Spotlight Report

REBUILDING RESPECTFUL RELATIONSHIPS IN THE DIGITAL REALM

Empowering Me2B Relationships through new legal and technical foundations for a complex digital ecosystem

Authored by Elizabeth M. Renieris[1]
Prepared for the Me2B Alliance
August 2020

[1] Elizabeth M. Renieris is a data protection and privacy lawyer (CIPP/E, CIPP/US), the Founder & CEO of HACKYLAWYER LLC, a Technology & Human Rights Fellow at the Carr Center for Human Rights Policy at the Harvard Kennedy School, and an Affiliate at the Berkman Klein Center for Internet & Society at Harvard University.

Table of Contents

ABSTRACT

With our lives under lockdown as COVID-19 rages on, our reliance on digital technologies and communications tools has perhaps never been greater, leading many to speculate that the pandemic has brought the digital future forward. At the same time, the shortcomings of digital life are now more apparent than ever, giving many a newfound appreciation for the value of human connection and relational states of being. In this context, the Me2B Alliance's efforts to recenter relationships in our digital lives takes on new meaning and urgency.

According to the Me2B Alliance, we have relationships with each of the product and service providers in our lives, in both the digital and physical spheres. In the digital sphere, our experience of these primary relationships is often through a digital product or service, such as a website, app, or connected device. Each of these digital relationships has at least three core dimensions—commercial, technical, and legal. They are primarily business and legal relationships mediated by a variety of hardware and software tools.

The technical dimension of digital relationships introduces a variety of intermediaries into our primary relationships and creates a parallel dimension of reality consisting of the data generated by transactions and interactions in the ordinary course of those relationships—a kind of "parallel dataverse." A commercial logic of extraction further complicates matters by introducing myriad parasitic entities who feed on and extract value from this parallel dataverse, undermining and distorting our primary relationships in the process.

Our prevailing legal paradigm for digital interactions stems from an overly simplistic and antiquated view of the digital universe, accounting only for primary relationships, without considering the impact of an increasingly complex digital realm and growing parallel dataverse. By only accounting for one dimension of our digital lives, this legal paradigm and its associated legal ceremonies leaves us exposed and vulnerable with insufficient safeguards and protections.

An alternative path forward must recalibrate our relationships and interactions in light of this increasingly complex and multidimensional view of the digital ecosystem. While digital will always be different, requiring intermediaries who enable our primary relationships, the more we can translate norms and expectations from the physical world into the digital realm, the closer we get to establishing effective standards and rules for our digital interactions.

Our legal paradigms must also evolve to capture this new reality by introducing base-level protections through prohibitions on certain activities and practices, mandating a risk-based approach to digital products and services, reestablishing context for our digital interactions, limiting default data collection and processing to what is necessary for primary business purposes, and imposing higher standards and obligations on parties who seek to go beyond what is necessary in the context of a bonafide commercial relationship.

Through this new paradigm, we can more easily define rules and norms for digital interactions that map to our expectations, according to the nature of our relationship to a given product or service provider. At the same time, we can also leverage and harness technology itself in the service of, rather than for purposes of extracting value from, these primary relationships. With new legal and technological foundations in place, the hope is to rebuild our digital relationships based on an ethos of mutual respect, in line with the Alliance's mission.

INTRODUCTION

The Me2B Alliance (the "Alliance") is an innovative standards development organization whose mission is to grow the availability of trustworthy technology choices in part through a certification mark (like the "Organic" food label) that helps people understand how a connected product or service is treating them and their personal information. The work of the Alliance is premised on the existence of a relationship between an individual (a "Me") and a business providing that individual with a product or service (a "B"), known as the "Me2B Relationship." Additionally, the Alliance has developed a series of principles ("Me2B Principles") and ethical rules of engagement ("Me2B Rules of Engagement") that apply in and out of Me2B Relationships (see Appendix A - Me2B Materials).[2]

The Alliance is now exploring alternatives to the prevailing "notice and choice" or "notice and consent" model for Web-based user interactions, based on whether or not an individual is in a Me2B Relationship with a given service provider. This paper is the result of a series of interviews and conversations with key stakeholders in the Me2B community,[3] including Me2B leadership, participation in a series of Policy and Legal Working Group meetings, an analysis of pre-existing Me2B materials, and relevant research and scholarship. The Alliance is encouraged to view this whitepaper as a starting point for a long-term conversation about overhauling the context for, and nature of, our Web-based interactions in a way that more closely aligns with the Me2B Principles and Me2B Rules of Engagement.

This paper proceeds in five parts. Part I begins by examining the Me2B Relationship in context, including in the macro-context of a phenomenon known as surveillance capitalism, which distorts and undermines the very ethos of the Me2B Relationship. Part II outlines the failures of the prevailing "notice and choice" paradigm for digital interactions, including its legal and practical defects, as well as how such defects result from a failure to account for the effects of surveillance capitalism. Part III seeks to provide an alternative path forward by mapping the expectations we have in the physical world onto the digital world, including through new legal foundations and innovative uses of technology to realign expectations and reality. Part IV examines what digital interactions might look like in this new paradigm, according to the relevant Me2B Relationship state. Finally, Part V draws some conclusions and recommends next steps for research and exploration by the Alliance.

I. FOUNDATIONS OF THE M2B RELATIONSHIP

This section examines the Me2B Relationship in context by first examining the nature of digital interactions and the role of intermediaries. It also explains how the prevailing logic of surveillance capitalism creates a kind of "parallel dataverse" that distorts the nature of Me2B Relationships and undermines the interests of the individual, i.e. the "Me."

A. A MULTIDIMENSIONAL RELATIONSHIP

According to the Alliance, we have two-sided or 1:1 "relationships" with each of the product and service providers in our lives, in both the physical and digital spheres.[4] In the physical realm, these relationships have at least two core dimensions: (1) a commercial dimension, typically in the form of exchanges of mutually agreed upon value, and (2) a legal dimension, typically in the form of a contract, such as a sales receipt, membership

[2] While essential when in a Me2B Relationship, the Me2B Principles and Me2B Rules of Engagement are also intended as defaults for respectful behavior whether in or out of a Me2B Relationship. Conversation with Lisa LeVasseur on 8-20-2020.
[3] From June through August 2020, the author conducted a series of interviews with Me2B community members, including Lisa LeVasseur, Nancy Kim, Scott David, Nathan Kinch, Eve Maler, and Richard Whitt, and attended a series of PaLs Working Group meetings.
[4] *See* Lisa LeVasseur, Me2B Webinar (July 3, 2020), at slide 30 (hereinafter "Me2B Webinar"). While the alliance has defined a Me2B Relationship as a "two-way relationship that exists between a person and a product or a service," the law recognizes relationships between people and other people and/or legal entities. Thus, Me2B Relationships to products and/or services are actually relationships between an individual and a product or service provider, typically a commercial entity.

agreement, or loyalty subscription. Additionally, where a physical or in-person interaction has a digital component, such as a digital payment method, there is a third technical dimension.

In the digital realm, each of our interactions and relationships has all three dimensions—commercial, technical, and legal. Commercially, there are actual and potential transactions or exchanges of value in return for products and services. Technically, these commercial transactions or exchanges are achieved via an array of hardware and software products and services. And legally, there are formalities that establish certain legal relationships between the various parties to a given digital interaction or transaction. Due to a phenomenon known as surveillance capitalism (as further outlined below), there is also a fourth hidden dimension.

1. Commercial

Commercially, our relationships are created through interactions and sharing over time.[5] In general, these relationships tend to evolve according to a lifecycle consisting of five key stages: (1) acquaintance, (2) buildup, (3) continuation, (4) deterioration, and (5) termination, per Figure 1 below.[6] A Me2B Relationship begins with a specific ceremony, such as signing up for an account, joining a loyalty program, agreeing to a website's terms of service, or any other process by which individual credentials are created establishing a business relationship between a "Me" and a "B."

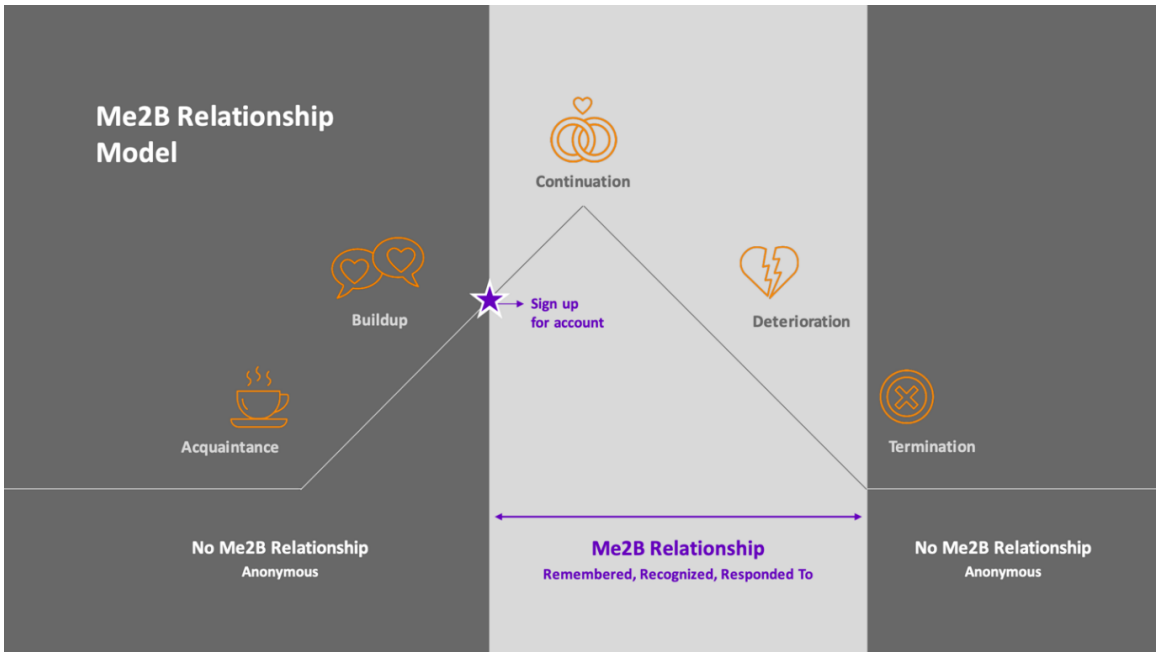

Figure 1 - Me2B Relationship Model

According to the Alliance, a Me2B Relationship is characterized by the individual having agency throughout the entire relationship lifecycle, including when to start and end the relationship, as well as what data to share or keep private, among other considerations.[7] Before a Me2B Relationship is formed, and before a business relationship requires sharing personal information or exchanging value, the individual should have a reasonable expectation of anonymity. As she approaches the start of a Me2B Relationship and gets closer to establishing that business relationship, she gradually loses anonymity, becoming more pseudonymous or identifiable to a given service provider over time.

[5] *See* "Me2B Relationships," Me2B.org, https://www.me2ba.org/principles
[6] This is known as the George Levinger relationship ABCDE lifecycle model, *see* https://en.wikipedia.org/wiki/Interpersonal.
[7] *See* "Me2B Principles" at https://www.me2ba.org/principles,

Once in a Me2B Relationship with a given service provider, the individual becomes personally identifiable. Nevertheless, she should still have the choice to remain unknown or anonymous in respect of specific transactions or interactions with that provider. Upon termination of the Me2B Relationship, she should be forgotten by and return to a state of anonymity in relation to that entity. In this way, a Me2B Relationship can also be described as a state of being "recognized, remembered, and responded to" by a given entity.[8]

In order to exercise this kind of agency, individuals must be able to accurately identify the counterparties to a given interaction or transaction, which entities they are in relationship with, and where they are in the relationship lifecycle in relation to each entity, and be able to adjust their expectations accordingly. Undergirding the Me2B Relationship is a "Me2B ethos" or a core belief that a respectful relationship between an individual and the technology they are using, whether a website, connected device, app, or otherwise, benefits the individual and the service provider. Unfortunately, the complexity of the digital ecosystem as it exists today undermines both individual agency and the Me2B ethos.

2. Technical

While offline, in-person interactions require the physical presence or proximity of the parties, digital interactions do not. Rather, individuals (Me-s) and product or service providers (B-s) are connected by some combination of technical tools and architecture, typically provided by commercially owned and operated entities known as "technical intermediaries."[9] In the prevailing centralized, client-server model of the Web, these technical intermediaries include hardware and software providers that "serve" an end user or "client" with access to certain digital resources from a "B," as requested by the end user.[10] In this way, the digital version of a Me2B Relationship can be recharacterized as a kind of "Me–T–B" relationship.

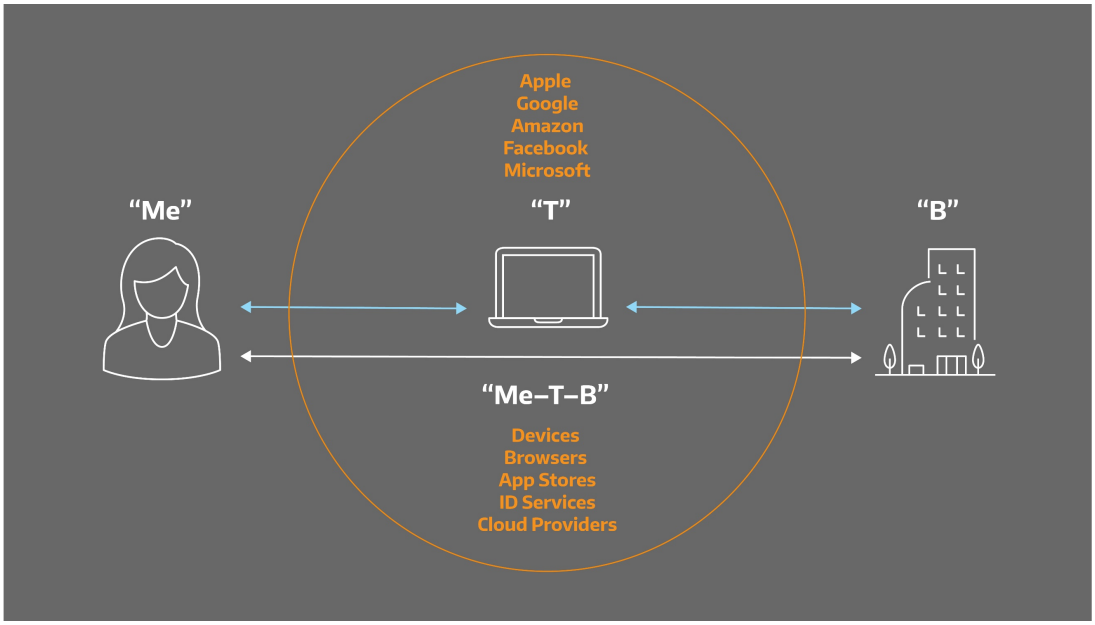

Figure 2 - Technical intermediaries & the "Me–T–B" relationship

[8] *See* Me2B Webinar, *supra* note 4. *See also* Joe Andrieu, "Five Mental Models of Identity," Rebooting Web of Trust 7 Toronto (Sept. 2018), available at https://github.com/WebOfTrustInfo/rwot7-toronto/blob/master/topics-and-advance-readings/five-mental-models-of-identity.md.

[9] In fact, if digital infrastructure and tools were publicly owned or operated, as in the case of government owned or operated utilities, much of the resulting analysis in this whitepaper might be different.

[10] In an alternative decentralized, peer-to-peer model of computing, end users could connect directly through functionally equivalent devices that can act as both clients and servers, capable of requesting and retrieving the relevant resources.

These technical intermediaries may include Web browsers (such as Google Chrome or Apple's Safari), app stores (such as Google Play and the App Store), identity services (such as "login with Facebook" or "login with Google"), cloud services providers (such as Amazon Web Services or Microsoft's Azure), and device manufacturers (such as Apple and Google), among others. From the perspective of a "Me" trying to do business with a "B," we often overlook the importance of these technical intermediaries and their impact on our relationships. When interacting or transacting with a "B" through a device by digital means, we tend to view our commercial relationship with the "B" as primary and our relationships with T-s as secondary.

3. Legal

Though they may feel secondary, we are in primary legal relationships with technical intermediaries who facilitate our digital Me2B Relationships. Thus, we can also classify these technical intermediaries in terms of their legal status in relation to the "Me" in a given interaction. Those in privity of contract, i.e. in a direct contractual relationship, with the "Me" are "first parties" who sit in between the primary parties to a commercial transaction or interaction, with obligations to both sides. In the current paradigm of Me2B Relationships, a "Me" has a direct contractual relationship with the "B" and a parallel contractual relationship with each first-party technical intermediary who facilitates it.[11]

Additionally, there are a variety of intermediaries who are not in privity, i.e. not in a direct contractual relationship with, the "Me" in a given transaction or interaction but are in a direct contractual relationship with the "B" or a "T" involved. From the perspective of "Me," these are "third parties" or "third-party intermediaries" and may include payment processors, data processors, and other vendors and participants in a supply chain who are acting on behalf of a "B" or a "T" in the course of their ordinary business operations. Such third parties are necessary to provide technical or commercial functionalities in support of the primary business relationships between a "B" and its customers.

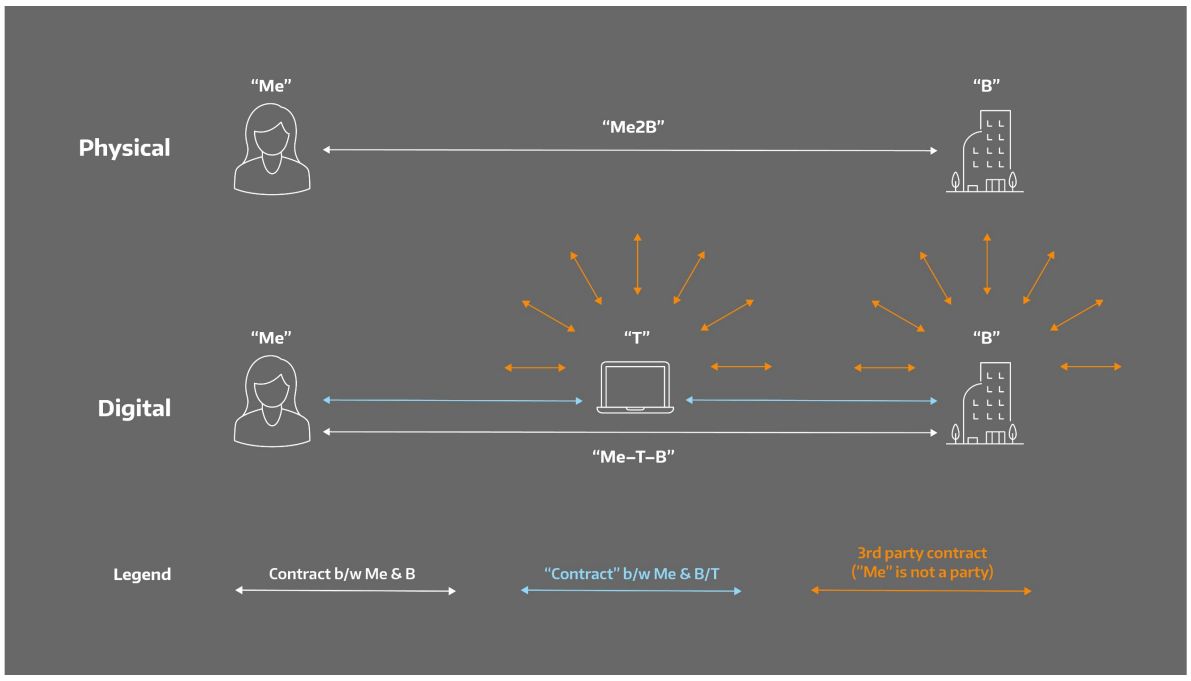

Figure 3 - First- and third-party intermediaries

[11] The problem is that individuals are forced into contractual relationships with product and service providers in the digital realm even when they are not in a Me2B Relationship State with that product or service provider. As explained below, there are significant issues with the validity of these "contracts." *See* text accompanying notes 37-41.

Oddly, there are also a number of entities who are not commercially or technically necessary for a transaction or interaction between a "Me" and a "B" but who are lurking in the ambient digital environment around their relationship. Because they exist to extract value from Me2B Relationships but lack a direct or indirect relationship to the "Me" in a given relationship, they are akin to "parasites." That digital interactions require an array of technical and commercial intermediaries does not by itself explain the presence of these parasites. Rather, their pernicious nature is the product of a particular phenomenon known as surveillance capitalism and its resulting distortions of the digital ecosystem.

B. ON SURVEILLANCE CAPITALISM

Through their devices, browsers, authentication protocols, communications tools, and other infrastructure, it is almost impossible to interact or transact by digital means without the involvement of companies like Apple, Google, Facebook, Amazon, and Microsoft, among others. The reality is that large corporate intermediaries who provide the connective tissues of our digital relationships penetrate even the most intimate aspects of digital life.[12] Unfortunately, many of these entities also participate in a new economic order known as "surveillance capitalism," which "claims human experience as free raw material for hidden commercial practices of extraction."[13] This extractive logic results from, and results in, vast asymmetries of power along at least four dimensions.

1. Scale

With two and three billion users worldwide, Google and Facebook, respectively, have more users than the population of the largest countries on earth, reaching more people than governments, traditional media outlets, publishers, and any other platform in history.[14] Scale is also concentrated in the market for mobile devices and applications. Together, Apple and Google control 99% of global market share[15] and act as gatekeepers for all apps designed for iPhone and Android devices; in effect, all devices.[16] Similarly, Amazon, Microsoft, and Google control more than 60% of the market for cloud services.[17] As a result, many service providers or B-s have little choice but to accept the terms set by the surveillance capitalists, often compromising their relationships with Me-s in the process by sharing their data.

2. Information

Given their size and scale, and aided by exponentially increasing computational power, the surveillance capitalists have unmatched tools to collect and harness vast hordes of data and, in turn, to derive behavioral, psychological, and other insights about people, groups, and societies at large. They track and analyze our thoughts, preferences, and behaviors, leading many to conclude that privacy is dead. Meanwhile, the inverse is true of these intermediaries. Due to opaque algorithms (the so-called "black box" phenomenon), robust intellectual property rights and trade secrets, and limited technical competence on the part of law and

[12] *See* Kashmir Hill, "I Tried to Live Without the Tech Giants. It was Impossible," NY Times (July 31, 2020), available at https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html.
[13] Although there is no singular definition of the multi-dimensional concept of "surveillance capitalism," this one is most relevant for purposes of this whitepaper. *See* Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs (2019), at "The Definition" (hereinafter "Surveillance Capitalism").
[14] Even top news outlets like CNN and FOX News only reaching a few million combined. *See* Rick Porter, "TV Ratings: Cable News Has Record-Setting Second Quarter," The Hollywood Reporter (June 30, 2020), available at https://www.hollywoodreporter.com/live-feed/tv-ratings-cable-news-has-record-setting-second-quarter-1301220.
[15] *See* S. O'Dea, "Market share of mobile operating systems worldwide 2012-2020," Statista (Aug. 17, 2020), available at https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/.
[16] For example, we have seen this dominance play out in the public health response to contact tracing and exposure notification in response to the COVID-19 pandemic, wherein Apple and Google have dictated the terms of such tools to governments by controlling access to their application programming interfaces (APIs). *See, e.g.*, Stephen Nellis & Paresh Dave, "Apple, Google ban use of location tracking in contact tracing apps," Reuters (May 4, 2020), available at https://www.reuters.com/article/us-health-coronavirus-usa-apps/apple-google-ban-use-of-location-tracking-in-contact-tracing-apps-idUSKBN22G28W.
[17] *See* Felix Richter, "Amazon leads $100 billion cloud market," Statista (Aug. 18, 2020), available at https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

policymakers trying to hold them to account, we know almost nothing about how their technology operates or how our data and any insights derived therefrom are used. As a result of the steep information asymmetries, we have fully transparent people and fully opaque platforms.

3. Resources

Asymmetrical scale and knowledge are further fueled by vastly asymmetrical resources as between individuals, service providers, surveillance capitalists, and their parasites. Through legal and accounting loopholes and aggressive lobbying, surveillance capitalists largely evade regulation and taxation.[18] Failing to account for their externalities, they undermine and rent-seek from traditional businesses, such as traditional news media and journalistic outlets, free ride on public infrastructure, and take advantage of taxpayer funded subsidies,[19] despite being among the richest companies of all time.[20] Worse yet, they divert limited resources that could support the development of alternative technologies to promote the interests of Me-s online, perpetuating toxic, extractive practices to maximize shareholder value instead.

4. Capacity for control

With multidimensional asymmetrical power, the surveillance capitalists have an unprecedented capacity to exert equally unprecedented behavioral control and experimentation on people, without legal limits. Through recommendation engines, hyper-personalization, psychometric profiling, behavioral advertising, micro-targeting, and other tools, they have the ability to influence and alter our preferences, our expression, and ultimately our behavior.[21] If mutual respect is a two-way street that recognizes both parties in a relationship as equally valuable in terms of their contributions and individual agency, a relationship built on the parasitic logic of extraction and control is a fundamentally one-sided relationship in which one party is more valuable to the other for purposes of extracting value.

C. THE HIDDEN DIMENSION

Taken together, these asymmetries distort the power dynamics between Me-s and B-s and undermine the foundation of the Me2B Relationship, an ethos of mutual respect, by introducing a fourth hidden dimension into the relationship.

1. The "parallel dataverse"

While data is relevant to and exchanged in all interactions, non-digital information gleaned from an offline interaction tends to be ephemeral, difficult to store, transfer, and otherwise process, and of limited market or industrial value as a result. In contrast, digital data generated in online or digital interactions is often permanent, cheap and easy to store, transfer, and process, and, as a result of surveillance capitalism, fed into a highly lucrative data economy.[22] The perverse power dynamics of surveillance capitalism distort Me2B Relationships, hosting an infinite number of parasites extracting value from them. Such parasites may include general and financial data brokers, commercial databases, fraud detection providers, ad networks and ad tech

[18] *See, e.g.,* Chloe Taylor, "Silicon Valley giants accused of avoiding over $100 billion in taxes over the last decade," CNBC (Dec. 2, 2019), available at https://www.cnbc.com/2019/12/02/silicon-valley-giants-accused-of-avoiding-100-billion-in-taxes.html.
[19] *See, e.g.,* Ethan Baron, "Google, Tesla, Apple, Facebook rake in massive subsidies: report," The Mercury News (July 3, 2018), available at https://www.mercurynews.com/2018/07/03/google-tesla-apple-facebook-rake-in-massive-subsidies-report/.
[20] *See, e.g.,* Jack Nicas, "Apple Reaches $2 Trillion, Punctuating Big Tech's Grip," NY Times (Aug. 19, 2020), available at https://www.nytimes.com/2020/08/19/technology/apple-2-trillion.htmlAp.
[21] In this way, the logic of surveillance capitalism is the same logic that undergirds all surveillance societies, including authoritarian regimes like China. The surveillance capitalist framing is an indirect form of authoritarianism vis-à-vis the government, but a direct one via behavioral control over our actions, decisions, and preferences. Moreover, when big tech aligns with Big Brother, individuals are arguably at even higher risk of manipulation, exploitation, and control, than from either acting alone.
[22] *See, e.g.,* Michael Fertik, "Why Your Data Will Never be Deleted," Forbes (June 9, 2015), available at https://www.forbes.com/sites/michaelfertik/2015/06/09/why-your-data-will-never-be-deleted/#3a401c952371.

companies, credit reporting agencies, and myriad other entities motivated by their own commercial interests. Surveillance capitalism coopts digital intermediaries in service of these parasites, subverting and exploiting Me2B Relationships in the process.

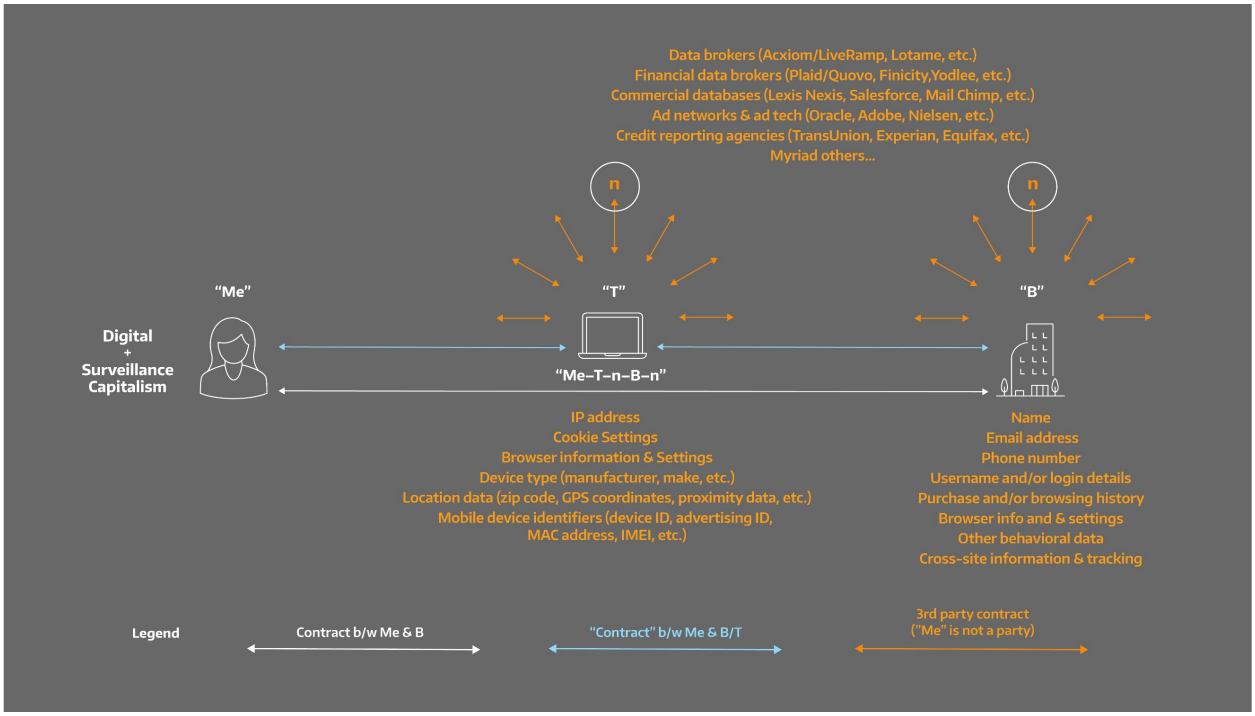

Figure 4 - Parasites and the Me-T-n-B-n relationship

While the parties to an offline, in-person interaction typically share a similar perspective and ability to assess the mechanics of that interaction, as well as the information and value exchanged, the same is not true of digital interactions. If relationships form the perceptible matter in the material universe around us, data forms the imperceptible anti-matter consisting of black box algorithms, dark patterns, and other hidden processes that feed these parasites. As a result, our digital lives exist in two parallel dimensions: (1) the realm of digital relationships, including Me2B Relationships; and (2) ambient data swirling in a kind of "parallel dataverse." We see, perceive, and participate in the former, while we tend not to see or perceive the latter, though it distorts our experience of digital relationships. Unwittingly and under the pretense and familiarity of relationships, the opaque parallel dataverse expands.[23]

2. Time and space in the parallel dataverse

While time and space are highly correlated in physical interactions, the same is not true for digital ones. The relationship between digital time and space is distorted by the parallel dataverse. A short-lived physical interaction, such as a one-off purchase, requires showing up to a place once.[24] A longer-lived series of physical interactions, as in the case of a regular customer, requires showing up repeatedly over time. In the digital realm, we can be in different places at the same time and persist in space over time through our data long after we stop showing up.[25]

[23] Each act that we see in isolation (e.g. sharing an email address with a vendor) expands the dataverse in ways unseen, exposing us to harms that we cannot assess (e.g. the risk of that email address being sold on the dark web to an identity thief).
[24] Although you may be recognized and responded to, you likely will not be remembered, and therefore not in a Me2B Relationship.
[25] Under the current paradigm of the Web, even a one-off retail purchase in "guest mode" can create a persistent and wide-reaching data trail spanning both time and space, as further explained below.

More concretely, take the example of a simple "Me2B Deal" or an exchange of mutually agreed upon value, such as going to a restaurant and paying $20 for a meal. The deal is a quid pro quo agreement that defines and bounds the scope of sharing, i.e. you give the restaurant $20 in cash and get a meal in return.[26] The same in-person interaction with a form of digital payment may look and feel the same but significantly complicates things. For example, if you pay with a credit card instead of cash, your credit card provider now has the restaurant or merchant information, details of your order, and potentially your location data. Pay with something like Apple Pay and now your credit card provider, telecommunications operator, and smart phone vendor may all have this information too.[27]

If you did this every week at the same restaurant, and became recognized, remembered, and responded to, you may expect to end up in a Me2B Relationship with the restaurant owner. However, you may not expect parasites in the parallel dataverse to compile and resell behavioral data about when you visit the restaurant, the details of your order, and where you were before and after each visit, among other insights about you. As a result of surveillance capitalism, even light-touch, short-lived interactions can form expansive and persistent data trails that extend through time and space across the parallel dataverse, the dimensions of which can be hard for individuals to grasp.[28] This sharing is both undefined and theoretically unbounded, violating the Me2B ethos.

II. CRACKS IN THE FOUNDATION: ON "NOTICE AND CHOICE"

The logic of extraction based on asymmetrical power is also antithetical to the notions of "choice" and "consent" that theoretically undergird the legal foundations of our digital relationships. The prevailing paradigm for digital interactions is "notice and choice," also called "notice and consent." Originating from the Fair Information Practices of the 1970s, it is predicated on the idea that users of an online service can make informed decisions about whether and how to transact or interact with a given entity or service provider on the basis of transparent disclosures about its information and privacy practices.[29] It still forms the foundation of the Federal Trade Commission's enforcement authority over "unfair and deceptive" trade practices, the primary enforcement tool over online activity in the U.S.[30] This section outlines the failures of "notice and choice," including its many legal and practical defects.

A. LEGAL DEFECTS

As U.S. companies like Apple, Google, Facebook, and others continue to dominate the global market for digital technologies, this framework has been exported to and imposed on individuals around the world, even influencing the application and interpretation of other legal frameworks.[31] Due to the ubiquity of "notice and consent," the two primary ceremonies we encounter in the digital realm are notices, typically in the form of a privacy policy or privacy notice, and contracts, in the form of terms and conditions or terms of service seeking our consent. We are also frequently presented with a variety of licenses. Our perception of these tools does not align with how they operate in practice.

[26] *See* "Me2B Relationships," Me2B Alliance, at https://www.me2ba.org/principles
[27] In fact, you cannot use Apple Pay without enabling location data. *See* Stilgherrian, "Apple Pay isn't magic, and it isn't 'private'," ZDNet (Oct. 27, 2014), available at https://www.zdnet.com/article/apple-pay-isnt-magic-and-it-isnt-private/.
[28] The same $20 transaction also arguably "costs" more when you pay by digital means because the transaction takes on a life of its own through the data collected and may later be exploited in the form of other currencies such as your time and attention when it is eventually harvested by parasites, advertisers, and other stakeholders in the parallel dataverse.
[29] *See* Federal Trade Commission, Privacy Online: A Report to Congress (1998), available at http://www.ftc.gov/sites/default/files/.
[30] *See* Section 5 of the Federal Trade Commission Act (15 U.S.C. 41 et seq.).
[31] For example, while Europe's General Data Protection Regulation (GDPR) is not a notice-and-consent law, it has largely been interpreted as such, with an overemphasis on individual consent as a lawful basis for processing personal data in digital interactions. *See* Dr. Gabriela Zanfir-Fortuna, *10 Reasons why the GDPR is the Opposite of a "Notice and Consent" Type of Law*, Future of Privacy Forum (Sept. 13, 2019), available at https://fpf.org/2019/09/13/10-reasons-why-the-gdpr.

1. Notices

A "notice" is a legal notification or warning delivered in a written format or as a formal announcement.[32] Online, notices typically take the form of a website or app's privacy notice, sometimes called a privacy policy. A notice is meant to be a transparency tool that provides clear but comprehensive disclosures on how a website or online service collects, uses, discloses, retains, and otherwise handles the information of its users.[33] On the basis of this notice, individuals are presumed to make informed choices about whether and how to share data or otherwise engage with the service. This is the "notice" prong of the "notice and choice" model.

Although "notice and choice" is touted as promoting individual autonomy, and consumers tend to perceive notices as making binding promises, courts have typically regarded online privacy notices as general statements of information policy rather than as legally enforceable contracts.[34] This is largely due to their passive presentment, often located on a separate webpage, without requiring a user to accept or even read them to proceed or use a website or service.[35] It has also been industry practice to draft privacy policies in ways that do not constitute legally enforceable agreements.

It is also due to the unilateral nature of notices, which bind all users of a website or service regardless of their relationship to the site owner or service provider. In practice and at law, privacy policies or notices actually act more like property notices that proffer one-way terms and attach in rem to a service provider's digital property, rather than in personam to an individual user. In other words, such notices act more like signage in a shopping mall.

2. "Contracts"

When we think of contracts online, we tend to think of terms and conditions or terms of service, and ceremonies like ticking a box or consenting to terms by clicking "I accept." These actions form the "choice" prong of "notice and choice." While property law is one-sided to favor the property owner, contract law seeks to equally protect both sides of a bargain. As such, a contractual basis for digital interactions should "facilitate certainty, predictability, and care in entering productive relationships,"[36] providing a better foundation for Me2B Relationships built on mutual respect. But the digital ceremonies we perceive as contracts often do not hold up in theory or in practice.

A contract is an agreement between private parties creating mutual obligations or legally enforceable promises.[37] The basic elements required for contract formation are mutual assent, expressed by a valid offer and acceptance, adequate consideration, capacity, and legality. Acceptance requires a "meeting of the minds" such that both parties to the contract understand what is being offered, i.e. that acceptance is identical to the offer. In determining whether an electronic contract has been validly formed, there must be "reasonable notice" of terms and a "manifestation of assent" by the consumer.[38] In this way, valid contract formation in the digital realm follows the "notice and consent" approach.

[32] *See* Black's Law (2019 Ed).
[33] *See* Richard Raysman & Peter Brown, *Contractual Nature of Online Policies Remains Unsettled*, N.Y.L.J., Aug. 10, 2010, at 2.
[34] *See* Thomas B. Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model,* 27 Fordham Intell. Prop. Media & Ent. L.J. 181 (2016).
[35] In other words, privacy policies or notices are akin to "browsewrap" rather than "clickwrap" and are largely unenforceable contracts. *See, e.g.,* L. LeVasseur and E. Maler, "Beyond Consent: A Right-to-Use License for Mutual Agency," in IEEE Communications Standards Magazine, vol. 3, no. 4, pp. 52-59, December 2019.
[36] Patterson, Mark, *Must Licenses Be Contracts? Consent and Notice in Intellectual Property*, 40 Fla. St. U. L. Rev. (2012), available at https://ir.law.fsu.edu/cgi/viewcontent.cgi?article=1017&context=lr, at 110.
[37] *See* Black's Law (2019 ed).
[38] *See* Kim, Nancy S., *Situational Duress and the Aberrance of Electronic Contracts* (February 27, 2014), Chicago-Kent Law Review, Vol. 89, No. 1, p. 265 (2014), at 267.

Unfortunately, courts also tend to interpret electronic contracts as acting more like property notices that need only be reasonably displayed and can be assented to by a user through mere use of a website or service, even where they are not seen or read by the user. In this way, digital "contracts" operate more like property instruments that protect digital property owners, undermining the rationale for relying on "notice and choice." As one scholar puts it, "the inutility of contract law for enforcing privacy policy promises calls into question the effectiveness and legitimacy of the Notice and Choice model for privacy protection."[39]

Finally, the unilateral ability of a service provider to modify the terms of an electronic contract at will, in a way that is more typical of notices, also means "the bargain itself is a moving target," making it hard to establish a meeting of the minds at a given point in time in the relationship lifecycle.[40] The decoupling of time and space that allows us to persist in the parallel dataverse through our data long after a transaction, interaction, or relationship ends, means that what we agree to in the moment of contract presentment and execution does not capture future uses of that data or activities with consequences on our lives. Moreover, the asymmetries of power and information that characterize our digital interactions in the surveillance capitalist paradigm further undermine any "meeting of the minds."

3. Licenses

Finally, we may encounter end-user license agreements (EULAs) and other licenses when we access a copy of software or download an app. A license is a grant of permission to do something otherwise prohibited by law.[41] Its nature is ill-defined as a license can be contractual or non-contractual.[42] Under intellectual property law, as in the case of a EULA, a license is a contract granting written permission to exploit an invention, creative work, or trademark, and must satisfy the rules for contract formation, including valid offer and acceptance. Under real property law, a license is a unilateral commitment to grant certain restricted rights to property even where a grantee is unaware of those restrictions.[43] A contractual license requires an act by the licensee that constitutes assent to its terms, while the licensee of a non-contractual license accepts its terms through performance, such as by entering a physical place or continuing to use a website. Contractual licenses have the same legal defects as digital contracts, as outlined above.

B. PRACTICAL DEFECTS

As a light-touch, self-regulatory mechanism, the "notice and choice" model is theorized to promote individual autonomy by centering the individual's informed consent and decisionmaking. However sound the theoretical foundations of "notice and choice," the model has not panned out in practice.[44]

1. Quantitative challenges

As more of the population comes online, the volume of digital interactions increases exponentially. We send more than one hundred and fifty million emails and sixteen million text messages each minute, while Google

[39] Norton, at 195.
[40] *See* Kim, *supra* note 38, at 274 ("Where the party seeking consent unilaterally makes a material change to their terms and conditions, terms of service, privacy policy, or any other relevant notices, the onus is on the individual to monitor and accede to the altered terms or else to opt out of the service. This is often not practical or possible, leaving the individual with limited actual choice in the matter.").
[41] *See* Black's Law. (2019 ed).
[42] *See* Patterson, *supra* note 36 ("Restrictive licenses lie at the intersection of property law and contract law. The usual way in which a private party is bound to restrictions on its conduct is by contract. But property law grants property owners the right to exclude others from their property.")
[43] *See id*.
[44] The GDPR does set a higher bar for consent than "notice and choice" does. Per the GDPR, data controllers are required to provide data subjects with transparent information, communication, and modalities for exercising their rights, typically through a written privacy notice; on the basis of this notice, the theory is that a data subject can provide a "freely given, specific, informed, and unambiguous indication" of consent by "a statement or clear affirmative action." *See* Art. 4(11), GDPR.

processes nearly four billion searches per day.[45] The frequency with which we have to accept or consent to a variety of legal terms and conditions via our digital interactions is already unmanageable. According to one study, it would take an average of seventy-six days to read the privacy policies of every website an individual encounters in one year.[46] The more people and devices that come online and connect as we approach a world with the "Internet in everything,"[47] the more unmanageable this will become.

The ubiquity of "notice and choice" has resulted in rather unpleasant user experience and user interface (UX/UI) features, including a variety of cookie pop-ups, banners, and tick boxes, among other nuisances, compounding the cognitive overload challenges. Efforts to require meaningful informed consent in Web-based interactions have actually worsened the problem. For example, UX/UI has been a key challenge in implementing Europe's ePrivacy Directive,[48] which outlawed passive or implied consent to cookies via banners or pre-ticked boxes and required affirmative, opt-in consent to all cookies not strictly necessary for a website's technical operation. Where complied with, it has resulted in a proliferation of popups and notifications.

"Notice and choice" also does not translate well to mobile devices with smaller interfaces or to emerging and future technologies. As we move beyond the graphical user interface (GUI) to new interfaces, including voice, gesture, and gait, as well as neural or brain-machine interfaces, implementing "notice and choice" will get even trickier. Add the proliferation of smart devices, the Internet of Things, and sensor technologies, and a corresponding growth in ambient data collection, and the idea of having written terms and conditions and privacy policies to accept on a regular basis in real-time through clicks and scrolls becomes wholly untenable. The lack of future proofing also demonstrates the unsustainability of the notice and choice paradigm.

2. Qualitative challenges

These quantitative challenges also result in qualitative challenges in practice. While commercial entities continue to benefit from exponential improvements in computational capacity and power, the cognitive limits of the human mind have remained relatively static or fixed. As a result, the cognitive strain of the "notice and choice" paradigm further increases the asymmetry of knowledge and capacity as between individuals and the entities seeking consent. It is difficult, if not impossible, to establish meaningful, informed consent under these circumstances, as it simply exceeds our capacity for good decisionmaking.[49]

"Notice and choice" is also applied uniformly to our relationships with product and service providers, whether B-s or T-s, despite our limited choice and the toxic business models of many T-s. These large commercial entities, so pervasive that they can be nearly impossible to avoid, intermediate most of our digital interactions.[50] As a result, "consent" for entering into "contractual" relationships with them is not freely rendered but results from limited choice,[51] anti-competitive tactics, and impediments to interoperability and data portability. Where we cannot interact with a B without accepting the terms of surveillance capitalist T-s,

[45] *See* Data Never Sleeps 5.0, DOMO, available at https://www.domo.com/learn/data-never-sleeps.
[46] *See* Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, The Atlantic, March 1, 2012 https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies.
[47] *See* DeNardis, Laura, *The Internet in Everything*, Freedom and Security in a World with No Off Switch, Yale University Press (2019).
[48] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.
[49] Privacy-related harms can be intangible, diffuse, and difficult to identify in isolation. Where individuals cannot easily perceive or identify harms, they may be further disincentivized from reading terms and conditions or privacy notices. *See, e.g.,* Danielle K. Citron & Daniel Solove, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 Texas Law Review 737 (2018).
[50] *See* Hill, *supra* note 12.
[51] For example, the German Federal Court of Justice recently held that Facebook users face a false choice in "consenting" to the comingling of their personal data across various Facebook services, including Facebook, Messenger, Instagram, and WhatsApp, due to the ubiquity and near impossibility of avoiding these services in practice. *See* https://www.nytimes.com/2020/06/23/technology/facebook-antitrust-germany.html?smtyp=cur&smid=tw-nytimes.

consent to B's terms is also undermined. Without voluntariness, this is "defective consent"[52] and cannot form the basis of meaningful "choice."

Finally, there are mounting qualitative challenges to the nature of "notice" itself in respect of digital technologies. Consumer-facing notices are difficult to read and understand from the perspective of legal rights and obligations, and increasingly unable to communicate the true implications of data collection or technology use. New and emerging technologies such as artificial intelligence, machine learning, and neural or deep neural networks feature opaque processes and lack explainability. In such cases, technologists themselves may be unable to explain how certain decisions are made or outputs are derived, let alone communicate these ideas to the general public. Where explainability impedes notice, consent sought on the basis of that notice is also undermined.[53]

3. Context collapse

The law is filled with ceremonial activities that have traditionally involved physical acts, such as placing one's hand on a Bible while taking an oath of office or affixing one's signature in ink to enter into a contract. We tend to scale the level of effort required by a ceremony to the gravity of the obligation undertaken or status conferred. For example, signing a marriage license requires the physical presence of the parties, at least two witnesses, and a state-sanctioned officiant, while executing corporate documents may require simple notarization, and accepting a delivery only a simple signature. The more cumbersome the ceremony, the more likely we are to perceive a decision as having serious consequences.[54] As one scholar puts it, "The heft of a document tends to correspond to the onerousness of the obligations agreed to by the consumer."[55]

The digital realm collapses all of our actions and behaviors into a series of one-dimensional clicks and scrolls. As a result, it can be difficult to assess the relative heft or gravity of a decision to interact or transact with a given service provider, share or consent to certain personal uses of data, or make any variety of other decisions. While legal ceremonies are meant to help us assess the heft of a decision, the ubiquity of "notice and choice" makes nearly all digital interactions feel the same. Just as digital activities are designed to remove as much friction as possible,[56] companies "intentionally minimize the disruptiveness of contract presentment in order to facilitate transactions and to create a smooth website experience for the consumer," thereby reducing the signaling effect of online contracts.[57]

4. The hidden dimension

Even if the legal and practical defects with the "notice and choice" paradigm were corrected, it would still fail to provide an effective foundation for Me2B Relationships based on an ethos of mutual respect. We have seen how a Me2B Relationship in the digital realm is rarely a two-sided, or 1:1 relationship. Rather, it is situated in the context of a complex web of relationships between individuals (Me-s), service providers (B-s), technical intermediaries (T-s), and a potentially infinite array of parasites (n-s).[58]

[52] *See* N. S. Kim, *Consentability*. Cambridge Univ. Press, 2019; (e-book), Kindle Edition.
[53] *See* Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, Harvard University Press (2018).
[54] For example, we typically cannot vote or get married online is because it is desirable to impose friction in these activities for reasons of public policy, economics, security, and integrity, among others.
[55] *See* Kim, Nancy S., *Situational Duress and the Aberrance of Electronic Contracts* (February 27, 2014), Chicago-Kent Law Review, Vol. 89, No. 1, p. 265 (2014), at 270.
[56] In fact, we aspire to seamless and frictionless digital interactions, such as contactless debit cards, one-click purchasing, and "passwordless" login.
[57] *See* Kim, Nancy S., *Situational Duress and the Aberrance of Electronic Contracts* (February 27, 2014), Chicago-Kent Law Review, Vol. 89, No. 1, p. 265 (2014), at 265.
[58] Occasionally, the technical intermediary is also the primary product or service provider or "B" resulting in a kind of "Me—T/B" relationship.

The "notice and choice" construct is based on an overly simplistic and acontextual view of relationships that fails to account for the complex and multidimensional nature of the modern digital sphere. By only capturing direct contractual relationships, such as Me2B Relationships, the "notice and choice" paradigm misses an entire dimension of the digital realm—the toxic, extractive practices of parasites and surveillance capitalists in the parallel dataverse. Any legal foundation or ceremony that ignores this context will always be deficient to protect and promote the rights and interests of individuals in Me2B Relationships.

III. REBUILDING RESPECTFUL RELATIONSHIPS

One reason that the "notice and choice" model persists despite the mounting evidence of its deficiencies[59] is the failure to put forward a workable alternative or to imagine an entirely new paradigm. This section seeks to provide an alternative path forward by attempting to map the expectations we have in the physical world onto the digital world through new legal foundations and innovative uses of technology to support respectful digital relationships.

A. REALIGNING EXPECTATIONS VS. REALITY

Any viable path forward must recalibrate our relationships and interactions in light of the increasingly complex and multidimensional nature of the digital ecosystem. While digital will always be different, requiring intermediaries who enable our primary relationships, the more we can realign our expectations in the physical world with our experiences in the digital realm, the closer we can get to establishing effective norms and rules for digital interactions. As a starting point, we can map our expectations in the physical realm to the digital realm, taking the analogy of a shopping mall.

1. The physical shopping mall

When we walk through a physical shopping mall, we inhabit a space that constitutes a series of overlapping relationships and legal statuses with respect to different parties, both known and unknown to us. We can window shop and weave in and out of individual shops at will, without signing any contracts or affirmatively accepting any terms. In fact, there are few legal ceremonies in a trip to the mall, apart from the occasional receipt that needs signing. That is not to say the mall is a lawless place.

The mall's entrances may display a host of written notices about a prohibition on smoking, penalties for unlawful trespassing, maximum occupancy limits, or the use of security or surveillance cameras, among other conditions of entry. By law, such notices must be clear and easily legible and they must be posted conspicuously, such as near the main entrance and exit or access doorways in a given room or space.[60] The terms of these notices are not negotiable and we are not asked to sign a consent form; we likely do not even know the identity of the property owner who is providing such notice. Rather, by entering the mall, we are presumed to understand and accept the conditions notified.

While inside the mall, we are generally anonymous apart from individuals personally known to us or while in shops or spaces we regularly visit; even then, we might be recognized but not identified by name or personal credentials. Typically, we can travel through the mall as one of many faces in the crowd, in a 1:N relationship to the mall and shop owners.[61] While we may be on notice of security staff or the use of surveillance cameras in

[59] *See* Susser, Daniel, "Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't." *Journal of Information Policy* 9 (2019): 37-62, available at www.jstor.org/stable/10.5325/jinfopoli.9.2019.0037.
[60] *See* International Building Codes 2018 https://codes.iccsafe.org/content/IBC2018/index.
[61] We would likely be surprised to learn of the generalized use of facial recognition technologies to identify specific individuals against a database. Sadly, this is changing as the commercial application of facial recognition technologies grows more prevalent.

the mall's common areas or individual shops, we still have a reasonable expectation of privacy in fitting rooms, restrooms, medical clinics or consultation rooms, and other areas.[62]

Finally, property owners have basic obligations to maintain the safety and security of their premises and are typically liable for any harm or injury suffered as a result of their negligence.[63] Individual store owners are typically responsible for keeping their premises clean and safe for customers, while mall owners are responsible for common areas like parking lots, walkways, elevators and escalators, and ensuring the safety of visitors in these areas. Moreover, shopping malls are quasi-public spaces where individuals retain certain fundamental rights.[64] Compare this to the experience of browsing the Web as it exists today.

2. The virtual shopping mall

Typically, we enter into the online or digital space through a browser such as Google Chrome or Apple's Safari. If we download a new browser, we may be asked to click a box to accept a license agreement, terms of service, and/or privacy policy. Where a browser is preinstalled or the default browser on a device, consent may be bundled into an operating system's blanket terms or license agreement.[65] Even if we are unaware of a browser's terms or privacy policy, its use is deemed to be implied "consent" or acceptance of them.

Once "online" via the browser, we can enter and exit various web properties such as individual websites and webpages owned and operated by different product and service providers. As in the physical realm, these property owners may stipulate conditions that apply to "being on their premises," i.e. using their website or app, via written notices. But unlike in the physical realm, the terms are presented as contracts. In fact, we are "practically unable to engage in any online activity without being forced to accept the terms of an electronic contract,"[66] notwithstanding their deficiencies.[67] This includes the digital equivalents of window shopping, weaving in and out of shops without making a purchase, and an array of other activities that do not require contracts in the physical world.

Where we expect to be an anonymous face in the crowd to a mall or shop owner, we are typically identified, known, and tracked by digital equivalents, including the browser and website operator, with no reasonable expectation of privacy, even when we are not "logged in." We are equally exposed whether in a perceived public forum like a social media newsfeed or a presumed private setting such as talking to a therapist through a mental health app.[68] Even when using Google's Chrome in Incognito mode, our activity may still be visible to third parties.[69] Our activity is tracked across sites and properties, and shared with or sold to an infinite number of other entities for their unlimited purposes.

Unlike in the physical realm where we have some legal precedent to protect our fundamental rights, the digital realm is largely devoid of such protections, at least in the U.S., where we lack a comprehensive federal privacy

[62] Because of this expectation and social norm, we would expect prominent signage where this is not the case, e.g. where cameras are in use in fitting rooms.
[63] *See* "Property Owners' Legal Duty to Prevent Injury," FindLaw (September 6, 2018), available at https://realestate.findlaw.com/owning-a-home/property-owners-legal-duty-to-prevent-injury.html.
[64] Although most shopping malls are privately owned and deemed to be private places from the perspective of property law, the public often perceives them as public spaces where certain rights are still guaranteed. This is at least partially true. For example, the Supreme Court has upheld individuals' right to the freedom of expression in a private shopping mall, concluding that such a constitutionally-protected right under California law did not constitute an unlawful taking or interference with the mall owner's private property rights, including the right to exclude people from the shopping mall. *See* Pruneyard Shopping Ctr. v. Robins, 447 U.S. 74 (1980).
[65] *See, e.g.,* Software License Use Agreement for Safari, Apple Inc., available at https://www.apple.com/legal/sla/docs/Safari10.
[66] *See* Kim at 276.
[67] *See* Section II.a. above.
[68] *See, e.g.,* Matthew Rozsa, "Therapy app Talkspace allegedly data-mined patients' private conversations with therapists," Salon (Aug. 10, 2020).
[69] *See* Aatif Sulleyman, *Incognito Mode Doesn't Protect Your Privacy and Can Let Your Boss See What You're Browsing,* The Independent (Nov. 20, 2017), https://www.independent.co.uk/life-style/gadgets-and-tech/news/incognito-mode-chrome-safari-firefox-meaning-privacy-nsfw-content-who-can-see-google-a8064876.html.

law or equivalent legal safeguards. Moreover, unlike physical property owners, app developers, website operators, and other digital service providers have virtually no obligations to undertake routine maintenance or to ensure minimum safety and security protections for their users as visitors or invitees on their properties. The deep divergence between our physical and digital realities is not a feature of technology but results from the economic logic of surveillance capitalism and defective legal foundations for the digital realm.

B. A NEW LEGAL FOUNDATION

In order to realign our norms and expectations in the physical and digital realms, we need better legal frameworks that move away from the hyper-individualistic or atomistic approach of "notice and choice." Each of the components listed below provides an alternative to notice and choice. Together, they could create a more robust foundation for protecting the rights and interests of individuals in the context of digital interactions, whether in a Me2B Relationship or not.

1. Prohibitions on processing

First, we must end digital exceptionalism, i.e. what is illegal offline should also be illegal online.[70] Just as there are capacity limitations, building and fire codes, and other restrictions imposed on physical property owners, digital services providers should be subject to specific prohibitions on certain data processing activities or uses of technology, particularly where an individual cannot opt out of a generalized practice. For example, a number of cities have recently banned the use of general facial recognition technologies to collect and process the biometrics of constituents.[71] Other proposals would impose bans or prohibitions on the use of personal data to discriminate in decisions related to housing, employment, credit, insurance, and public accommodations.[72] In such instances, individual preferences are overridden by a collective interest in prohibiting these activities.[73] Reestablishing meaningful Me2B Relationships in the face of pervasive surveillance capitalism may require similar prohibitions, such as outright bans on the business of data brokers, the commercial sale of personal data and behavioral insights, and cross-site tracking outside of a relationship.

2. Risk-based frameworks

Second, just as physical shop owners owe a duty of care and must undertake regular maintenance to promote the safety and security of their customers, digital product and service providers should owe a similar duty and be subject to risk-based measures to ensure the safety and security of their customers. At present, technical intermediaries, including browsers and apps, have virtually no legal obligation to protect the rights and interests of their users. As a result, they tend to privilege the commercial interests of customers, advertisers, and other parties, over those of individuals. In some cases, their competitive interests may result in better protections. For example, Apple undertakes a minimal vetting process, and mandates certain base level privacy and security requirements, before making an app available to consumers in its App Store. While this helps shift the burden of assessing risk away from the individual and onto the app provider, who is better positioned to assess it, corporate goodwill is not a sufficient basis for a new legal paradigm.

This burden-shifting must be mandated by law through the imposition of risk-based frameworks. Rather than outright prohibitions, this may entail prohibiting the use of a technology or data processing activity by an

[70] *See, e.g.,* The European Commission, *Shaping Europe's Digital* Future, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2020) 67 Final, 19 February 2020, available at https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf.
[71] *See, e.g.*, San Francisco Board of Supervisors Ordinance, File No. 190110 (May 6, 2019), https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A.
[72] *See*, e.g., Sherrod Brown, *Data Transparency and Accountability Act of 2020*, Discussion Draft, available at https://www.banking.senate.gov/imo/media/doc/Brown (hereinafter the "**DATA Act**"), at Sec. 103(b).
[73] Similarly, the DATA Act would ban the use of facial recognition technology as well as the processing of any personal data obtained from it. *Id*.

entity before it has undertaken a variety of ex-ante impact assessments. In addition to traditional privacy and data protection impact assessments, these may include social, ethical, economic, civil rights, and human rights-based impact assessments.[74] More radical proposals would require entities to demonstrate safety and efficacy, as well as freedom from bias, before going to market.[75] The aim of such proposals is to shift the burden of identifying, assessing, and mitigating risk away from individuals and onto the asymmetrically more powerful entities creating the risk, thereby reducing the cognitive load on individuals when deciding how to interact and transact digitally.

3. Contextual integrity

In addition to prohibitions and risk-based frameworks, it is critical to reestablish context in the digital realm. One method of doing so may be by adapting the theory of privacy as contextual integrity to digital life. Contextual integrity "ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it."[76] For example, a norm of appropriateness makes it acceptable for a doctor to inquire about a patient's weight, but unacceptable for an employer to do so. Similarly, a norm of distribution makes it appropriate for a doctor to share a patient's prescription with a pharmacist (under the condition it remains confidential), but inappropriate for the same doctor to share that information with the patient's employer (at least not without the patient's informed consent).

While we can easily identify context in the physical realm, we tend to treat the online or digital realm as a single monolithic context, tolerating behaviors and practices we would find objectionable offline. For example, we allow Google to read our email and Facebook to read our messages even though we would likely object to a neighbor reading our snail mail[77] or a spouse reading our texts.[78] Moreover, we use the same legal ceremonies and the same deficient "notice and choice" paradigm in wildly different contexts, whether a medical chat bot or Facebook's newsfeed. With the reduced signaling effect of legal ceremonies in the digital realm, context is ever harder to establish. In the face of this context collapse, establishing norms of appropriateness and distribution requires reestablishing context in digital interactions, including by determining relationship states relative to specific entities.[79]

4. "Necessity" and minimization

With contextual integrity restored in the digital realm, we could limit data collection and processing to what is necessary in a given context. Rather than requiring individuals to "consent" to each individual instance of data collection or use, limiting data collection and processing to what is necessary for a given transaction or interaction by default would help reduce cognitive strain and realign expectations with reality. It could also limit the distortions caused by an unbounded parallel dataverse and behavioral "surplus" that feeds parasitic actors in the surveillance capitalist paradigm. Much of this surplus results from the widespread reliance on "notice and choice" and consent-based frameworks that fail to account for data processing outside of primary commercial relationships.

---

[74] *See, e.g. id.*
[75] See, e.g., Roger McNamee, *Big Tech Needs to Be Regulated. Here Are 4 Ways to Curb Disinformation and Protect Our Privacy*, TIME (July 29, 2020), available at https://time.com/5872868/big-tech-regulated-here-is-4-ways/. The Alliance is also testing a rubric that would measure the ethical behavior of a technology product or service via a product certification scheme. *See* "Me2BA Testing Rubric - Working," Me2B Alliance (via Sharepoint).
[76] Helen Nissenbaum, *Privacy as Contextual Integrity*, WASH. L. REV., Vol. 79, No. 1, pp. 119-157 (2004).
[77] In fact, it would be an actual criminal offense.
[78] While the Alliance is helping develop some of the norms we need in the digital realm, the Me2B Relationship only captures expectations in respect of known or identified actors, neglecting parasitic activity in the parallel dataverse.
[79] In fact, the most frequently cited hurdle to applying a theory of contextual integrity to digital interactions is the lack of any norms at all in the digital realm. Even the Supreme Court has admitted that it could not discern societal expectations of privacy in text messages." *See, e.g.*, City of Ontario v. Quon, 130 S. Ct. 2619, 2625 (2010), at 2629.

Necessity is not new. European data protection law, which requires data minimization, allows for processing personal data[80] where necessary for the "performance of a contract" or prior to entering into a contract[81] and for "legitimate interests" pursued by a controller or third party.[82] In the U.S., the draft Data Accountability and Transparency Act of 2020 would go further to prohibit an entity from collecting, using, sharing, or otherwise processing any personal data unless it can demonstrate it is "strictly necessary to carry out a permissible purpose."[83] Permissible purposes include providing a good, service, or specific feature requested by an individual in an intentional interaction, and non-targeted advertising.[84] As with contextual integrity, limiting collection by default may require overhauling technical infrastructure and the difficult task of establishing norms about what is "permissible" or "necessary."[85]

5. Fiduciary duties

Finally, where it may be desirable to share personal data beyond what is strictly necessary for a given transaction or interaction, such as to save payment information or remember personal preferences, or for any other purposes that would serve the individual's interests while respecting her preferences, an obligation must attach to that sharing. The Alliance describes this principle as "no data about me without an obligation."[86] Such obligation may take the form of legally mandated fiduciary duties imposed on parties seeking to collect or use personal data. For example, a leading proposal would treat existing online providers as "information fiduciaries" legally bound by general fiduciary duties.[87]

The most common fiduciary obligation is the duty of care, often expressed in data security terms, requiring enterprises to take reasonable or prudent care in securing personal data and to avoid deliberately causing harm.[88] A higher duty of loyalty may require entities to avoid conflicting duties (the "thin" version)[89] or to act in an individual user's best interests (the "thick" version).[90] For example, the duty of loyalty may require preventing uses of data that would harm or offend a reasonable user.[91] Finally, a duty of confidentiality would require enterprises to bind data processors and sub-processors to the same duty of confidentiality as binds them in performing their obligations for that enterprise.[92]

---

[80] The Alliance contests the notion of "personal data" itself as problematic when everything is increasingly personal data over time.
[81] Art. (6)(1)(b), GDPR. "Necessary" need not be absolutely essential but must be more than just useful or desirable. *See* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis.
[82] Art. (6)(1)(f), GDPR. An entity may not rely on "legitimate interests" where such interests are "overridden by the interests or fundamental rights and freedoms of the data subject." *Id.* This balancing test can make it hard to apply "legitimate interests" in a blanket fashion at scale. For example, many entities in the adtech ecosystem have tried and failed to rely on "legitimate interests" only to revert back to consent. *See, e.g.*, *Adtech and the GDPR*, Taylor Wessing, available at https://globaldatahub.taylorwessing. As a result, many parties in the digital ecosystem rely on "consent" that is technically easier to obtain, even where it is unlikely to be meaningful. As noted above, while the GDPR is not a "notice and consent" law, it still features heavy reliance on consent as a lawful basis for processing personal data in the online or Web-based context. *See* Zanfir-Fortuna, *supra* note 31.
[83] *See* the DATA Act, *supra* note 72.
[84] Advertising "based on the use of any personal data collected or stored from previous interactions with the individual" is not a permissible purpose. *See id.*
[85] Notes from Lisa LeVasseur.
[86] *See* conversations with the Me2B Alliance, the PaLs Working Group, and Lisa LeVasseur.
[87] *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183 (Apr. 2016).
[88] *See, e.g.,* the DATA Act, *supra* note 72, at Sec. 207 (entities must "implement and maintain reasonable security procedures and practices" appropriate to the nature of an activity).
[89] Indeed, there are solid arguments that attempting to legally impose a duty of loyalty on U.S. corporations would run afoul of fiduciary-style duties owed to customers, shareholders, and other stakeholders. *See* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 Harv. L. Rev. (2019). Some proposals, such as GLIAnet's "digital trustmediary" model seek to overcome these challenges by creating a new opt-in class of digital fiduciaries, voluntarily providing digital services to their clients under heightened duties of loyalty. *See* Whitt, *Old School Goes Online*, Santa Clara High Tech Law Journal (February 2020), available at https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1648&context=chtlj.
[90] *See id*.
[91] *See, e.g.*, Data Care Act of 2018, S. 3744, 115th Cong. (2018) at Sec. 3 (fiduciaries may not use personal data "in any way that will benefit the online service provider to the detriment of the end user, [result] in reasonably foreseeable and material physical or financial harm . . . or would be unexpected and highly offensive to a reasonable user").
[92] *See id.* at Sec. 3.b.3.C (enterprises must take reasonable steps to ensure they fulfil the duties of care, loyalty and confidentiality, "including by auditing [their] data security and data information practices"). This is not unlike the requirement that data controllers must impose certain data security and other obligations on processors acting on their behalf per the GDPR.

Fiduciary-style obligations and duties are typically grounded in asymmetrical personal relationships such as between doctors and patients or attorneys and clients. Applying them to the digital realm requires identifying appropriate relationships to which they might attach. Moreover, as such obligations only make sense in the context of primary relationships, they could not, standing alone, provide a sufficient legal foundation to remedy the nefarious effects of the parallel dataverse and logic of surveillance capitalism on Me2B Relationships. Rather, they must be layered on top of these other foundational building blocks as laid out above.

C. TECHNICAL SCAFFOLDING

Without a new legal paradigm, technology can do little to restore respectful digital relationships in the face of powerful commercial incentives.[93] Even with such a foundation in place, there will still be too many interactions and touchpoints to effectively scale our cognitive capacity and human agency in the digital realm. Without scaling, we cannot address the steep power asymmetries at play as between individuals and entities in the digital sphere. By helping scale the individual's ability to express and promote her interests and preferences in the digital realm, technology can act as a kind of scaffolding to support and uphold the new rules in practice, thereby restoring mutuality to Me2B Relationships.

1. The browser as "digital proxy"

Until we can physically inhabit a digital space, we will require some kind of technical infrastructure to act as our "digital proxy." Right now, we show up through a combination of technical intermediaries who have competing interests, none of which uniquely represents our own. In other words, we lack an effective digital proxy. As such, many proposals for fixing the Web call for new intermediaries, such as digital avatars, personal artificial intelligence, and virtual assistants.[94] The idea is that these tools could help individuals scale their knowledge, capacity, and resources to lessen the asymmetrical power dynamics that exist in the digital realm and approximate the dynamics of offline, in-person interactions. But why not begin by leveraging existing intermediaries in service of the new paradigm?

The browser is in a unique position to support this paradigm by helping to realign our experiences in the digital realm with our expectations in the physical one. In order to act as our digital proxy, we must be known to the browser by establishing credentials and setting out our preferences. This means, we must enter into a genuine Me2B Relationship with the browser by executing a valid legal contract and providing meaningful, informed consent to its terms of service and privacy policies. Under this validly formed contract, the browser could not make any material changes to the contract unilaterally and any violations would be enforceable at law, unlike under the current paradigm.

To act as our digital proxy, the browser must be bound by a thick duty of loyalty mandated by law, not commercial preference. This duty would require it to promote and privilege our individual interests above the interests of all other parties or stakeholders in a given interaction or transaction. The browser would also have heightened obligations to store, communicate, and manage our individual preferences vis-à-vis other web properties, including preferences such as "do-not-track" or "do-not-sell-my-data" requests under laws like

[93] One proposed technical means of buttressing and enhancing this loyalty-based governance model is to provide clients with advanced technological tools, such as personal AIs, localized data pods, identity layers, and symmetrical interfaces, to instantiate strong fiduciary duties to individuals. For example, the tiered GLIAnet proposal constitutes three interrelated elements: (1) duties of care mandated for entities accessing or using personal data (via legal instruments such as binding laws and regulations), (2) duties of loyalty volunteered by entities willing to serve clients/patrons under such obligations (achieved via legal instruments such as self-certification regimes, and/or enforceable codes of practice and conduct), and (3) edge-based technology overlays, such as Personal AIs, to provide agential support. *See* Whitt, *supra* note 88.

[94] The Alliance refers to these as "Me2B Relationship Managers."

the California Consumer Privacy Act (CCPA).[95] Finally, the browser must be held to a duty of confidentiality with respect to our browsing activity and search history.

The browser could also help streamline legal ceremonies in the digital realm. Acting as our digital proxy to enforce our preferences, the browser could scan and read the many property-style notices we encounter.[96] Rather than forcing us into defective contracts with each product or service or digital property we explore, it could undertake an initial screening process to eliminate any providers whose terms do not align with our values or meet our preferences. After this initial gating, we could decide whether to enter into a Me2B Relationship with a relevant service provider for purposes of completing a transaction or interaction through a validly formed contract. Reducing the number of contracts should also reduce the cognitive strain and help restore the signaling effect of digital legal ceremonies.

Going back to the shopping mall analogy, the browser would enter digital space as we would physical space, carrying our own preferences and inclinations forward into the digital realm. Through the browser as our digital proxy, we could visit websites, webpages, and other digital properties anonymously. This would require a technical means by which to obscure our identity vis-à-vis our digital proxy. We could then explore or weave in and out of these properties, as we can in the physical world, without establishing a commercial relationship or entering into a defective contract. Finally, the browser could help further reestablish context by locating us in digital time and in space, to give us a fuller picture of the various stakeholders involved in a given interaction or transaction as well as its potential data footprint.

IV. ME2B RELATIONSHIPS IN THE NEW PARADIGM

Having outlined a vision for a new legal foundation, supplemented by new applications of technology, this section examines what digital interactions might look like in this new paradigm, according to relationship state.

A. RESPECTFUL DEFAULTS

With general prohibitions in place to outlaw toxic and pernicious behaviors that are impossible to opt out of at an individual level and the imposition of mandatory risk-based frameworks to assess the safety and security of digital products and services before they hit the market, our digital interactions would be inherently more protective of our interests. As a matter of principle, ending digital exceptionalism by prohibiting online what is illegal offline offers a good starting point. Working to articulate the acceptable bounds of our digital interactions, achieving consensus on specific behaviors and practices that should be outlawed, and determining the necessary risk-based assessments that must be undertaken by a product or service provider, are also key steps. Once in place, all digital interactions would benefit from more respectful defaults and baseline protections, whether in the context of a Me2B Relationship or not.

B. RELATIONSHIP STATES

1. The No Me2B Relationship State

The "No Me2B Relationship State" can exist: (1) before an individual has entered into a Me2B Relationship and established unique credentials with a given product or service provider; (2) after the individual's credentials have been destroyed upon termination of a Me2B Relationship with a given product or service provider; or (3) when an individual has an existing Me2B Relationship and unique credentials with a given product or service provider but chooses to participate in a specific transaction or interaction anonymously without presenting those credentials, rather than through the relationship. For example, a retail customer of Target.com who has

[95] California Consumer Privacy Act (Cal. Civ. Code § 1798.100, et seq.) (hereinafter the "CCPA"). The CCPA requires companies to honor "do-not-sell-my-data" requests automatically submitted by an individual's browser. *Id.*
[96] *See, e.g.,* Machine Readable Privacy Terms Working Group, IEEE P7012 Working Group, https://sagroups.ieee.org/7012/.

a customer account with Target may nevertheless decide to checkout in "guest mode." In the new paradigm, the browser acting as our digital proxy could "know" our relationship state in relation to each digital product or service provider we encounter online.

In the No Me2B Relationship State, having no unique business relationship with an entity,[97] an individual has no need to establish unique credentials with it. Rather, the individual will be able to interact with that entity's digital properties as an anonymous face in the crowd, in a 1:N property-based relationship, just as she would in relation to shops in a physical mall. The browser would provide a technical means by which to obscure our identity vis-à-vis the service provider. Unlike in the current "notice and choice" paradigm, defective contractual instruments in the form of terms and conditions or terms of service would be unnecessary in the No Me2B Relationship State under the new paradigm. Instead, the default legal ceremony would be a property-style notice not requiring any affirmative act from the individual. In the new paradigm, contracts become the exception rather than the norm, helping restore their signaling effect.

Before entering into the Me2B Relationship State with a given entity, the browser as our digital proxy would have scanned and pre-screened that entity's terms and conditions, privacy policies, and any other relevant notices for compliance with our indicated values, preferences, and requirements. We could then enter the service provider's digital space with awareness and acceptance of these conditions. Should the browser detect any unreasonable notices that violate our values or preferences, it could provide a notification or alert recommending "exit" or "caution." Even while in a digital space in a No Me2B Relationship State, the service provider would still owe us a duty of care, having to take reasonable or prudent steps to secure any data or insights gleaned, ensure minimum safety standards, and avoid deliberately causing us harm.

2. The Me2B Relationship State

Should we want to establish a business relationship with an entity to be "recognized, remembered, and responded to," we would enter into a Me2B Relationship by creating an account, signing up for a membership or loyalty scheme, or by otherwise establishing unique credentials with the entity, with the help of the browser as our digital proxy. This would be achieved through a validly formed electronic contract requiring an affirmative act on our part, and may also be supplemented by means of "whitelisting" or other technical mechanisms implemented by the browser.[98] Once in this Me2B Relationship, the service provider could not unilaterally change the terms of such contract without jeopardizing the relationship or risking legal liability. We could now participate in specific transactions or interactions in a "Me2B Relationship State."

While in a Me2B Relationship State, we would remain identified, share personal information, and participate in exchanges of mutually agreed upon value through our browser as our digital proxy. The website owner or operator would owe us more than a mere duty of care as in the No Me2B Relationship State. Rather, when transacting or interacting with an entity in this Me2B Relationship State, the entity would also be legally bound by duties of loyalty and confidentiality. Even with these heightened duties owed, the browser could help provide additional context for specific interactions or transactions by giving us a fuller picture of the various stakeholders involved and even its potential footprint in the parallel dataverse. We could then elect to participate in either relationship state.

The browser could provide this ability to transition between relationship states, affording us the same agency in digital spaces as we have in physical ones, carrying our own preferences and inclinations forward into the

[97] Apart from generally being an undifferentiated prospective customer, such as a window shopper.

[98] For example, the draft ePrivacy Regulation in Europe would implement a similar framework in respect of terminal equipment. *See* Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Council of the European Union (Feb. 21, 2020) ("Providers of software are encouraged to include settings in their software which allows end-users, in a user friendly and transparent manner, to manage consent to the storage and access to stored data in their terminal equipment by easily setting up and amending whitelists and withdrawing consent at any moment.")

digital realm. In this way, the browser would no longer be a mere technical intermediary or T. Rather, it would be transformed into an approximation of the "Me" in a Me2B Relationship. With the browser acting as "Me's" genuine digital proxy and obligated to promote Me's interests in all digital interactions, what were previously Me—T—B style relationships become much more like direct Me2B Relationships again. In this way, the new paradigm helps to restore the mutuality of Me2B Relationships to approximate relationships in the physical realm.

CONCLUSIONS AND RECOMMENDED NEXT STEPS

A. CONCLUSIONS

Based on the above analysis, we can draw a number of preliminary conclusions. First, Me2B Relationships in the digital realm are multidimensional relationships with commercial, legal, and technical dimensions. Through this technical dimension, data generated in the ordinary course of our Me2B Relationships creates a fourth hidden dimension—a kind of "parallel dataverse" that is largely invisible to us as individuals. This hidden dimension has significant consequences for Me2B Relationships despite exceeding our cognitive capacity to appreciate them.

Second, as a result of surveillance capitalism, myriad parasitic entities feed off of this parallel dataverse in ways that exploit and undermine our primary Me2B Relationships. Thus, a given Me2B Relationship cannot be assessed in isolation from the complex and overlapping relationships between various parties directly and indirectly involved in a given digital interaction or transaction, including individuals (Me-s), product and service providers (B-s), technical intermediaries (T-s), and parasites (n-s).

Third, our prevailing legal paradigm for digital interactions, in the form of "notice and choice," stems from an overly simplistic and antiquated view of the digital universe formed in the 1970s. It is comprised of defective legal ceremonies and also suffers from a growing number of practical defects. Moreover, it only accounts for primary relationships, failing to consider the impact of an increasingly complex digital realm running on the logic of surveillance capitalism. By only accounting for one dimension of our digital lives, this legal paradigm and its associated legal ceremonies leaves us exposed and vulnerable with insufficient safeguards and protections.

Fourth, any viable path forward must acknowledge this complexity and provide a strong underlying foundational framework to situate Me2B Relationships in this broader context and help realign our expectations in the digital world with our experiences in the physical realm. This realignment can help guide the development of effective norms and rules for our digital interactions regardless of relationship state.

Fifth, a robust new legal foundation must prohibit certain activities and practices, mandate a risk-based approach to commercializing digital products and services, reestablish context for digital interactions, limit default data collection and processing to what is necessary for primary business purposes, and impose higher standards and obligations on parties who seek to go beyond what is necessary in the context of a bonafide commercial relationship.

Finally, existing and emerging technologies could help play an important role to support and help enforce this new legal paradigm in practice, starting with the browser as our "digital proxy." Through legal mandates requiring technological tools like the browser to act in service of, rather than for purposes of extracting value from, our Me2B Relationships, we can help rebuild respectful relationships in the digital realm based on an ethos of mutual respect.

B. RECOMMENDED NEXT STEPS

While beyond the scope of this paper, the Alliance may consider researching the following questions as next steps:

- What rights are necessary to protect the individual end user in digital interactions and transactions, regardless of relationship state? For example, what are the individual's digital rights in respect of privacy, freedom of thought, network interoperability, data portability, explainability, and third-party rights delegation, among others? How might these rights translate into necessary prohibitions on certain activities or form part of the necessary ex ante risk assessments required before digital products and services go to market?

- How can existing technical intermediaries and emerging technological tools help to reestablish context in the digital realm so as to allow the application of a contextual integrity framework or norm-based approach to digital transactions and interactions? How might the Alliance help to develop and articulate the norms that would apply in different contexts?

- What fiduciary duties or obligations could and should attach to various stakeholders in the digital ecosystem, to which ones, and under what circumstances? Which should be mandated by law versus encouraged by commercial standards or self-regulatory codes? How might a tiered legal and technological trust model help to enforce fiduciary duties, including a duty of care, duty of loyalty, and a duty of confidentiality, among others?

- What is the role of "identity" in establishing relationship states? How should we configure our identity in relation to the browser itself when it is acting as our digital proxy? How can we configure the identity of the browser vis-à-vis digital product and service providers to indicate different relationship states, including the No Me2B Relationship State and the Me2B Relationship State?

APPENDIX A - ME2B MATERIALS

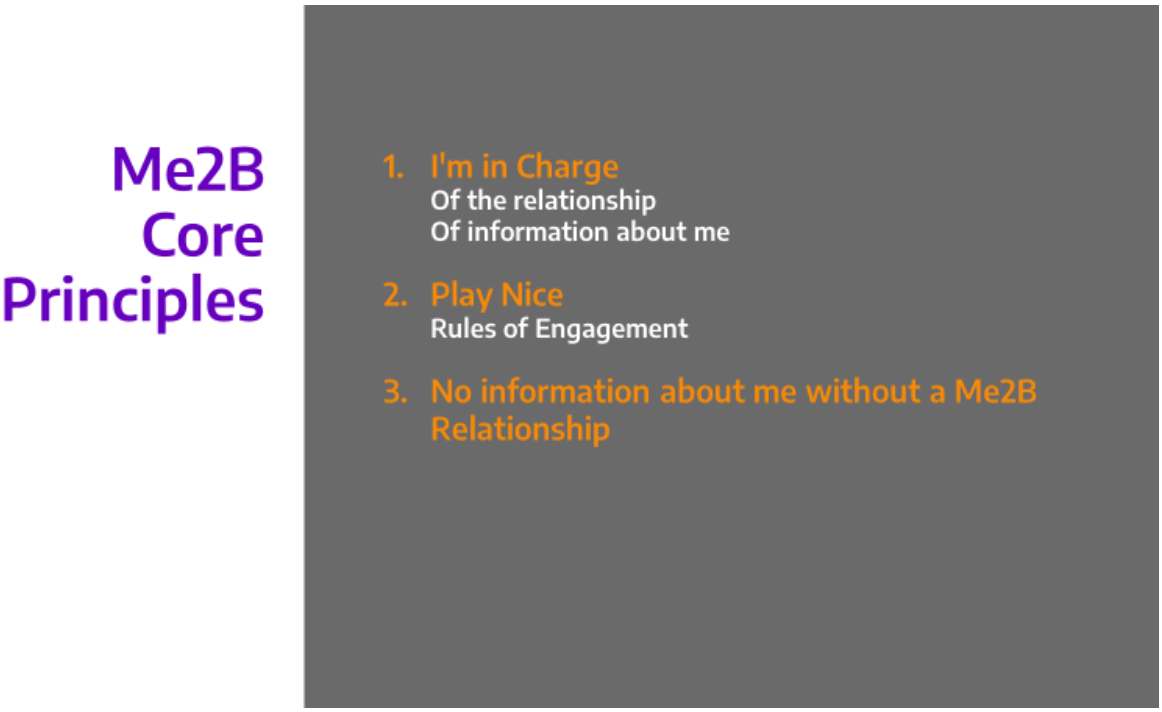

Figure 1 - Me2B Core Principles via Me2B Alliance

Figure 2 - Me2B Rules of Engagement via Me2B Alliance

APPENDIX B - ME2B RELATIONSHIP MODEL

		Acquaintance	Buildup	Continuation	Deterioration	Termination
Physical World		• I am window shopping outside • I am browsing inside of a store	• I buy something • I sign up for a newsletter • I open an account • I join a loyalty program	• I am a regular customer • I have a subscription • I have a membership	• I visit less frequently • I make fewer purchases • I cancel my subscription	• I no longer visit that shop • I have closed my account • I have cancelled my subscription • I have terminated my membership
Body of law		PROPERTY	CONTRACT	CONTRACT	CONTRACT	PROPERTY
Digital World	I want to do X	• I browse a website (but have not logged into anything) • I check out an app in the app store • I download an app but do not create an account/use it in "guest" mode	• I log into a website • I buy something from a website in "guest" mode or logged in • I create an account • I download an app and create an account	• I am a regular customer • I regularly use the service/app • I have a subscription • I have a membership	• I visit the website less often • I make fewer purchases • I open the app less often • I spend less time in the app when I do open it	• I no longer use or even open the website/app • I delete my account
Me2B Expectations		• I'm anonymous until I say otherwise • I am 1:N	• I can transact without being forced into a Me2B Relationship.	• I decide to start a Me2B Relationship • I can BYOID and privacy terms & permissions.	• I can report problems with impunity; problems are readily resolved.	• The Me2B Relationship is over. • I'm in charge.
Reality Today		• You are not anonymous; between pseudonymous and identified. • Data collected includes device IDs, ad IDs like IDFAs, GPS location data/IP address, etc. ("acquaintance data") • You are forced into defective contracts.	• You are not anonymous; between pseudonymous and identified. • Data collected includes acquaintance data + cookies and other trackers, analytics, personal data, etc. • You are forced into defective contracts.	• You are identified. • Data collected includes acquaintance data + cookies and other trackers, analytics, payment info, personal data, etc. • You are forced into defective contracts.	• You are identified. • Data collected includes acquaintance data + cookies and other trackers, analytics, payment info, personal data, etc. • You are forced into defective contracts.	• You remain identified. • Your data is retained.