed organizations with the capacity to gather, store and use these individuals' data at will. Organizations' ability to collect and process user data to provide personalized experiences, has highlighted data privacy and security issues, leading to public scrutiny, as seen in cases such as the Facebook-Cambridge Analytica scandal. Personalized U-commerce experiences, such as Netflix's recommendation algorithm, subtly guide user behavior. The algorithm promotes longer user interaction by tailoring content based on users' viewing history, subtly shaping their viewing preferences by recommending specific shows and movies. However, the manipulation of viewing experiences raises ethical considerations about the extent to which personal data should be used to steer consumption and platform engagement. The result is ethical complexities on both an individual and organizational level, such as those associated with smart devices that constantly record data, the actions of autonomous vehicles in dangerous situations, and algorithms making recruitment decisions.

Beyond manipulation, the advent of U-commerce has inadvertently given rise to socio-economic disparities. The not-so-obvious digital divide leaves some struggling for equal access to opportunities and services, particularly owing to economic constraints or geographic locations. The shift to online learning due to the COVID-19 pandemic exemplifies this digital divide, where students without reliable internet connections were more likely to fall behind peers with sufficient digital access. Perhaps most alarmingly, the tendency to view and treat consumers merely as 'users' or numerical data points results in a dehumanizing effect. This perspective fails to appreciate the individuality of consumers, who have data rights and responsibilities in the digital space. But where do we draw the boundary lines between individuals' responsibility and organizations' accountability?

While corporate digital responsibility is frequently highlighted, a comprehensive understanding of digital responsibilities necessitates focusing on the individual's role as well, as individuals engage with digital technologies in diverse capacities. An initial step in grasping digital rights and responsibilities involves discerning the roles individuals assume within the framework of U-commerce. Each individual-role capacity involves a nuanced level of engagement in the digital realm, as well as associated expectations concerning digital responsibilities and rights relating to the use of personal data. Fig. 1 illustrates these roles – user, consumer, and digital citizen – highlighting each role's level of engagement and expectations regarding digital responsibilities and rights within this interconnected digital environment.

A user primarily engages with digital platforms and services on a functional level, where the interaction might not involve financial transactions. Here, the focus is on the access and use of digital tools. Conversely, a consumer enters into economic transactions, buying or

Table 1
Mapping digital responsibilities using the U-commerce framework.

U-Commerce Dimension and Practical Example	Consumer Data Rights	Digital Citizen Responsibility	Corporate Digital Responsibility
Uniqueness, e.g., *chatbots*. Chatbot interactions can be tailored to each user, providing personalized advice and customer service based on the user's previous interactions with an organization. Chatbots adapt their responses according to user behavior, preferences, and feedback, thus making each user's interaction distinct and unique.	1. *Be informed: Consumers should be notified when their feedback, preferences, or behaviors are being used to personalize chatbot interactions.* 2. *Opting-out: Consumers should have the right to choose if their data is used for personalizing the service.* 3. *Deletion: Consumers should be allowed to request deletion of their personal data used for tailoring the chatbot interactions.*	1. *Informed consent: Be aware and provide informed consent to the chatbot to personalize your data for a unique user experience.* 2. *Personal privacy settings: Check and update your privacy settings as needed, ensuring the data shared for personalization aligns with your comfort level.* 3. *Constructive feedback: Provide constructive feedback to assist in the evolution of these AI-powered tools.*	1. *Obtain explicit consent: Ensure the chatbot is programmed to clearly request and obtain user consent before collecting any personal data for personalization.* 2. *Be transparent: Clearly explain how user data is collected, stored, used, and protected.* 3. *Provide controls: Allow users to modify or delete their personal data at any given time.*
Universality, e.g., *blockchain technology*. Blockchain technology has universal implications by contributing to secure and transparent transactions worldwide, benefiting industries from finance to supply chains.	1. *Transparency: Information about how and why consumer data is being used should be made available to all universally.* 2. *Auditing: Users should have the right to request an audit of transactions involving their data.* 3. *Control: Consumers should have the right to control who has access to their data, expressing the universality of the rights themselves.*	1. *Be transparent: Recognize your role in maintaining the integrity of a distributed and transparent transaction system by being forthcoming and truthful in transactions.* 2. *Manage access controls: Regularly check and manage access controls to maintain data privacy.* 3. *Responsible engagement: Engage with blockchain ecosystems responsibly, prioritizing community benefit and considering the potential implications of your actions within the network.*	1. *Ensure fair access: Given the universal nature of Blockchain networks, equal access for all participants must be safeguarded.* 2. *Maintain transparency: Regularly report on how data is shared publicly on the ledger, always adhering to data protection laws.* 3. *Uphold security: Diligently maintain and enhance the security of the network to resist cyber threats.*
Ubiquity, e.g., *augmented reality (AR) and virtual reality (VR)*. These technologies, because of their mobility and virtual nature, allow users to access immersive experiences from anywhere at any time.	1. *Consent: Users should be informed and express consent before their data is collected for immersive experiences.* 2. *Anonymity: Users have the right to access ubiquitous AR/VR services without giving up personal data when unnecessary.* 3. *Security: Regardless of where the technology is accessed, users have a right to strong, reliable data security.*	1. *Informed consent: Make sure to provide validated consent for data collection when using AR/VR.* 2. *Use responsibly: Use these platforms responsibly, recognizing potential implications on physical and mental health, especially when the platform is used in shared or public spaces.* 3. *Check device security: Maintain the security of your own devices to protect your immersive experiences from misuse.*	1. *Respect privacy: Even though the technology is ubiquitous, respect the boundaries of privacy. Only collect user data that is necessary and always with consent.* 2. *Ensure safety: Develop guidelines to ensure the safety of users from physical harm and psychological effects from extended use.* 3. *Provide accessibility: Make efforts to ensure the technology is accessible, considering factors such as user mobility, network connectivity, and varying device configurations.*
Unison, e.g., *recognition technology*. The application of advanced technologies such as facial recognition, biometrics, and voice recognition effectively demonstrates the principle of unison. By enabling a coherent and consistent user experience across a variety of devices and platforms, these recognition technologies enhance user experience by facilitating hassle-free, personalized authentication procedures.	1. *Notification: Consumers should be informed when their biometric data is being collected.* 2. *Consent: Explicit consent should be obtained before collecting or using biometric data.* 3. *Revocation: Users should be able to revoke consent and request deletion of their biometric data at any time.*	1. *Informed consent: Understand the potential implications of sharing biometric data and give consent accordingly.* 2. *Manage personal data: Continuously review and manage your biometric data on devices/platforms.* 3. *Maintain device security: Take appropriate steps to protect your biometric data.*	1. *Protect sensitive data assets: Recognize that recognition technologies deal with highly sensitive data. Ensure that robust data protection mechanisms are in place.* 2. *Be transparent: Clearly articulate what biometric data is collected, how it is used, and for what purpose.* 3. *Consent and controls: Prioritize obtaining explicit consent before any data collection or processing occurs and allow users to easily revoke consent or request deletion of their data.*

subscribing to digital offerings, with set expectations regarding their privacy rights and the quality of services received. The consumer role emphasizes the marketplace aspect of digital engagement, where consumer protection laws and ethical business practices become crucial. A digital citizen, however, embodies a more comprehensive, holistic and responsible engagement with the digital world. This role goes beyond usage or consumption, embracing an understanding of wide-ranging digital rights and responsibilities. Digital citizens advocate for a safe, respectful, and ethical online environment, demonstrating a

commitment to positive digital community contributions and an awareness of the personal and societal impact of their digital footprint. Digital citizenship also refers to the norms, rules, and responsibilities that come with the use of digital technologies. It highlights that consumers who are users of digital spaces should engage in a manner that is safe and responsible both for themselves and for other users of the technologies.

Given these different individual-role capacities and parameters, organizations have to actively reach beyond their immediate stakeholders to engage with the wider digital ecosystem. This entails a commitment to ensuring user privacy, upholding consumer data rights, and enhancing transparency for digital citizens about the use of their data to proactively bridge the digital divide – actions that should be fundamental to how corporations operate within the digital realm.

Mapping digital responsibilities: digital citizenship and corporate digital responsibility

Just as we strive for equitable societies in our physical existence, the same should be true for our digital existence. In a digital-first world, digital citizens have rights regarding the collection, storage and use of their personal data. Under regulations such as the European Union's General Data Protection Regulation (GDPR), digital citizens have the right to access, rectify, or delete their data. This allows them to exercise control over their own information and enjoy a degree of data sovereignty. In our roles as digital citizens, we generate vast amounts of personal data, and this brings significant attention to data rights. These rights refer to principles around the collection, storage, use and disposal of personal information by organizations. However, it is imperative to note that digital citizenship also carries certain responsibilities for all users of technology, including ensuring that the information shared is accurate and not harmful to others and taking individual responsibility for maintaining good digital hygiene. It also includes being aware of and respecting the digital rights of others, thereby maintaining a healthy, respectful, and secure digital community.

Digital citizens are, however, part of a larger ecosystem; their actions can significantly impact the broader digital community. It is a shift in perspective that recognizes user agency and fosters a sense of shared digital community. It acknowledges that users, aside from being consumers, have a role in shaping their own digital landscape, and as their rights must be upheld, so should their responsibilities be outlined. Organizations, in turn, are keystone actors in this digital society. Understanding their corporate digital responsibilities and implementing processes that uphold them will contribute to a safer, fairer, and more inclusive digital society. This perspective emphasizes a participatory approach that encompasses shared responsibilities in a U-commerce environment, where proactive engagement and mutual respect would form the cornerstone of trust and security in the digital age.

Using the U-commerce framework with contemporary examples, a mapping of digital responsibilities is provided in Table 1. The mapping serves to practically explain and delineate, with relevant examples, what rights consumers should have regarding their personal data, as well as what demarcates digital citizen responsibilities and corporate digital responsibilities in the context of a digital-first world. As such, technology, while critical in shaping our lives today, should be leveraged in ways that support and champion democratic ideals, stimulate fairness, promote transparency, and strengthen individual agency. The goal is not to resist or combat technology, but rather to ensure its design and application uphold every digital citizen's dignity, rights, and well-being.

Revisiting ubiquitous commerce from a participatory digital responsibility perspective

The notion of digital citizenship in a digital-first world can at times make it difficult to discern where responsibility for certain actions lies when considering the multitude of interactions between corporate entities and individuals. By adapting and evolving the four dimensions of the U-commerce framework to our present time, we take a first step to develop an updated perspective on how organizations should engage with the digital frontier. Reconsidering the U-commerce framework in the updated context of digital responsibility serves two purposes. First, while the U-commerce framework underscores the collaborative dynamic between consumers and firms in an interconnected world, the ever-increasing pervasiveness of technology necessitates an update to this framework. Such an update must account for how technological advancements influence the rights and responsibilities of all participants within this ecosystem. Second, the U-commerce framework offers a lens through which we can understand how, in this interconnected digital world, data ubiquity demands a *participatory* approach to digital responsibility. By reflecting on the participatory nature of digital responsibility in the context of U-commerce, we seek to contribute to the development of a more cohesive and accountable digital landscape, emphasizing clearer alignment in expectations and digital engagements.

Uniqueness: balancing hyper-relevance with data protection in the digital age

The first U-commerce dimension, *uniqueness*, suggests that information can be easily customized to a particular context to meet individual needs. In our current digital landscape, the proliferation of AI and machine learning technologies have enabled organizations to harness large amounts of data, analyze customer behavior, and provide highly tailored, user-unique experiences based on distinct user preferences. Hence, uniqueness in the U-commerce context is about providing hyper-relevant digital experiences tailored to individual needs. It is, however, not just about personalization in the digital space, but also about crafting an entire digital experience around individual user preference. However, the collection and storage of this sensitive, personal data results in tech companies becoming custodians of big data – leaving them and their consumers vulnerable to unauthorized data access and resultant cybercrime. For all entities using the digital landscape to collect data, the responsibility lies in complete transparency regarding how data is collected, stored and used. This suggests that organizations should safeguard data in a manner that protects it from unauthorized access. While growing legislation seeks to mandate this data protection, we view this as a duty that must be upheld by organizations to ensure a fair digital society.

Universality: maintaining privacy in an 'always-on' world

The second concept, *universality*, suggests that universally usable technologies possess the greatest usefulness. The 'always-on' nature of portable consumer devices presents a clear example of the universality of these devices combined with the seamless integration thereof. The original U-commerce framework highlighted issues with the universal nature of certain devices given their inability to integrate with other devices. Their predictions for a universal phone that allows users to remain in constant connectivity have certainly been realized. Smartphones today provide a clear example of a device that offers a continually expanding application and thereby acts as a replacement for multiple devices. A further aspect of universality that is ever more relevant today is the universal user experience across a multitude of devices. Applications that can be used across devices – for example, the popular instant messaging platform WhatsApp, or cloud-based services like Google Drive that allow seamless access and interaction with data across various devices – provide the same user experience regardless of the device, offering the same functionality. Of critical concern, as it relates to the universality of technological devices today, is the sharing of personal information between a multitude of devices with varying security and privacy permissions. This brings with it an individual responsibility to ensure the privacy of one's personal data. It is vitally important that digital citizens have a clear understanding of what and

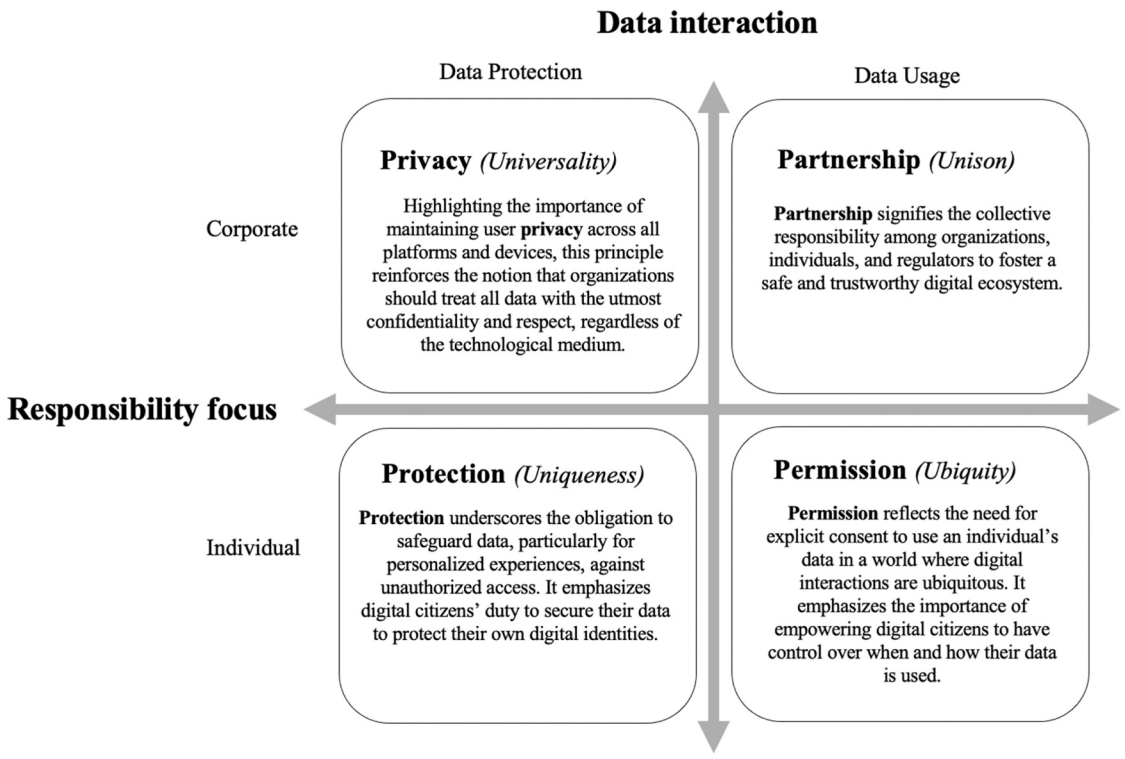

Fig. 2. The UP framework of digital responsibility.

how they are contributing to the digital landscape, which requires an intimate understanding of how their data is collected, stored and managed by third parties.

Ubiquity: digital presence with permission

The third component of the U-commerce framework originally predicted that embedding microprocessors and network connections in all electronic devices would significantly enhance everyday utilities' usefulness and information-processing capabilities. As technology has evolved in recent years, the power of information *ubiquity* has substantially increased. One of the most powerful features of portable consumer devices today is their ubiquitous access to information. Users can gain access to information from anywhere at any time through ubiquitous internet access which greatly enhances the utility it offers its users. The dimension of ubiquity is also evident in our ability to access services like e-commerce platforms, Internet banking, or digital entertainment regardless of our location or time zone. Aspects such as around-the-clock availability of customer support through robust security measures that protect user data across different access points highlight the relevance and prevalence of ubiquity in our digital lives. This ubiquity of technology reflects the need for explicit user permission when it comes to data collection and monitoring. Encouraged by the elimination of cookie tracking, more organizations are shifting from third-party to first-party data management strategies, one that actively seeks the consent of users with an opt-out option for users that do not agree to the data usage and/or management protocols.

Unison: shaping digital communities and integration through partnership

The final component of the U-commerce framework relates to *unison*, which, in the original framework, considered the ability for information to always be readily available regardless of the device, rendering the location of the user (or the device) irrelevant. This would require a complex integration of different communication systems to provide a location-independent unified user experience. An example of this is cloud-based platforms, which allow for consistency in data and a seamless user-experience across a multitude of different devices. Unison further considers the ability for disparate devices to be fully synchronized in real-time – the consistent synchronization of data across wearable technologies, smartphones and those with permission to access this data provides a clear example of this component. The collective pool of data generated and shared in unison can, however, be misused by organizations, either by selling it to third parties without consent or by using it for purposes other than those initially agreed upon by the owners. Partnerships between technology providers and data owners can help establish safeguards and governance mechanisms for responsible data sharing, ensuring collective data is used ethically and securely across platforms.

A renewed perspective of the U-commerce framework thus needs to reflect the participatory digital responsibilities of all stakeholders within the ubiquitous networks. Fig. 2 depicts an updated view of this *Ubiquity to Participatory* perspective, or, and UP framework of digital responsibility. The UP framework provides a delineated perspective on digital responsibility, emphasizing both the responsibility focus and nature of data interaction.

As per the UP framework, the *uniqueness* dimension underscores the individual's duty to manage and ***protect*** their digital identity, thereby protecting personal information and data interaction flow. Conversely, *universality* charges corporates with the critical task of maintaining user ***privacy*** across all platforms by treating data with utmost confidentiality. Moreover, *unison* champions the establishment of a collaborative ***partnership*** between individuals and corporates, fostering an ecosystem where ethical data use and shared responsibility are the foundational pillars, ensuring a collectively secure digital environment. Lastly, under the auspices of *ubiquity*, while organizations are entrusted with the responsibility to obtain explicit ***permission*** from individuals, it is imperative that individuals fully comprehend what data they allow organizations to collect, store and use when offering explicit permission. This empowers individuals to control the use of their data across diverse digital interactions.

The UP framework aligns well with Jean-Jacques Rousseau's

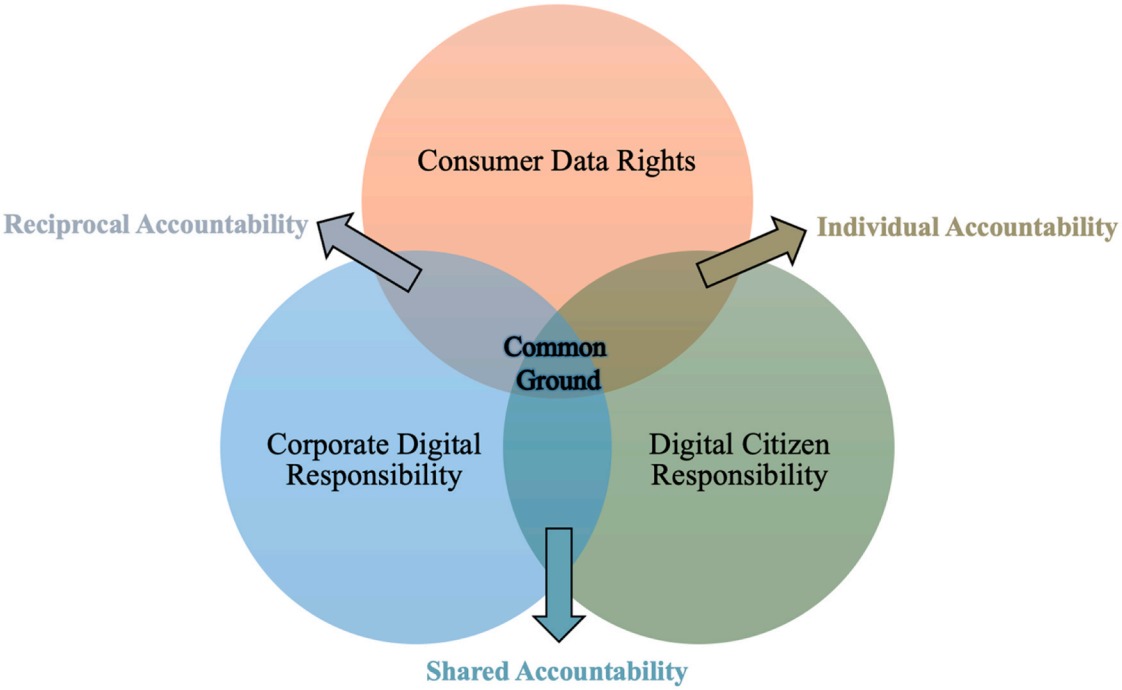

Fig. 3. The role of digital social contracts in facilitating cooperative accountability.

classical social contract theory, which emphasizes the significant role of agreements and responsibilities in shaping interactions. While outlining digital responsibilities provides parameters regarding the boundary lines of ethical behavior, social contracts focus on the obligations related to executing these responsibilities effectively. This lays the groundwork for understanding, what we propose as, digital social contracts – the modern extension of traditional social contract principles into the digital realm.

Digital social contracts: with digital responsibility comes digital accountability

Digital social contracts aim to describe how individuals, organizations, and the larger digital citizenry formulate interaction rules and establish responsibilities within the digital realm. At its core, a digital social contract is an online agreement among individuals that sets out to establish a self-governed, egalitarian, and fair society in the digital world. The purpose of a digital social contract is to guide the digital ethics and societal responsibilities of all digital citizens, informing them of their consumer data rights, digital citizen responsibilities, and corporate digital responsibilities.

As guiding principles or norms that govern the behavior and interactions within the digital realm, digital social contracts should serve to raise awareness and educate digital citizens about their rights and responsibilities, while also promoting transparency by encouraging clear communication and disclosure of information regarding data collection, usage, and privacy practices. Digital social contracts empower individuals, organizations, and other entities to actively control their digital footprint and make choices aligned with their privacy preferences. By adhering to these digital social contracts, individuals and corporations can be held accountable for their actions and behaviors in the digital world. In Fig. 3 we illustrate how digital social contracts can facilitate cooperative accountability among individuals and organizations in the digital realm, focusing specifically on its value in the context of consumer data rights, digital citizen responsibilities and corporate digital responsibility.

Consumer data rights represent the rights that individuals have over their personal data. It includes concepts like the right to privacy and the right to be "forgotten". Individuals have the right to control how their data is collected, used, and shared in the digital space. In turn, digital citizen responsibilities refer to the responsibilities that individuals have as participants in the digital world. It includes behaving ethically and respectfully, following the norms and guidelines of the digital spaces they engage with. Digital citizens are accountable for their actions and contribute to shaping the overall "climate" of the digital sphere. Lastly, corporate digital responsibilities denote how organizations, as facilitators of digital connections, contributions, and communities, are responsible for creating safe and respectful digital spaces. They are expected to protect user data, ensure privacy measures, and uphold ethical standards. This includes implementing proper data security measures and being transparent about how user data is handled.

In Fig. 3, all three spheres work together to reach *common ground* or collective benefits, by upholding the digital society's shared principles, values, and goals. It signifies the areas of agreement and mutual understanding where all parties can find commonality and work together towards a positive digital ecosystem. The overlap between consumer data rights and digital citizen responsibilities highlights the *individual accountability* to make informed decisions about sharing one's data and actively protecting their own privacy. The overlapping area between digital citizen responsibilities and corporate digital responsibilities reflects the *shared accountability* that individuals and corporations hold in creating a positive and trustworthy digital environment. The area where consumer data rights and corporate digital responsibilities overlap, illustrates the *reciprocal accountability*, where both parties have interconnected commitments to not only uphold their end of the bargain, but also to hold one another accountable.

Managerial implications

To contribute to establishing a democratic and equitable digital society, we provide four practical guiding principles based on concepts from the UP framework and digital social contract concept. The four guiding principles offer a distinct perspective on the digital behaviors that govern a well-functioning digital society, with practical and actionable implications provided with each.

Principle 1: Data dignity

To uphold data dignity, organizations must ensure that privacy controls and data policies serve the individual, emphasizing transparency and empowerment. Education around digital safety and ethics becomes key, alongside facilitating individuals' abilities to manage, understand, and exert their data rights. Making data rights comprehensible and actionable honors each digital citizen's digital dignity.

Managerial implications:

1. Implement privacy controls and clear data policies that champion the data dignity of the individual.
2. Educate on digital safety and ethics.
3. Facilitate (and exercise) a corporate understanding of consumer data rights.

Principle 2: Privacy pledge across platforms

A privacy pledge encourages a shared commitment to privacy that spans every digital touchpoint. It involves embedding privacy from the start with a privacy-by-design approach, conducting thorough and regular assessments to mitigate data risks, and ensuring uniform privacy protections across all digital interactions. This pledge signifies a steadfast commitment to digital citizen privacy, irrespective of platform or service.

Managerial implications:

1. Advocate for privacy-by-design.
2. Conduct regular privacy impact assessments to mitigate risks.
3. Ensure consistency in privacy protections across platforms.

Principle 3: Ethical alliance

The principle of an ethical alliance centers on forming partnerships built on the bedrock of ethical data usage. It involves creating meaningful dialogues with digital communities, working collaboratively with industry peers and regulatory bodies, and developing standards that embody data ethics. This alliance underscores the shared pursuit of integrity in the digital ecosystem, fostering a culture of trust and collective responsibility.

Managerial implications:

1. Engage in partnerships that prioritize ethical data use.
2. Create feedback channels with digital communities.
3. Collaborate (with industry and regulators) to promote data ethics standards.

Principle 4: Consent compass

It is imperative that users, consumers and digital citizens are guided through what it means to be informed about their individual data responsibilities and rights, to ensure that they can make informed and voluntary decisions about their own data. By using clear, revocable consent mechanisms that facilitate the easy adjustment or withdrawal of consent, organizations align their digital responsibilities with their accountability in terms of expectations and the required regulatory landscapes. This principle acts as a compass, ensuring that individual autonomy and choice are always respected, and that consent remains informed and sincere.

Managerial implications:

1. Use understandable and revocable consent mechanisms.
2. Provide options for users to modify or withdraw consent.
3. Regularly review consent practices for alignment with digital citizen expectations.

By focusing on these principles and actionable implications, organizations can effectively navigate digital complexities, build trust among digital citizens, and foster a safer, more responsible digital world. Upholding individual rights while promoting ethical corporate practices shapes a balanced approach to digital responsibility and accountability, crucial for the modern digital ecosystem.

Conclusion

Almost two decades ago, the U-commerce framework emerged, aiming to offer a conceptual basis for understanding next-generation marketing influenced by ubiquitous networks. Although technology has advanced rapidly since the inception of the framework, the underlying concept remains ever relevant. As novel consumer devices and technologies have extended the applicability of the U-commerce concepts, new discussions about digital responsibility and where the boundary lines between personal responsibility and organizational accountability lie have come to light. In this conceptual paper, we have revisited the U-commerce framework as a starting point with which to explore these challenges and have mapped the digital responsibilities of users, consumers, digital citizens and organizations. To demarcate the boundary lines of responsibility, we also propose the future development of the notion of digital social contracts to govern the respective and overlapping digital accountabilities.

The continuous emergence of new technologies, including quantum computing, blockchain, and the Internet of Things, introduces new challenges and opportunities in the context of digital ethics and identity management. The way these technologies interact with data – how they store, protect, and process it – could dramatically reshape our understanding of digital security and ethical data management. Consequently, exploring how these advanced technologies might redefine digital identities, enhance or challenge current security measures, and shift the foundational principles of ethical data handling, presents a significant area for future research. Similarly, future research could also concentrate on the areas of algorithmic transparency and accountability, focusing on developing frameworks and methodologies that can shed light on the inner workings of AI and machine learning decision-making processes. By unpacking the complexities of these advanced computational systems, researchers can contribute to making them more transparent and accountable, thereby safeguarding user rights and promoting ethical technology use.

Selected bibliography

To understand the concept of U-commerce, see the following seminal paper: Watson, R., Pitt, L., Berton, P., & Zinkhan, G. (2002). U-Commerce: Expanding the universe of marketing. *Journal of the Academy of Marketing Science, 30*(4), 333–347. **To understand the concept of corporate digital responsibility, see the following resources:** Isaksson, I., Kiessling, T., & Harvey, M. (2014). Corporate social responsibility: Why bother? *Organizational Dynamics, 43*(1), 64–72; Kunz, W. H., & Wirtz, J. (2023). Corporate digital responsibility (CDR) in the age of AI: Implications for interactive marketing. *Journal of Research in Interactive Marketing*. (In-Press); Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. J*ournal of Business Research, 122*, 875–888; Mirvis, P. H. (2020). From inequity to inclusive prosperity: The corporate role. *Organizational Dynamics*, 100773; Wirtz, J., Kunz, W. H., Hartley, N., & Tarbit, J. (2023). Corporate digital responsibility in service firms and their ecosystems. *Journal of Service Research, 26*(2), 173–190. Zhang, J., & Hon, H. W. (2020). Towards responsible digital transformation. *California Management Review Insights,* March. **To understand the concept of digital social contracts, see the following resources:** Berkelaar, B. L. (2014). Cybervetting, online information, and personnel selection: New transparency expectations and the emergence of a digital social contract. *Management Communication Quarterly,*

28(4), 479–506. Hollensen, S., Kotler, P., & Opresnik, M. O. (2022). Metaverse–the new marketing universe. *Journal of Business Strategy*. (Ahead-of-Print) Srinivasan, R., & Ghosh, D. (2023). A new social contract for technology. *Policy & Internet, 15*(1), 117–132.

CRediT authorship contribution statement

Jeandri Robertson: Conceptualization, Writing - original draft, Writing - review & editing. **Caitlin Ferreira**: Conceptualization, Writing - original draft, Writing - review & editing. **Richard T. Watson**: Conceptualization, Writing - original draft, Writing - review & editing. **Ian McCarthy**: Conceptualization, Writing - review & editing. **Jan Kietzmann**: Conceptualization, Writing - review & editing. **Leyland Pitt**: Conceptualization, Writing - original draft, Writing - review & editing.

Declaration of Competing Interest

None.