Received: 21 October 2021 | Revised: 30 April 2022 | Accepted: 11 May 2022

DOI: 10.1111/joca.12471

the journal of consumer affairs ACCI

WILEY

RESEARCH ARTICLE

Digital exchange compromises: Teetering priorities of consumers and organizations at the iron triangle

Monica C. LaBarge[1] | **Kristen L. Walker**[2] | **Courtney Nations Azzari**[3] | **Maureen Bourassa**[4] | **Jesse Catlin**[5] | **Stacey Finkelstein**[6] | **Alexei Gloukhovtsev**[7] | **James Leonhardt**[8] | **Kelly Martin**[9] | **Maria Rejowicz-Quaid**[10] | **Mehrnoosh Reshadi**[11]

[1]Queen's University, Kingston, Canada

[2]California State University, Northridge, Northridge, California, USA

[3]University of North Florida, Jacksonville, Florida, USA

[4]University of Saskatchewan, Saskatoon, Canada

[5]California State University, Sacramento, Sacramento, California, USA

[6]Stony Brook University, Stony Brook, New York, USA

[7]Aalto University, Aalto, Finland

[8]University of Nevada, Reno, Reno, Nevada, USA

[9]Colorado State University, Fort Collins, Colorado, USA

[10]University of Edinburgh, Edinburgh, UK

[11]California State University, Fullerton, Fullerton, California, USA

Correspondence

Kristen L. Walker, California State University, Northridge, 18111 Nordhoff

Abstract

Societal well-being is challenged by the complexity and intangibility of the compromises inherent in digital exchanges. Increasingly these exchanges rely on technology, with competing priorities that challenge cooperation and communication among key parties involved. The authors examine the factors that drive tensions between consumers and organizations in digital exchanges, as well as how and why interest groups, lawmakers, and bureaucrats (also known as the "iron triangle") try to mediate these exchanges through policy and regulation. By explicating the nature of these relationships, the authors illustrate various trade-offs faced by all parties and depict a novel, comprehensive framework to facilitate holistic assessment of the factors underlying these ubiquitous but complex digital relationships with vague ethical stewardship. This framework serves as a lens to help guide business and

St, Northridge, CA 91330, USA.
Email: kristen.walker@csun.edu

regulatory policymaking and as a platform for identifying future research opportunities.

KEYWORDS
compromise, digital exchange, iron triangle, reciprocity norms

> *All compromise is based on give and take, but there can be no give and take on fundamentals.*
>
> —*Gandhi*

1 | INTRODUCTION

Digital environments present complex challenges for consumers, organizations, and policymakers, and the seemingly intractable tensions between these parties are rising to the level of a crisis (Bak-Coleman et al., 2021). The ongoing digital transformation of organizations such as schools, workplaces, health care systems, and governments has increased the number of exchanges that unavoidably occur online. Technology is leveraged out of both necessity and advantage by consumers and organizations in their interactions and exchanges. Despite being frequently considered a static feature of digital exchanges, technology is central to "social interactions and connections between industry, government, and individuals, influencing privacy values and social norms in complex ways most do not well understand" (Walker et al., 2019, p. 411). Societal well-being, especially in health-related contexts, is challenged by the complexity, intangibility, and elusiveness of compromises inherent in digital exchanges (Ashworth & Free, 2006; Chen et al., 2008), and no clear interdisciplinary framework exists for informing policy and ethical stewardship (Bak-Coleman et al., 2021). We aim to address this gap.

Marketplace exchanges are more than simple trades of money for goods or services (Bagozzi, 1975; Hill & Martin, 2014) but are much more encompassing. For example, even collection and dissemination of information online can be considered exchange (Ashworth & Free, 2006). As in offline exchanges, digital exchanges include both monetary and nonmonetary exchanges (i.e., exchanges of financial and nonfinancial assets, respectively; Okada & Hoch, 2004). Purchasing a product from an online retailer (e.g., Amazon.com) is an example of monetary digital exchange, whereas sharing personal information (e.g., email address) for access to a social media platform (e.g., Facebook) is an example of nonmonetary digital exchange.

Social exchange theory (Emerson, 1976) suggests that both consumers and organizations, in marketplace exchanges, seek to optimize value—providing resources to the other only insofar as a net gain is attained from the outcome of the exchange. In the context of digital exchanges, social exchange theory shows that consumers will disclose personal information to marketers only if the perceived benefits (e.g., improved service experiences such as tailored content; Marwick & Hargittai, 2019) outweigh the perceived negative consequences (White, 2004); otherwise, consumers will terminate the relationship. However, digital exchanges, for reasons we outline subsequently, are often more about negotiating concessions than about negotiating optimal value. We term this digitally centered process of negotiation, of both tangible (known) and illusive (unknown or recognized) exchange terms, "digital compromises."

Digital compromises are influenced by the number of parties involved in these exchanges and the decisions each makes, sometimes referred to as network effects (Reddy, 2018). Network effects are influenced by collective behavior (coordinated action with no overt leader) (Bak-Coleman et al., 2021) and are ultimately challenged by societal norms that guide the responsible and ethical behavior of all parties. We argue that society is facing a collective crisis of compromise (and resistance) dependent on technology, and thus it is crucial to understand the nature of online exchanges, the key parties involved, and the resultant societal implications.

2 | EXCHANGE IN THE DIGITAL ENVIRONMENT

The key parties in digital exchanges have unique needs and differing power, creating struggles over whose needs take precedence. Specifically, consumers may be concerned about privacy—the right to control information about themselves, limit others' access to their presence, body, or property, and make decisions without interference (Chen et al., 2008)—but also seek the convenience of digital resources to access products and services (Ortiz et al., 2018).

Organizations rely on digital environments to develop and maintain competitive advantage and foster customer relationships, while safeguarding their information assets and reassuring key stakeholders of their good stewardship of those assets (Reeves & Whitaker, 2020). Regulators attempt to keep pace with technological advancements, simultaneously working to balance commercial interests and economic considerations with consumer concerns about privacy, access, and control (Espinoza, 2021; Sullivan, 2018).

Consumers and organizations engage in mutually beneficial and interrelated exchange relationships bound by each party's goals (Hill & Martin, 2014). Although the exchange is usually voluntary and provides value to both parties, there are inherent tensions as not all consumers' and organizations' goals are aligned, potentially creating conflict. Digital exchanges are contingent on compromise because, among consumers, organizations, and regulators operating in these environments, there are collective but competing priorities. Compromise in digital exchanges is important because of network effects, the ambiguity of value in digital environments, and the interplay of privacy. Network effects concentrate capital and power in the hands of a few service providers, such that they occupy a quasi-monopolistic market position (Haucap & Heimeshoff, 2014). These strong network effects may influence consumers' ability or willingness to terminate otherwise disadvantageous exchange relationships. An example of this phenomenon is platformization (Poell et al., 2019), where a limited number of technology corporations (Apple and Google), retailers (Amazon), and social media platforms (Facebook) have attained dominant positions in their respective markets. In such cases, the balance of power in the consumer/organization exchange relationship is tilted firmly in favor of the service provider (van Dijck, 2021). An absence of competing alternatives renders consumers effectively locked into a potentially unfavorable exchange relationship and creates dependency problems.

The ambiguous and subjective nature of valuing assets in digital exchanges also contributes to the need for compromise. Consumers routinely exchange personal information such as social security numbers, medical records, and behavioral data through digital products, services, platforms, and software applications. Organizations are clearly aware of the value of consumers' information, given it is included in their metricization (e.g., user engagement), financials (e.g., earnings estimates), and third-party valuations (Birch et al., 2021). Consumers, by contrast, are often less informed of the value of the personal information they provide in digital exchanges (Summers, 2020). The fluid nature of digital exchanges further complicates consumers' ability to both accurately assess the cost and benefits of a potential exchange relationship and exit the relationship when perceived costs, for example, loss of privacy, outweigh benefits. Lacking awareness, consumers participate in imbalanced digital exchanges in which the compromises they make exceed those made by organizations.

3 | DIGITAL COMPROMISES

In practice, many exchanges in digital environments are intangible, complex, and elusive, in frequent violations of *reciprocity norms* (i.e., equity, fairness, honesty, respect, and trust) that are otherwise inherent in marketplace exchanges (Palmatier et al., 2009). Given the delicate balance of consumer/organization needs in digital environments, exchange in this context requires explicitly considering how reciprocal norms can inform and guide compromises. We acknowledge that incorporating reciprocity norms in any context, including digital compromise, is not without challenges in meaning and implicature. The philosopher Paul Grice argued that this could be overcome through cooperative and rational communication among relevant stakeholders (Neale, 1992). Following Grice, we suggest that cooperation and communication are central to navigating digital compromises.

We examine the factors that drive digital compromises between consumers and organizations and explore how and why the iron triangle mediates these exchanges through policy and regulation. We address the following questions: What are the compromises that shape digital marketplace exchanges, and how can these explain consumer and organization behavior and lawmaker response? How can competing interests of these parties inform a more sustainable orientation toward negotiating the compromises required for functioning exchange environments? How do reciprocity norms operate to guide these compromises? We propose a framework that highlights the tension among consumers, organizations, and the iron triangle as they navigate the use/centrality of technology in digital exchanges.

In the following sections, we introduce a conceptual digital exchange compromise framework, focusing on US consumers, organizations, and members of the iron triangle.[1] The framework guides our examination of (1) technology as the central object of tension, (2) the frequently conflicting goals and concerns of consumers and organizations, (3) the iron triangle as the power/compromise fulcrum facilitating (or inhibiting) digital exchange, and (4) the reciprocity norms governing exchange, all of which operate within broader digital environments.

The framework depicts the possibility of mutually beneficial exchanges (Hill & Martin, 2014) and advances consumer well-being on both individual and societal levels. For example, by identifying consumer needs and vulnerabilities in everyday digital exchanges, we highlight focal areas for consumer online education campaigns. Our framework also helps identify the power balance in any given digital exchange, highlighting whether it is unfairly tilted in favor of organizations (vs. consumers) and if the imbalance requires regulatory intervention for consumer protection.

To highlight the framework's relevance and application, we employ three health-related examples (fitness trackers, patient-provider health portals, and digital vaccine certifications) to illustrate both barriers and enabling forces that allow researchers, policymakers, and industry to identify a path toward more harmonious and less adversarial relationships among all parties involved.

4 | CONCEPTUAL FRAMEWORK

We conceptualize the interrelationship between consumers, organizations, and the iron triangle as infused with tension. Consumers and organizations—situated on a beam of technology—are often out of balance as they negotiate digital exchange priorities, and regulators—the fulcrum—govern compromises for societal well-being. This balance beam and fulcrum are embedded in and influenced by the technological environment, as well as the sociocultural reciprocity norms and philosophical organizing principles (Mittelstaedt et al., 2006) that govern all exchanges, including digital ones.

In digital environments, technology is the mechanism for exchange, but it does not supersede the relationship between exchange parties. Our framework views technology as facilitating interactions and exchanges, but in practice it also obfuscates the clarity and details of these exchanges in digital environments, enabling consumers and organizations to surrender to technology (Walker, 2016). With the inherent intangibility of digital exchanges, the power–compromise fulcrum (i.e., iron triangle) shifts—always catching up or lagging behind the progress of technology and reacting to uncertainty in the digital environment (Figure 1). The convenience that consumers desire, combined with the agile nature of organizations, means that exchanges are frequently initiated without necessarily reflecting the reciprocity norms that *should* guide the technology and character of exchange.

Satisficing the needs of consumers and organizations because of technological convenience is not ideal for interactions and exchanges that should encompass societal values and reciprocity norms (Walker, 2016).

4.1 | Balancing priorities of consumers and organizations

In the context of exchange in digital environments, consumers want the benefit of access, smooth and convenient processes, personalized and relevant content, peace of mind, and social connection (Walker, 2016). Simultaneously, however, they must also willingly provide sometimes sensitive personal information and spend time learning to safeguard themselves online. Organizations, by contrast, desire access to customers' data that allow them to provide superior

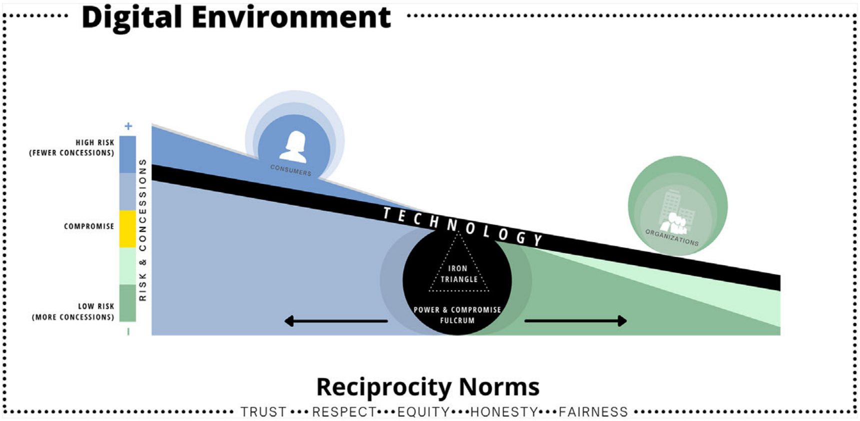

FIGURE 1 Conceptual framework: Digital exchange compromises

service tailored to their needs and wants, as well as to gain customer and market insights that confer sustainable competitive advantage (Martin et al., 2017). Yet organizations must temper data acquisition with consumer privacy concerns and regulatory standards.

The relative power in exchange, where power is reflected in a party's ability to pursue primary goals without having to compromise or make concessions, affects the (im)balance and (a) symmetry of the balance beam. The more powerful side is "heavier" and sets the terms of exchange (e.g., for consumers, the "cost" of access to products or services; for organizations, the "cost" of serving customers). The "weight" of each party is represented by the size of the concentric circles labeled "consumers" and "organizations"; the "heavier" and more powerful party is represented by a larger circle. The extent to which consumers and organizations must eventually compromise depends on the relative power or agency each holds and how that is exercised in the exchange.

For both parties, power and agency are constrained by the other's ability to terminate or limit the exchange; organizations can restrict access to services or withhold status or "preferential treatment" from consumers who do not consent to data collection, while consumers can switch to alternative service providers that require fewer data concessions. Consumers' power is further constrained by their awareness and understanding of privacy issues and the potential harm inherent in everyday digital exchange. Organizations' power is further constrained by protective regulations or, in some cases, voluntary self-regulation (Martin & Murphy, 2017).

4.2 | The iron triangle as fulcrum

The complexity in digital exchanges between consumers and organizations "highlights important policy questions involving power versus process and knowledge versus access" (Walker, 2016, p. 147). Three key participants who negotiate issues of power and influence include: interest groups, lawmakers, and bureaucrats, forming what Adams (1989) originally coined as the "iron triangle." The iron triangle concept reflects how "key participants from each of these groups habitually coalesce to form a tripartite arrangement from which…policies emerge" (Overman & Simanton, 1986, p. 584). As in exchanges between consumers and organizations, the power of one participant in the iron triangle directly influences that of the others. Decisions among these parties are also mediated by trade-offs and compromise, separate from compromises made by consumers and organizations.

One side of the triangle includes people who form groups or coalitions around a cause or issue (i.e., interest groups). Another side includes lawmakers, describing legislative bodies globally. These lawmakers include elected, appointed, or ruling parties who create laws. The last side includes bureaucrats or the people and structures that make decisions and enforce policy, which tends to be highly structured and hierarchical with a focus on setting institutional goals, resolving conflict, handling policy fluctuations, applying rules, and making decisions (Lutzker, 1982).

Parties in the iron triangle act as the fulcrum on which the consumer–organization balance beam rests; they do so by enacting or enforcing regulations to curb or increase the agency of either exchange party (practically, primarily organizations). For example, regulations can limit the type of data organizations may collect and use, ease consumers' ability to opt-out of data collection and use, encourage digital literacy education efforts, or expand access to protective technologies (e.g., end-to-end encryption, VPNs). Regulation can push the fulcrum horizontally toward either end of the beam, with the goal of remedying imbalance when either party has too much power. Regulation can also better align the balance by reinforcing societal values through policy development and implementation with remedy for accountability. However, regulation is often only a partial solution, operating merely as a rearguard (i.e., lagging technology it attempts to regulate), or is inadequately enforced; thus, unintended consequences arise.

Although the fulcrum's position affects the balance of consumer/organization power, the iron triangle can also *be* influenced by consumers and organizations. New regulations that result from interactions between policymakers and organizations (via lobbying) and consumers (via interest groups and elected representatives) can shift the fulcrum toward the less powerful party, thus enabling equilibrium of the balance beam. The ability of consumers and organizations to influence the fulcrum depends on the interactions and power balance between parties in the iron triangle, influencing the position of the fulcrum itself.

4.3 | Enabling and enacting reciprocity norms

Marketplaces are embedded in a broader social context that includes not only legal and regulatory structures (the fulcrum) but also sociocultural norms and higher-order philosophical organizing principles (Mittelstaedt et al., 2006). Philosophical questioning of, for example, the importance of free markets, the imperative to pursue economic growth, data as an engine of innovation, the role of government in society, or privacy as a human right influences the position of the fulcrum and how much it intervenes in the balance between consumers and organizations (Gaskell et al., 2005). Where regulation is a tangible boundary for consumer–organization exchange, philosophies are intangible norms guiding exchange.

Reciprocity is valuable in relationships, and research shows its importance in guiding or constraining exchanges (Kozlenkova et al., 2017). In digital exchanges, we view relevant reciprocity norms as including equity, fairness, honesty, respect, and trust. Assessing the extent and effectiveness of those norms in guiding exchanges is challenging and typically varies by circumstance for several reasons. First, norms manifest in different ways for different groups. Second, perspective and perception also determine reciprocity; if one party perceives reciprocity norms as lacking, it may withdraw or feel like it is being forced to compromise, either of which exacerbates the (dis)equilibrium of power depicted in our framework. Third, reciprocity norms are interrelated. For example, if one party is dishonest, the other party may lose trust and respect from lack of integrity. Furthermore, obvious or perceived inequities set the stage for altered perceptions of trust, respect, and fairness. Parsing these reciprocity norms is difficult and may contribute to why ideal and mutually beneficial exchange relationships are so challenging, especially in digital environments. Fundamentally, however, these norms serve as critical societally informed and grounded constraints to limit the exercise of power by any party in the model.

5 | DIGITAL COMPROMISES: THREE HEALTH-RELATED CONTEXTS

Beyond the salience of "health" (public health, health systems, global health) as a significant concern during the COVID-19 pandemic, digital systems are becoming more central to how health services are delivered; how health information is recorded, stored and transferred; and how individuals track and try to improve their health-related behaviors. In many cases, growth in service delivery and information exchange is outpacing modernization of the standards and regulations that exist to constrain such digital exchanges and protect all parties involved (Walker et al., 2019). Health is an important and timely context for the three examples we investigate herein to explore the wide range of digital compromises for and among consumers, organizations, and the iron triangle.

5.1 | Fitness trackers

A fitness or activity tracker is a wearable device and/or application that can monitor and record various physical and biological measurements, such as location, steps, distance, heartbeat, and calories. Fitness trackers can take the form of hardware devices or software platforms or applications that use data collected through other devices. For example, a Fitbit wristband is a fitness-tracking device that records physical and biometric data. The Strava app is a running/cycling fitness-tracking application that uses data collected through mobile or wearable devices (e.g., smartphone, smartwatch). In many cases, there is integration across devices and platforms—a Fitbit wristband tracks user data and can be set up to automatically transmit this information to the Strava app. Part of the value of fitness trackers is that data are shared not only with companies but also publicly with other users, creating risks related to widespread disclosure of personal information (e.g., physical location, biometric data) and necessitating compromise.

5.2 | Health portals

Health portals involve digital platforms through which healthcare providers and their teams can interact with patients. Portal features include appointment scheduling and check-in, messaging capabilities, medical history and medication information, recent diagnoses and release of test results, and billing. Examples include Epic, PrognoCIS, and NextGen, and according to the National Coordinator for Health Information Technology (Johnson et al., 2021), these portals are increasingly adopted by healthcare organizations and patients. Unlike a personal health record, data generated by patient-provider portal interactions are owned and managed by the healthcare organization (Kruse et al., 2015). Unsurprisingly, medical technology research has raised concerns about privacy and security within these portals (Latulipe et al., 2020) and has questioned equity and balance of patient/provider power on these portals (Antonio et al., 2019).

5.3 | Vaccine certifications

The uncertainty wrought by the pandemic has consumers longing for convenience, social connection, and return to normalcy; yet they are increasingly unable to achieve these desires without evidence of vaccination (Hart, 2021). Vaccinations are increasingly required in many parts of the world and by many organizations for access to public and commerce services, such as education, entertainment, and travel (Shepardson, 2021). Businesses are eager to avoid prolonged shutdowns due to COVID-19 outbreaks because they entail lost earnings and productivity; thus, some are requiring vaccination of employees and customers in hopes of mitigating risk. Employing digital vaccine passports as a mechanism to reduce risk and stimulate a return to “normal” seems an obvious solution, but their use is accompanied by complex sources of resistance and objection, again, requiring digital compromise.

6 | CONSUMER GOALS AND COMPROMISES IN THE DIGITAL ENVIRONMENT

Consumers have a range of priorities and concerns about digital exchanges with organizations and even with other consumers. Consumers' exchange-related goals are often traded off against one another and are frequently circumscribed by what an exchange partner, or the technology itself, will permit. Consumers expect societal norms of reciprocity across digital exchanges (Kozlenkova et al., 2017), but the extent to which these are demanded, demonstrated, perceived, and experienced may be elusive or difficult to evaluate. Drawing from a combination of the cases examined and extant literature (e.g., Lee & Rha, 2016), we posit six primary goals of consumers in their digital exchanges: (1) access and capabilities, (2) convenience, (3) personalization, (4) peace of mind, (5) social connection, and (6) status and recognition. Below, we summarize these goals and provide examples of (un)intended compromises consumers make as they attempt to meet their goals in digital environments.

6.1 | Access and capabilities

When interfacing with technology, consumers want access to content and experiences, as well as the functionality and capabilities these technologies afford. Consumers expect free or low-cost access (Dou, 2004), but the real price may be information divulgence. Concerns about surrendering information in exchange for access are a key criticism of vaccine passports, their protective public health purposes notwithstanding (Yallop et al., 2021). Even for paid services, consumers are often asked to create an account or share an email address and some may believe that their privacy is forsaken or that they have “nothing to hide” (Adorjan & Ricciardelli, 2019). With reoccurring requests, consumers have grown accustomed to providing information with few inhibitions, particularly when requests come with the promise of additional functionality or access (Fernandes & Pereira, 2021). In the case of fitness trackers, platform use is free, but data (which are not governed by existing health privacy legislation) are housed by private entities, with little transparency about data use. Consumers may be acquiescing to such long-term data use not only because decision making in general is biased toward the present (Hofmann et al., 2012) but also because the true nature of such abstract and aggregated digital exchanges is not readily understood. Even consumers with heightened privacy concerns may not understand what information is collected or how it is used. This represents a violation of reciprocity norms, as information is not distributed equitably, and power imbalances result.

6.2 | Convenience

Beyond strict functionality, consumers seek efficiency—processes that are smooth, streamlined, and convenient. Logging into frequently used applications, memorizing an interminable list of passwords, and going through multiple steps to make a purchase can create hassles and waste time. Consumers appreciate organizations that reduce “friction”—that remove barriers to use and protect their time (Gilly et al., 2012). In exchange for reduced friction, organizations expect consumers to trust them and their technology, particularly when saving passwords, payment information, or other sensitive information. In exchange for their trust, consumers expect honesty and respect; however, whether organizations adhere to these norms is difficult (or impossible) to truly assess. With patient-provider portals, convenience is certainly increased for patients, who can now book appointments, communicate with their provider, and review/archive their health data, all on their own schedule (Dendere et al., 2019). However, with both these portals it is not always evident—to consumers, health providers, or other users—where sensitive digital health data and communications are housed or how they are protected. Thus, all exchange participants are required to trust that the system was created and is maintained in compliance with HIPAA and related legislation.

6.3 | Personalization

While consumers may not articulate desires for or actively seek out tailored content, they appreciate relevance and personalization benefits (Aguirre et al., 2015). Online sellers/marketers often highlight products and services that will be most interesting or relevant to consumers and, in some cases, even provide solutions to known problems. In exchange for personalization, individualized data must be gathered, stored, and analyzed for algorithms to generate relevant, targeted content. Consumers may value this hyper-relevant content but also fear undue influence or manipulation (Kim et al., 2019)—signals of mistrust, disrespect, and dishonesty—and ultimately may resent the tracking nature of these technologies. For example, the highly personal nature of fitness trackers may lead consumers to underestimate the value and/or vulnerability of their data (Truong, 2020). Device makers themselves may have secure controls, but "anonymized" data are often shared and integrated with third parties, and it is difficult to evaluate these other parties' stewardship of the data or whether and how the anonymization process actually works (Perez, 2019). Many third-party applications (e.g., Lose It!) capture data from fitness trackers, and such integration is complex and complicated for consumers to control. Consumers' data can even be combined outside their awareness to make "inference attacks"—the ability to make inferences about things such as basal metabolic rate, blood pressure, and stroke risk from the information collected (Torre et al., 2018).

6.4 | Peace of mind

Increasing media coverage of privacy-related issues heightens consumers' (perceived or real) vulnerability when using digital technologies. Consumers naturally seek to dispel potential discomfort and to feel secure while using digital technologies. To obtain this sense of comfort, consumers expend considerable time and effort. To be sure, some consumers choose willful ignorance of privacy issues altogether to avoid stress and anxiety, but for others, peace of mind comes at the cost of vigilantly staying current with effective security measures and potential privacy pitfalls in an ever-changing digital landscape. Other consumers may outsource their privacy protection to third-party applications, but this requires familiarity with alternative solutions and may cost money. The burdens of trust—the time, effort, and money sometimes required for consumers to feel they can trust digital exchanges—might seem unfair and in violation of reciprocity norms. For example, for some people, vaccine passports reassure them that other individuals in the public or workspace are also vaccinated, thus reducing anxiety related to contracting COVID-19. For other people, though, such passports decrease peace of mind if personal health data (i.e., vaccination status) are shared with parties those individuals would otherwise restrict from having that information.

6.5 | Social connection

Digital exchange is a focal means by which consumers make social connections. Professionally and recreationally, technology facilitates social interaction regardless of physical location and time and in greater numbers. Yet, for many, increased connectivity creates pressure to always be available for interaction. Because digitally mediated connections are often superficial, consumers may ultimately trade more meaningful interactions at home and at work for surface-level interactions that reach larger audiences and have potential for more attention and immediate gratification (Nadkarni & Hofmann, 2012). These interactions can require increased disclosure of personal information, physical tracking, and online activity monitoring. Encroachment into one's personal content can violate norms of fairness and/or respect. Fitness trackers, for example, can foster connections and community with like-minded others and help hold oneself accountable to various health goals, but can also create obsessions with metrics for validation as opposed to more important indicators such as how one's body feels (Achauer, 2021) or the enjoyment of activity for its own sake (Etkin, 2016).

6.6 | Status and recognition

Digital technology can satisfy consumers' need for attention, social status, and recognition, but at the cost of significant privacy loss (Leite & Baptista, 2021). Technology enables status recognition for loyal customers through tailored content and status symbols (e.g., badges, titles) in exchange for increased patronage. However, such programs require customers to implicitly consent to having personal data tracked by the service provider. Because such status is fleeting, it also requires a constant reinvestment of effort. Moreover, status on social media entails loss of privacy through public personas, potentially leading to harassment, bullying, and disrespect—significant and potentially unfair consumer costs relative to benefits received.

Users of fitness trackers can experience unhealthy comparisons with others that have implications for self-esteem and mental health, similar to other forms of social media (Kent, 2020). Surveys suggest that consumers feel anxiety, pressure, or guilt related to their fitness trackers (e.g., for not living up to standards), and these feelings may interact with existing disorders such as anxiety in problematic ways (e.g., obsessive focus, perception of failure) (Achauer, 2021). Vaccine passports have a similarly bifurcated impact on status: they can serve as a (tacit) demonstration of shared values around either following public health advice and a communal ethos based on science or a refusal to give up personal choice and a rejection of the establishment and its purported expertise. Either way, they have simultaneously created unity *and* division, along with concerns about who is permitted to access “protected” spaces.

7 | ORGANIZATIONAL GOALS AND COMPROMISES IN THE DIGITAL ENVIRONMENT

Although consumers focus primarily on their interactions with organizations and the resulting impacts on privacy, organizations must consider digital exchanges with all potential stakeholders, including customers, the general market, competitors, regulators, partner organizations, suppliers, and employees. Reciprocity norms often manifest in business as guiding organizational principles (e.g., mission statements), specific operating procedures (e.g., codes of conduct), and/or factors for differentiation (e.g., brand values), depending on customer expectations and key stakeholder priorities. Reciprocity norms may be challenged, however, as organizations compete to achieve digital environment exchange goals. Drawing from both the cases examined and extant literature, we posit three primary exchange goals of organizations in their digital exchanges: (1) building and maintaining sustainable customer relationships, (2) creating marketing agility, and (3) developing organizational culture and values. Moreover, we identify organizations' compromises in pursuing digital exchange goals.

7.1 | Building and maintaining sustainable customer relationships

Creating sustainable customer relationships is essential to digital exchange and competitive advantage (Mikalef et al., 2020). Customer relationships rely heavily on technology and data analytics. Organizations use data for customer acquisition, retention, and termination activities and for market insights that support differentiation strategies (Suoniemi et al., 2020). Consumers' and organizations' digital exchange goals sometimes conflict and require compromise. As described previously, consumers demand functionality, access, capabilities, convenience, personalization, and peace of mind in digital exchanges but have also come to expect digital services at little or no cost (e.g., free applications, limitless information access). Organizations, however, require compensation via customer data in exchange for services rendered to maintain profitability and longevity.

Indeed, technological innovations offer benefits to organizations, but they also require compromises to honor the reciprocal norms ingrained in both customer expectations and regulatory standards. For example, customers expect to be treated with respect throughout data collection and usage by organizations, and regulations highlight honesty as a standard for organizations' digital conduct (Martin et al., 2017). Failing to meet norms-based expectations has consequences for organizations, including consumer privacy criticisms and heightened regulatory scrutiny (Bandara et al., 2021; Bleier et al., 2020), which may result in customer defection and switching (Cisco, 2019).

Practical examples of compromises related to sustaining customer relationships are frequent in digital environments. Digital interfaces such as patient-provider portals might help reduce consumer switching by increasing user (patient) perceptions of convenience, but perceived costs of adoption (e.g., transferring medical records, learning the new portal) can be high and create an immediate disincentive for consumers to switch in the future (Dendere et al., 2019). Fitness trackers, through their social- and status-conferring features, may increase user lock-in and hedge against switching, but demonstrated failures to safeguard user data may highlight the otherwise invisible (or ignored) vulnerability of user data within the platform (Truong, 2020). It is conceivable that regulations could be implemented that limit technological lock-in as an artificial barrier to competition and customer choice.

7.2 | Creating marketing agility

Although customer relationships are the foundation for organizations' digital exchange activities, marketing agility is imperative for organizations to achieve their goals during relentless technological change (Kalaignanam et al., 2021). Digital transformation continues to shape the customer experience, including customers' brand interactions and purchase journeys. In response, organizations are challenged to leverage technological capabilities to meet customer demands and outpace the competition. Effective operations and network collaborations not only contribute to marketing agility but also affect organizational compromise and the dynamics of reciprocal norms in digital exchange.

7.2.1 | Effective operations

Agility is essential to mitigate external threats to organizations' operational and informational ecosystems in digital environments. Data piracy, ransomware, malware, and foreign and domestic hacker communities are on the rise, and consumers and regulators expect organizations to offer sufficient protection (Shackelford, 2012). Reciprocity norms that govern exchange suggest that consumers can trust that their data will be protected by organizations and that they will not be harmed. Such protections, however, require organizations compromise in their resource allocation to foresee and limit potential externalities. Organizational failure to mitigate such vulnerabilities can result in significant losses (Martin et al., 2017), including poor reputation and negative word of mouth, which in turn can drive customer defection and switching. Garmin experienced a significant ransomware attack in July 2020 (Truong, 2020), and the vaccination information of prominent politicians in Quebec was hacked from its nascent vaccine passport system (Globe and Mail, 2021). Such breaches undermine confidence in these systems and create reputation risk.

7.2.2 | Efficient network collaborations

To remain agile and improve technological capabilities, organizations increasingly rely on specialists for services such as market research, advertising, customer relationship management, customer support, records retention, and billing. Organizations must weigh efficiencies gained through network collaborations with costs of violating reciprocal norms—losing consumer trust if transparency and/or oversight is lost to third-party service providers (Kane et al., 2019), or incurring costs due to cultural value differences (conflicting reciprocity norms) across the networked organizations. Notably, customers and regulatory agencies are likely to hold the focal organization accountable even if an interorganizational partner is at fault.

Patient-provider portals make obvious what patient data are in the system and what information could be shared with other healthcare providers to reduce patients' burden of repeatedly providing the same information to new providers. At the same time, patients rely on the original steward of their health information to ensure their data are shared appropriately and securely. The balance of sharing information while preserving security and privacy can be difficult to monitor and achieve for many organizations, particularly as the number of users with access to sensitive data increases (Tapuria et al., 2021). In the case of fitness trackers, many firms share "anonymized" data with third parties, but how data are made anonymous is not clear; moreover, "anonymized" data can be tied back to individual users (e.g., location patterns revealing identity). Fitness-tracking devices are increasingly networked with third-party applications (e.g., Lose It! draws on fitness tracker data for weight loss, Strava for wearable tracking with Zwift for cycling/running) that may not have the same protections in place as the device manufacturer (all of which are difficult to verify or track). With each new application that connects to another, privacy settings become increasingly difficult to control, and privacy risks become increasingly blurred.

7.3 | Developing organizational culture and values

To facilitate sustainable customer relationships, marketing agility, and effective digital exchange, organizations ideally design and foster organizational cultures of reciprocity. Organizational culture comprises the values, beliefs, and norms that set boundaries for acceptable and prohibited behavior in an organization (Schein, 2010). Cultural changes may lead organizations to develop internal corporate digital responsibility (CDR) initiatives to deal with new technologies and corresponding reciprocity challenges. CDR is the set of shared norms and values guiding an organization's operations related to digital technology and data (Lobschat et al., 2021). Currently, most organizations, especially in North America, lack CDR guidelines. However, similar to historical expectations of corporate social responsibility (Shabana et al., 2017), organizational stakeholders may expect intentional CDR guidelines going forward. These guidelines, which exceed regulatory requirements, create consumer data management procedures, rules about privacy protection, employee access, data breach notices, and algorithmic audits to protect stakeholders.

The cost of developing a culture around digital exchange is high, and compromises often occur. The expertise required to understand, develop, and implement innovations that meet customers' and regulators' norms-based expectations requires specialized employees who are costly to recruit and retain. Introducing new technologies in organizations requires cultural buy-in from executives to employees to overcome resistance, which also necessitates setting boundaries to prevent misappropriation of technology (Kane et al., 2019). As ransomware attacks become more common and the wide-ranging impacts across sectors become more obvious, it will be imperative for organizations to demonstrate they take cybersecurity seriously.

8 | GOALS AND COMPROMISES OF THE IRON TRIANGLE IN THE DIGITAL ENVIRONMENT

Beyond consumers and organizations involved in digital exchanges, additional stakeholders seek to influence, govern, and circumscribe the conditions of these exchanges—the iron triangle. How the three sides of the iron triangle navigate their roles influences and is influenced by the balance of power and compromise among the parties. Vaccine passports (and pandemic control measures generally) embody this struggle: public health officials (members of the bureaucracy) attempted to create policy that was supported by some legislators and opposed by others, who in turn were subject to influence by interest groups both in favor of more stringent requirements for access to protected spaces (e.g., teachers, healthcare workers) and those opposed to vaccine requirements (e.g., "anti-vax" groups).

Issues in the iron triangle are countless and may require forbearance due to overlapping or competing interests. Interest groups may have resources to lend more power to one lawmaker over another, lawmakers may be elected officials representing constituents with the desire to create meaningful legislation, and bureaucrats may be indebted to prioritizing certain goals and ideals. The networked iron triangle exerts enormous power on consumers and organizations and has a central role as a balancing force and a fulcrum upon which consumer–organization interactions sit. Customer-facing applications can be directly compared by legislation (i.e., HIPAA) with which they must conform (patient-provider portals) or from which they are exempt (fitness trackers). The limited technological innovation, increased friction, and reduced interoperability characteristic of patient-provider portals are partly a function of how these systems must comply with HIPAA; yet those trade-offs are considered acceptable because the privacy of sensitive health information is deemed paramount. Conversely, fitness app data security is questionable, and many require users to surrender their data to access their primary functionality (Truong, 2020).

The speed of technological change means all participants in the iron triangle may not have equivalent expertise or expectations. The digital environment also generates struggles around power and compromise among stakeholders in the iron triangle as they negotiate rules to address the societal and practical concerns technology creates, informed by reciprocity norms such as those depicted in our model. For example, compared with many European countries, the United States has historically exhibited more pro-technology cultural values, such as greater optimism about innovative technology and its potential to improve quality of life and lead to economic progress. This optimism has tempered public and government desires to regulate innovative technology (Gaskell et al., 2005), which in turn has decreased the power/position of the iron triangle. This exercise of power and the compromises that result sustain a delicate balance between consumers and organizations as they use technology.

Even the most seemingly benign use of technologies can have systemic impacts that the iron triangle needs to be aware of and attend to. With patient-provider portals (including the back-end of electronic medical records), there is the potential to decrease system costs by reducing duplication of testing, catching potentially harmful medication interactions, and increasing efficiency of service delivery (Tapuria et al., 2021). Fitness trackers can have systemic impacts via "fit leaking" (e.g., Strava's heat maps allow the public to detect military operations, diplomatic outposts, and other classified facilities). Location data can also increase the risks of commercial espionage and kidnapping or assault through tracking individuals' daily routines (Scott-Railton, 2018).

In essence, the iron triangle is a multifaceted network of parties with competing goals and expertise, whose commitment to an issue "changes as the particular policy problem moves from definition to resolution and implementation" (Overman & Simanton, 1986, p. 585). The intricacies involved in the iron triangle's networked relationships have been widely debated (Golden, 1998). As "human collective behavior" is a "complex adaptive system" (Bak-Coleman et al., 2021, p. 2), the negotiation in the iron triangle and the struggle for influence that results exemplify this behavior and complexity. We view the iron triangle as reacting to technology changes, with each participant possessing unique power and perspective affecting the interaction dynamics at the vertices—causing tension and creating crisis points.

9 | DISCUSSION

9.1 | Conceptual contributions

Digital environments, and their inherent compromises, pose a crisis for consumers, organizations, and the iron triangle. We examine that crisis and assess how its parties and their exchange goals shape digital marketplace exchanges (summarized in Table 1). As technology becomes even more pervasive and digital exchange partners are increasingly required to compromise, our conceptual model highlights critical implications.

First, consumer well-being is jeopardized by the current dynamics of digital marketplace exchanges. As our model exposes, the nature of the digital context and the goals that matter most to consumers and organizations in this context have tipped the burden of concession and compromise to the consumer. Consumers' perceptions of goal-related benefits, such as access to digital content or tools, are often tangible and instantaneous, while their perceptions of costs and concessions, such as anxiety or obsession with metrics, are more elusive. Consumers' costs are, for the most part, abstract and thus difficult for them to conceive. Any potential risk is at an unknown future time (or not at all)—consumers may be aware that their data are used and may pose future harm, but they have trouble understanding how or when such harm might occur. In addition, consumers' belief that organizations operate under norms of reciprocity can temper any anticipation of risk and their perceived costs.

By contrast, for organizations, exchange benefits are more concrete, immediate, and easy to defend as they contribute to the organization's viability (e.g., profitability, innovation, consumer demand). Although some organizational risks can be elusive, such as potential improper data uses and protection from ransomware attacks, organizational costs associated with digital exchange are by and large clear (e.g., data storage/protection fees, hiring talent).

A second important contribution is our expanded understanding of the balancing entity in these exchanges, beyond regulators in general, to the specific entities and priorities of the iron triangle. Together, the parties of the iron triangle help shift power and promote balance in digital exchange. To the extent possible, these parties also can use reciprocity norms as legislative guardrails to facilitate consumer–organization exchange in digital environments. Ideally, reciprocity norms of equity, fairness, honesty, respect, and trust can inspire greater agility across the iron triangle to ensure smoother and fairer exchange, reducing the collective threat from digital compromise crises.

9.2 | Practical implications and recommendations

As we illustrate, stabilization among consumers, organizations, and the iron triangle is difficult, and some tension is inevitable. Practical solutions to these compromises and struggles are equally challenging. Yet there are paths that progress toward stability, especially when considered holistically as part of a larger movement.

First, reciprocity norms must guide the conditions/character of all technological marketplace exchanges. These norms need to be encouraged, facilitated, and even mandated to ensure they are returned. Precise meaning of each norm to various groups also must be understood and tracked over time. Gradual changes in social norms and philosophies, as well as abrupt events such as whistleblowing reveals, can shift/destabilize the balance beam by putting public pressure on the fulcrum to move. Through organized action (e.g., social movements) and institutional entrepreneurship (e.g., Signal, Firefox, Apple) (Battilana et al., 2009), consumers and organizations may attempt to influence accepted norms regarding technology practices and ethical technology use, including acceptable data management practices and overall transparency provisions.

Second, technological innovation and reciprocity norms must coevolve. Technological innovation may tip the balance beam by creating new opportunities for data collection and analysis,

TABLE 1 Priorities, exchange issues, and perspectives with digital compromise

The struggle for (and with) digital compromise when balancing priorities			
	Consumers	**Organizations**	**Iron triangle**
Priorities	***Access, functionality, capabilities:*** *surrendering data, feeling exposed*	***Sustainable customer relationships:*** *customer switching*	***Clear policy development:*** *comprehensive policy development, implementation*
	Smooth, convenient process: *vulnerable, insecure, exposed*	***Marketing agility:*** *reputation damage*	***Free market competition:*** *protecting consumers and competition*
	Personalization, attention, relevant content: *manipulation, targeting, undue influence*	***Effective operations:*** *digital threats*	***Fair regulatory enforcement:*** *equitably address fraud and deception*
	Peace of mind, lack of worry: *self-protection, effort, vigilance, trust, ignorance*	***Efficient network collaborations:*** *lack of transparency*	
	Social connection: *effort, shallow connection, wasted time*	***Organizational culture and values:*** *extensive resource allocations*	
	Status and recognition: *loss of status, maintenance, expectation, compliance*		
Exchange issues	**Assumptions:** that information exchanges are protected and bound by confidentiality (when it may not be)	**Variance of useful tools:** to access and maintain information	**Slow pace:** of regulatory actions/reactions
	Reliance: on legal information/privacy protections (e.g., HIPPA, COPPA) to "certify" systems and operations as compliant	**Cybersecurity:** concerns with data security	**Challenges with uniformity:** of regulatory policies in complex competitive environment
	Concern: about government access to new information and potential consequences, intended or unintended	Goal of **convenient and seamless connections:** with consumers	**Acquiescence to use of innovative technology before understanding:** or consideration of societal risks/benefits
Perspectives	**Oversight:** Who should oversee (and how) consumer (mis)behavior and promote consumer well-being?	**Social responsibility:** How could organizational digital policies and social responsibility impact its performance and other measurable outcomes?	**Regulation:** What kind digital environment oversight is realistic and feasible?

(Continues)

TABLE 1 (Continued)

The struggle for (and with) digital compromise when balancing priorities			
	Consumers	**Organizations**	**Iron triangle**
	Incentives: What are the effects of nudging, or positive or negative reinforcements, on consumer digital technology behaviors?	**Innovative business models:** What are the implications of platform ecosystems, organizational partnerships, and mergers on data protections, transparency, and digital compromises? How do these collaborations (vertical or horizontal) affect organizational stakeholders?	**Flexible policies:** How do we design policies that are flexible enough to keep up with rapid changes in technology/ marketplace? Can regulatory processes be made more "agile"? How should policymakers approach and enforce transparency regarding data usage, data-based business models, and profit making from consumer data?
	Agency: How do (and can) consumers inform, educate, and protect themselves from bad actors in the digital marketplace? What are the gaps in knowledge?	When/how should organizations offer multi-tier systems to substitute profits from sale of personal data with pay-for privacy features?	**Auditing:** How and when should policymakers impose digital audits, third-party certifications, and ranking scales on organizations? How would such systems create checks and balances? What are potential organizational outcomes?
	Preferences: What individual characteristics determine consumer choice regarding information protection, surrendering their data, pay-for privacy, or willful ignorance?	**Data diet strategies:** Should organizations provide some minimum level of digital access (to content, information, and experiences) without requesting information or data in exchange? If so, how would such strategies impact the balance of power in digital spaces?	**Context:** How do contexts such as health care, financial, or personal data differ and impact policy requirements for creating a balance in information exchange? What contexts necessitate greater power shifts?
	Awareness and action: Are consumers truly able to see and weigh potential long-term risks and benefits? If not, how do we encourage it? If so, how do scale best practices and we change behavior?		

which empowers organizations, or by empowering consumers to protect their information. The growing innovations in digitalized services force customers to increasingly interact with service providers online, furthering data access and use. Facial recognition technology creates new opportunities for tracking consumers across platforms and in real-time. GPS and Bluetooth 2.0 allow for more accurate location tracking. These innovations skew the balance of power toward organizations, as customers find it increasingly difficult to avoid or opt-out of service interactions that involve data collection. Regulations are frequently one step behind the latest technological developments even as the iron triangle referees the levers that lead to compromise. However, technological innovation can also empower consumers, as seen in the case of end-to-end encryption, offering consumers greater data protection and potentially alternative ways of meeting their goals without compromise.

Third, organizations can nurture a culture that values reciprocity norms in all customer data practices (Martin et al., 2017). Organizations that do so not only create competitive advantage through their norms-based behaviors but also promote more balance on our model's beam. We highlight CDR initiatives as one example. These initiatives, which go beyond regulatory requirements, stipulate procedures to handle consumer data, protect privacy, provide employee access and training, disclose data breaches, and audit algorithms. They can also create competitive advantage and compelling positioning and may ultimately be incentivized through legislation.

Fourth, society-level awareness and understanding of digital compromise, as it is embedded in the dynamic nature of technological innovation and reciprocal norms, is essential. Key entities—consumers, organizations, and the iron triangle—must have opportunities and platforms to engage in difficult conversations around these topics. Just as media and information literacy education has gained traction globally (e.g., UNESCO, 2011), literacy around digital compromise should be an essential topic for K-12 school curricula. Outside schools, dialogue on costs and benefits of marketplace exchanges via technology (and for whom) might be achieved through grassroots movements and consumer activism spearheaded by those most knowledgeable and connected. When more stakeholders engage in difficult conversations around these topics, creative solutions emerge. With clear understanding of the compromises involved in technology-mediated marketplace exchanges, more informed choices are possible. Our research adds to this conversation and helps clarify this vision.

9.3 | An agenda for future research

Future research should address how consumers and organizations negotiate and make decisions for themselves or with others regarding compromises in the digital environment, as well as how these compromises affect consumer, organizational, and societal well-being. In addition, researchers should carefully consider the legislative protections required to maintain balance in the face of tensions surrounding digital exchange. How legislative protections work and their intended (and unintended) consequences should also be explored across individuals, firms, interest groups, and society.

The perspectives described in Table 1 can motivate future research across these key exchange entities and are drawn from our understanding of digital compromises. This research carefully explains the model foundations and offers necessary components to achieve such balance. Doing so may preserve important norms and offset observed tendencies toward even greater crises.

These research opportunities highlight an overarching need to articulate the reciprocity norms—or lack thereof—governing digital exchange now and in the future. Ideally, digital exchange should be governed by equity, fairness, honesty, respect, and trust. This normative proposition, however, begs the question of feasibility. Amid the fluidity of ongoing technological change, can consumers, organizations, and the iron triangle simultaneously acknowledge, communicate, and operationalize shared norms of reciprocity to govern their heterogeneous, often misaligned, and sometimes conflicting goals and motivations?

Marketers thrive on heterogeneity in the marketplace, yet heterogeneity also presents challenges in realizing shared norms of reciprocity. The philosopher Paul Grice approached a similar problem in his study of language, meaning, and implicature (Neale, 1992). His maxims of cooperative communication—quantity, quality, relation, and manner—insist on communicating no more than necessary (quantity), only what is believed to be true (quality), only that which is most relevant (relation), and in an orderly and clear fashion (manner). Assuming that digital exchange is somewhat universal, communication that adheres to these maxims should allow consumers, organizations, and the iron triangle to be clear about the costs and benefits of their exchanges, with the shared goal of reaching optimal outcomes (i.e., less compromise and less friction in exchange).

However, as with neoclassical economic theory, Grice assumes that exchange partners are rational, cooperate, and share background knowledge. Unfortunately, the assumption of shared background knowledge seems unlikely to hold in digital exchanges. As we have described, background knowledge of the costs and benefits of digital exchange is often opaque to consumers (and the iron triangle) than to organizations. Lobbying attempts by organizations such as Google, Meta, Apple, and Amazon currently have unique advantages due to their power over the technology employed. While consumers and the iron triangle may never understand the intricacies of digital exchange to the same degree as these large organizations and the efforts they exert to influence the iron triangle, society can still strive toward rational cooperation. Cooperation lies at the heart of marketing as it promotes more efficient marketing systems and a better understanding of exchange partners (Mittelstaedt et al., 2006). In essence, cooperation requires respect; it requires empathy among exchange partners, a clear understanding of the needs and wants of the other, and a view of the world from the perspective of the other (Ashworth & Bourassa, 2020). An important challenge for future research on digital compromise is identifying ways to encourage shared norms of reciprocity through cooperation and respect.

ORCID

Monica C. LaBarge https://orcid.org/0000-0002-3972-3025
Kristen L. Walker https://orcid.org/0000-0003-2021-7621
Alexei Gloukhovtsev https://orcid.org/0000-0003-3811-4073
James Leonhardt https://orcid.org/0000-0002-4633-9363
Mehrnoosh Reshadi https://orcid.org/0000-0001-8069-2198

ENDNOTE

[1] We focus on the United States because it offers a unique view of environmental complexity and privacy policies are still evolving or disaggregated compared to, for example, the EU GDPR. However tensions and compromises exist in other countries and are worth exploring further.

REFERENCES

Achauer, H. (2021) Is it time to stop using your fitness tracker? *The Washington Post*. Available at: https://www.washingtonpost.com/wellness/2021/12/21/fitness-activity-tracker-obsession-unhealthy/.

Adams, G. (1989) *The iron triangle: the politics of defense contracting*. New Brunswick, NJ: Transaction Publishers.

Adorjan, M. & Ricciardelli, R. (2019) A new privacy paradox? Youth agentic practices of privacy management despite "nothing to hide" online. *Canadian Review of Sociology/Revue canadienne de sociologie*, 56(1), 8–29.

Aguirre, E., Mahr, D., Grewal, D., De Ruyter, K. & Wetzels, M. (2015) Unraveling the personalization paradox: the effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, 91(1), 34–49.

Antonio, M.G., Petrovskaya, O. & Lau, F. (2019) Is research on patient portals attuned to health equity? A scoping review. *Journal of the American Medical Informatics Association*, 26(8–9), 871–883.

Ashworth, L. & Bourassa, M.A. (2020) Inferred respect: a critical ingredient in customer satisfaction. *European Journal of Marketing*, 54(10), 2447–2476.

Ashworth, L. & Free, C. (2006) Marketing dataveillance and digital privacy: using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics*, 67(2), 107–123.

Bagozzi, R.P. (1975) Marketing as exchange. *Journal of Marketing*, 39(4), 32–39.

Bak-Coleman, J.B., Alfano, M., Barfuss, W., Bergstrom, C.T., Centeno, M.A., Couzin, I.D. et al. (2021) Stewardship of global collective behavior. *Proceedings of the National Academy of Science*, 118(27), e2025764118. https://doi.org/10.1073/pnas.2025764118

Bandara, R., Fernando, M. & Akter, S. (2021) Managing consumer privacy concerns and defensive behaviours in the digital marketplace. *European Journal of Marketing*, 55(1), 219–246.

Battilana, J., Leca, B. & Boxenbaum, E. (2009) How actors change institutions: towards a theory of institutional entrepreneurship. *Academy of Management Annals*, 3(1), 65–107.

Birch, K., Cochrane, D.T. & Ward, C. (2021) Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech. *Big Data & Society*, 8(1), 20539517211017308.

Bleier, A., Goldfarb, A. & Tucker, C. (2020) Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, 37(3), 466–480.

Chen, J.V., Ross, W. & Huang, S.F. (2008) Privacy, trust, and justice considerations for location-based mobile telecommunication services. *Info*, 10(4), 30–45.

Cisco. (2019) Consumer privacy survey: the growing imperative of getting data privacy right. *CISCO Cybersecurity Series*, 1–14.

Dendere, R., Slade, C., Burton-Jones, A., Sullivan, C., Staib, A. & Janda, M. (2019) Patient portals facilitating engagement with inpatient electronic medical records: a systematic review. *Journal of Medical Internet Research*, 21(4), 12779.

Dou, W. (2004) Will internet users pay for online content? *Journal of Advertising Research*, 44(4), 349–359.

Emerson, R.M. (1976) Social exchange theory. *Annual Review of Sociology*, 2, 335–362.

Espinoza, J. (2021) Brussels faces test of its will to tackle big tech. *Financial Times*. Available from: https://www.ft.com/content/961def63-4f55-469c-b9d9-08cfe443bbc0

Etkin, J. (2016) The hidden cost of personal quantification. *Journal of Consumer Research*, 42(6), 967–984.

Fernandes, T. & Pereira, N. (2021) Revisiting the privacy calculus: why are consumers (really) willing to disclose personal data online? *Telematics and Informatics*, 65, 101717.

Gaskell, G., Eyck, T.T., Jackson, J. & Veltri, G. (2005) Imagining nanotechnology: cultural support for technological innovation in Europe and the United States. *Public Understanding of Science*, 14(1), 81–90.

Gilly, M.C., Celsi, M.W. & Schau, H.J. (2012) It don't come easy: overcoming obstacles to technology use within a resistant consumer group. *Journal of Consumer Affairs*, 46(1), 62–89.

Globe and Mail (2021). Quebec politicians' Covid-19 vaccine passport QR codes allegedly hacked, police complaints filed. https://www.theglobeandmail.com/canada/article-quebec-politicians-covid-19-vaccine-passport-qr-codes-allegedly-hacked/

Golden, M.M. (1998) Interest groups in the rule-making process: who participates? Whose voices get heard? *Journal of Public Administration Research and Theory*, 8(2), 245–270.

Hart, R. (2021) Not just Austria—here are the countries making Covid-19 vaccination compulsory for everyone. *Forbes*, November 19, 2021. https://www.forbes.com/sites/roberthart/2021/11/19/not-just-austria-here-are-the-countries-making-covid-19-vaccination-compulsory-for-everyone/?sh=1b7cf9714bf0

Haucap, J. & Heimeshoff, U. (2014) Google, Facebook, Amazon, eBay: is the internet driving competition or market monopolization? *International Economics and Economic Policy*, 11(1–2), 49–61.

Hill, R.P. & Martin, K.D. (2014) Broadening the paradigm of marketing as exchange: a public policy and marketing perspective. *Journal of Public Policy & Marketing*, 33(1), 17–33.

Hofmann, W., Baumeister, R.F., Förster, G. & Vohs, K.D. (2012) Everyday temptations: an experience sampling study of desire, conflict, and self-control. *Journal of Personality and Social Psychology*, 102(6), 1318–1335.

Johnson, C., Richwine, C. & Patel, V. (2021) *Individuals' access and use of patient portals and smartphone health apps*. ONC Data Brief. Report number: 57

Kalaignanam, K., Tuli, K.R., Kushwaha, T., Lee, L. & Gal, D. (2021) Marketing agility: the concept, antecedents, and a research agenda. *Journal of Marketing*, 85(1), 35–58.

Kane, G.C., Palmer, D., Phillips, A.N., Kiron, D. & Buckley, N. (2019) Accelerating digital innovation inside and out: agile teams, ecosystems, and ethics. *MIT Sloan Management Review*, 1–31.

Kent, J. (2020) Self-tracking over time: from the use of Instagram to perform optimal health to the protective shield of digital detox. *Social Media + Society*, 6(3), 2056305120940694.

Kim, T., Barasz, K. & John, L.K. (2019) Why am I seeing this ad? The effect of ad transparency on ad effectiveness. *Journal of Consumer Research*, 45(5), 906–932.

Kozlenkova, I.V., Palmatier, R.W., Fang, E., Xiao, B. & Huang, M. (2017) Online relationship formation. *Journal of Marketing*, 81(3), 21–40.

Kruse, C.S., Argueta, D.A., Lopez, L. & Nair, N. (2015) Patient and provider attitudes toward use of patient portals for the management of chronic disease: a systematic review. *Journal of Medical Internet Research*, 17(2), 40.

Latulipe, C., Mazumder, S.F., Wilson, R.K.W., Talton, J.W., Bertoni, A.G., Quandt, S.A. et al. (2020) Security and privacy risks associated with adult patient portal accounts in us hospitals. *JAMA Internal Medicine*, 180(6), 845–849.

Lee, J.M. & Rha, J.W. (2016) Personalization-privacy paradox and consumer conflict with the use of location-based mobile commerce. *Computers in Human Behavior*, 63, 453–462.

Leite, F.P. & Baptista, P.P. (2021) The effects of social media influencers' self-disclosure on behavioral intentions: the role of source credibility, parasocial relationships, and brand trust. *Journal of Marketing Theory and Practice*, 30(3), 295–311.

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M. et al. (2021) Corporate digital responsibility. *Journal of Business Research*, 122, 875–888.

Lutzker, M.A. (1982) Max Weber and the analysis of modern bureaucratic organization: notes toward a theory of appraisal. *The American Archivist*, 45(2), 119–130.

Martin, K. & Murphy, P.E. (2017) The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135–155.

Martin, K., Borah, A. & Palmatier, R. (2017) Data privacy: effects on customer and firm performance. *Journal of Marketing*, 81(1), 36–58.

Marwick, A. & Hargittai, E. (2019) Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society*, 22(12), 1697–1713.

Mikalef, P., Krogstie, J., Pappas, I.O. & Pavlou, P. (2020) Exploring the relationship between big data analytics capability and competitive performance: the mediating roles of dynamic and operational capabilities. *Information & Management*, 57(2), 103–169.

Mittelstaedt, J.D., Kilbourne, W.E. & Mittelstaedt, R.A. (2006) Macromarketing as agorology: macromarketing theory and the study of the agora. *Journal of Macromarketing*, 26(2), 131–142.

Nadkarni, A. & Hofmann, S.G. (2012) Why do people use Facebook? *Personality and Individual Differences*, 52(3), 243–249.

Neale, S. (1992) Paul Grice and the philosophy of language. *Linguistics and Philosophy*, 15(5), 509–559.

Okada, E.M. & Hoch, S.J. (2004) Spending time versus spending money. *Journal of Consumer Research*, 31(2), 313–323.

Ortiz, J., Chih, W.H. & Tsai, F.S. (2018) Information privacy, consumer alienation, and lurking behavior in social networking sites. *Computers in Human Behavior*, 80, 143–157.

Overman, E.S. & Simanton, D.F. (1986) Iron triangles and issue networks of information policy. *Public Administration Review*, 46, 584–589.

Palmatier, R.W., Scheer, L.K., Evans, K.R. & Arnold, T.J. (2009) Achieving relationship marketing effectiveness in business-to-business exchanges. *Journal of the Academy of Marketing Science*, 36(2), 174–190.

Perez, A.J. (2019) Use a fitness app to track your workouts? Your data may not be as protected as you think. *USA Today*. August 16, 2019. https://www.usatoday.com/story/sports/2019/08/16/what-info-do-fitness-apps-keep-share/1940916001/

Poell, T., Nieborg, D. & Dijck, J. (2019) Platformisation. *Internet Policy Review*, 8(4), 1–13.

Reddy, N. (2018) How to harness the power of network effects. *Forbes*. Available from: https://www.forbes.com/sites/forbescoachescouncil/2018/01/02/how-to-harness-the-power-of-network-effects/?sh=6085a8fe62e8.

Reeves, M. & Whitaker, K. (2020) *The why of digital transformation*. BCG Henderson Institute Available from: https://www.bcg.com/en-us/publications/2020/the-power-of-digital-transformation

Schein, E.H. (2010) *Organizational culture and leadership*. San Francisco, CA: Jossey-Bass.

Scott-Railton, J. (2018) *Fit leaking: when a Fitbit blows your cover*. Available from: https://www.johnscottrailton.com/fit-leaking/.

Shabana, K.M., Buchholtz, A.K. & Carroll, A.B. (2017) The institutionalization of corporate social responsibility reporting. *Business & Society*, 56(8), 1107–1135.

Shackelford, S.J. (2012) Should your firm invest in cyber risk insurance? *Business Horizons*, 55(4), 349–356.

Shepardson, D. (2021) U.S. extends covid vaccine requirements for non-citizens at land borders. *Reuters*. Available from: https://www.reuters.com/world/americas/us-extends-covid-vaccine-requirements-non-citizens-land-borders-2022-04-21/.

Sullivan, M. (2018) Members of congress can't possibly regulate Facebook: they don't. *Washington Post*. Available from: https://www.washingtonpost.com/lifestyle/style/members-of-congress-cant-possibly-regulate-facebook-they-dont-understand-it/2018/04/10/27fa163e-3cd1-11e8-8d53-eba0ed2371cc_story.html.

Summers, M. (2020) Facebook isn't free: zero-price companies overcharge consumers with data. *Behavioural Public Policy*, 1–25. https://www.cambridge.org/core/journals/behavioural-public-policy/article/facebook-isnt-free-zeroprice-companies-overcharge-consumers-with-data/130959160E179EF37705E6E60336D0CA#article

Suoniemi, S., Meyer-Waarden, L., Munnzel, A., Zablah, A.R. & Straub, D. (2020) Big data and firm performance: the roles of market-directed capabilities and business strategy. *Information and Management*, 57(7), 103365.

Tapuria, A., Porat, T., Klara, D., Dsouza, G., Xiaojhui, S. & Curryn, V. (2021) Impact of patient access to the electronic health record: systematic review. *Informatics for Health and Social Care*, 46(2), 194–206.

Torre, I., Sanchez, O.R., Koceva, F. & Adorni, G. (2018) Supporting users to take informed decisions on privacy settings of personal devices. *Personal and Ubiquitous Computing*, 22(2), 345–364.

Truong, K. (2020) The Garmin ransomware hack is horrifying. Vice.com. Available from: https://www.vice.com/en/article/5dzkd5/the-garmin-ransomware-hack-is-horrifying.

UNESCO (2011) Media and information literacy curriculum for teachers. Available from: https://unesdoc.unesco.org/ark:/48223/pf0000192971.

Van Dijck, J. (2021) Seeing the forest for the trees: visualizing platformization and its governance. *New Media & Society*, 23(9), 2801–2819.

Walker, K.L. (2016) Surrendering information through the looking glass: transparency, trust, and protection. *Journal of Public Policy & Marketing*, 35(1), 144–158.

Walker, K.L., Milne, G.R. & Weinberg, B.D. (2019) Optimizing the future of innovative technologies and infinite data. *Journal of Public Policy & Marketing*, 38(4), 403–413.

White, T.B. (2004) Consumer disclosure and disclosure avoidance: a motivational framework. *Journal of Consumer Psychology*, 14(1–2), 41–51.

Yallop, A.C., Gică, O.A., Moisescu, O.I., Coroş, M.M. & Séraphin, H. (2021) The digital traveller: implications for data ethics and data governance in tourism and hospitality. *Journal of Consumer Marketing*. https://doi.org/10.1108/JCM-12-2020-4278

How to cite this article: LaBarge, M. C., Walker, K. L., Azzari, C. N., Bourassa, M., Catlin, J., Finkelstein, S., Gloukhovtsev, A., Leonhardt, J., Martin, K., Rejowicz-Quaid, M., & Reshadi, M. (2022). Digital exchange compromises: Teetering priorities of consumers and organizations at the iron triangle. *Journal of Consumer Affairs*, 1–24. https://doi.org/10.1111/joca.12471