Beyond Consent: A Right-to-Use License for Mutual Agency

Lisa LeVasseur[1]
Eve Maler

Abstract: Digital apps and services handle consent and other types of permissions in structurally and practically flawed ways. Consent as conceived of in data protection regulation cannot express all of the dimensions of Internet-enabled relationships. Moreover, "consent" is a poor descriptor for the type of relationship trust assessment people perform in these circumstances. What's needed is a method to enable true mutual agency between any two parties in an Internet-enabled relationship. We propose a right-to-use license for access permissions as a practical alternative to consent and contract as used today, and a taxonomy that classifies important types of permissions. We also examine new data sharing scenarios, including decentralized identity, that may support their use.

[1] Lisa LeVasseur is with Wrethinking the Foundation, IEEE P7012, and the Me2B Alliance. Eve Maler is with ForgeRock and the Kantara Initiative's User-Managed Access (UMA) Work Group. The authors gratefully acknowledge Timothy S. Reiniger, Esq. for his review of the manuscript.

Introduction

Digital consent and other permission constructs as defined, practiced, and regulated today increase the power asymmetry in digital relationships between users and service providers. To build ecosystems that support *mutual agency* between individuals and organizations, users of services and applications need to be able to express their wishes to service providers in a way that is more respected and adhered to.

In this article, we analyze and compare the legal foundations of different types of permission currently used for digital data sharing. We then examine how these types of permission are applied today to common data sharing scenarios. With this background, we analyze ways in which the permissions are functioning poorly and use a human-centered perspective to derive criteria for an improved permission model. Finally, we propose right-to-use licenses as a more satisfactory model, along with a templated approach for its use, and analyze additional scenarios, including decentralized identity, to see if their characteristics are friendly to implementing this model.

Legal Foundations of Permission

This section offers a high-level description of the most common permission conveyance instruments: consent and contract. They persist in nearly every jurisdiction and every culture. We encounter them on a near-daily basis in digital contexts.

Requirements for Legally Binding Consent

Consent is designed to let one party traverse the ethical and/or legal boundaries of another party with the latter's permission; it literally turns the impermissible into the permissible. Legal scholar Nancy S. Kim states its capability as follows: "Consent permits private ordering, which in turn allows individuals to allocate their rights in a way that suits them." [1, p.7] Three conditions must be satisfied for consent to be legally binding [1]:

1. **Act or manifestation of consent:** The individual takes some action, for instance, clicking on an "Accept" button when asked to allow cookie storage.
2. **Knowledge:** The individual clearly and fully understands what they are being asked to allow.
3. **Voluntariness:** The individual is freely granting permission.

If there is no act or manifestation of consent in a consent-seeking scenario, there is no consent. If there is an act or manifestation without the condition of knowledge or voluntariness, it is a case of *defective consent* [1].

The form of all three conditions varies depending on the context of the consent request, and, in particular, the potential risk to the individual's physical and mental autonomy. For example, consent for a surgical procedure entails substantial doctor/patient interaction and reading and signing several physical pieces of paper. Given the risk to the individual's physical autonomy and security, the standard for consent is higher than that of consenting to share personally identifiable information with, say, an online service provider [1].

Where it is meaningful to do so, the consenter may unilaterally revoke their consent.

Requirements for Legally Binding Contract

A contract involves agreement to perform future acts by the parties. There are five generally agreed-upon requirements for a contract to be regarded as legally binding, and they bear similarities to the three conditions for consent. They are:

- Consideration: What is being given by each party in the agreement?
- Voluntary Acceptance: Is there a clear offer and autonomous response?
- Legal Purpose: Is the proposed purpose of the agreement legal?
- Competent Parties: Are both parties capable of making a contract?
- Mutual Acceptance: Do both parties commit to being bound by the contract?

Since contract acceptance (“consent to the contract”) must be mutual, it is not generally possible to withdraw or revoke acceptance unilaterally.

Terms of Service Contracts and Privacy Policies

Terms of Service (TOS, sometimes called Terms of Use) agreements are regarded as legally binding contracts in the eyes of the service provider, and superficially appear to satisfy the criteria for legally binding contracts.

Privacy Policies (PP), the published privacy notices that service providers typically pair with TOS, are sometimes considered contracts. If the individual is prompted to agree to PP as a condition for (say) creating an account, then it is part of the contract. If the user never affirmatively agrees to the PP, it is not a contract. It is, however, a legally binding commitment by the service provider that can be monitored and policed by government oversight entities, such as the FTC in the US.

Licenses

A license is a specific kind of contract that grants well-scoped rights, such as to use property, from one party to another. Licenses typically include the following components:

- Definition of property/scope of grant
- Definition of the parties involved
- Term, termination, renewal
- Territory
- Terms of agreement, including conditions
- Payments to licensor
- Reports and auditing requirements

Unlike contracts more broadly, a license can be issued unilaterally by a granter to a grantee and – depending on the details of its components – revoked unilaterally as well.

Comparing Legal Mechanisms for Digital Permissions

Though consent, contract, and license are similar mechanisms, they do not behave identically.

A distinction between consent and the two forms of contract is that consent can be requested and supplied at the time of the need, whereas contracts and licenses are typically established ahead of the time of need (potentially just ahead). Because people can later change their mind or underestimate what their future self would agree to, some experts contend that consent is therefore more apt in the context of digital permissions.[1]

As noted earlier, consent and licenses may be revoked at any time, whereas this may not be the case with a contract. This is a claimed advantage of consent in digital contexts. In practice, however, revoking consent may not be easy and sometimes not possible at all.

Consent is by its nature asymmetrical in that it tends to favor the consent-seeker. The consenter can affirm or deny only the options presented to them by the consent-seeker. This is perhaps the biggest challenge with consent in digital contexts because the consent-seeker is always the service provider.

Contracts explicitly lay out the *quid pro quo*, that is, the consideration, which is notably absent from the consent mechanism. The components of a contract as outlined above engender greater symmetry between parties, ideally defining an attractive offer.

Figure 1 compares the three mechanisms.

	CONSENT	CONTRACT	LICENSE
MEETING OF MINDS	Not required	Required	Not required
TIMING	Just in time	Beforehand	Beforehand or Just in time
REVOCABILITY	Unilateral (by Consenter)	Bilateral	Unilateral (by Issuer)
RECORDING OF TERMS	None	Included in Contract text	Included in License text

Figure 1. Comparison of Legal Mechanisms for Digital Permissions

Common Digital Information Sharing Scenarios

The majority of permission scenarios encountered by people today for digital data sharing are consent-based. The four most typical are as follows:

- **Cookie consent:** Most commonly experienced, with several patterns ranging from displaying only a “No Option” browse-wrap notice (possibly with a “Close” or “Dismiss” button) to a menu for selecting precise cookie options to an opt-out (pre-checked “Accept” button). Figure 2 illustrates offering a notice with a single option, “Accept”. Most patterns likely do not comply with European privacy law.[3]
- **Application permissions:** An app typically notifies the user about its need to access local resources, such as photos, and requests consent to access them. The individual is presented with specific disallow/allow options for each type of resource.
- **Marketing and communication preferences:** An app seeks to collect personal information such as an email address or mobile number to support one of a variety of service delivery and marketing activities, such as texting about flight delays or emailing about discount offers. Collecting and using the personal information for communications generally requires consent.
- **Third-party permissions:** An app may communicate with third-party service providers in a user-mediated way for a number of different purposes. This can enable features such as “social sign-in” or the addition of games and quizzes to a social networking platform (after the fashion of Facebook/Cambridge Analytica). The user mediation begins with consent.

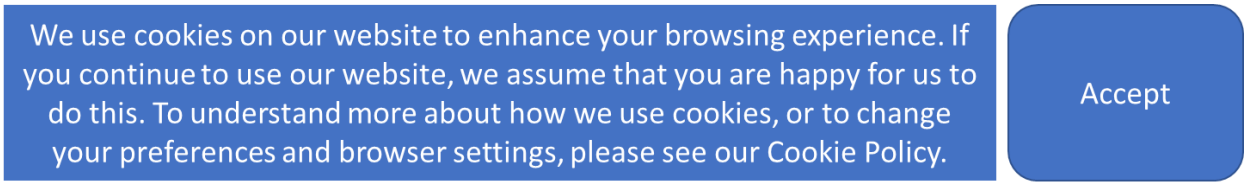

Figure 2. “One Option” Cookie Consent Management Example

In addition to these consent-based scenarios, there is one commonly encountered contract-based permission scenario:

- **TOS and PP:** The individual is prompted to accept TOS and sometimes PP, typically during login account creation. TOS contracts are commonly regarded as contracts of adhesion. People often encounter them as click-wrap by having to click a simple “Accept” button to gain access to the service, much like with cookie consent. In practice, the user experience fails to adequately deliver proper mutual acceptance.

The last common permission scenario is akin to a right-to-use license between people:

- **Peer to peer sharing:** Encountered in sharing services such as Google Docs, Dropbox, and TripIt, peer to peer sharing is the ability for an individual to share specific files or items directly with another individual, granting constrained access capabilities such as read, write, or comment-only.

Digital Permission Experiences Are Broken

Given the challenges with data sharing permission realities, what can we observe?

Digital Consent Is Inappropriate to the Task

Digital consent experiences frequently exhibit deficiencies when it comes to all three legally binding consent conditions outlined above: an act or manifestation of consent, knowledge, and voluntariness.

The often-used cookie consent “No Option” pattern discussed above suffers from a lack of manifestation of consent, and thus has no consent at all.

In many of the other cookie consent patterns, such as the “One Option” example in Figure 2, it’s unlikely the user fully understands the conditions for consent. This means the pattern would not meet the knowledge standard, and thus the consent is defective [1]. (It is a concern that cookie consent is a source of so many problems because it represents the first time an individual “meets” many service providers.) The Cambridge Analytica third-party permission issue was also in large part about lack of knowledge. Confusion about consent in digital user experiences abounds.

An Internet-connected hardware device, such as a set of speakers, that requires a user to consent to information tracking and sharing in order to receive a software upgrade, may put voluntariness of consent at risk depending on the timing and nature of the upgrade.

Such challenges remain even in the face of regulations such as GDPR, which requires consent to be freely given, specific, informed, and unambiguous, and has been enforced since May 2018. GDPR represents an attempt to put data subjects in greater control of their personal information. However, as noted, the nature of consent is to be asymmetrical. The consent-seeker pursues a private ordering of rights that the

consenter would not otherwise have considered [1]. To imagine the roles reversed in order to give the individual greater power is nonsensical.

Another structural challenge in the case of cookie consent is that it only gathers consent from a presumed individual using a particular browser, rather than an identified individual. Legal consent requires a relationship between properly identified parties. It's possible for the individual to claim that "someone else was using my device."

Digital Contract is Not Working Either

The composition of contract aligns better with the spirit of informed, explicit consent. However, digital contracts are not working; the length and complexity of TOS and PP defeat even those who attempt to understand them. Moreover, contracts are frequently presented as up-or-down "click-wrap", and therefore suffer many of the same flaws as digital consent.

A study that presented people with a chance to join the fictitious social network NameDrop illustrated this in dramatic fashion. [2] It offered either a "quick join" click-wrap option or a PP that should take 29-32 minutes to read, plus a TOS that should take 15-17 minutes to read. Only 26% chose to read the PP, spending an average of 73 seconds. The average time spent reading the TOS was 51 seconds. Almost all agreed to both contracts, with decliners spending only 30 seconds longer on the TOS and 90 seconds longer on the PP. This is despite the fact that the TOS contained "gotcha" clauses that bound individuals to share data with the NSA and to provide their first-born children as payment.

Additionally, because TOS – and, often, PP – are meant to be true contracts, they are not unilaterally revocable by the individual when something has changed in the relationship between them and the service provider. Although the provider is free to update a TOS version and require the user to agree to the contract all over again to continue service, the courtesy of canceling the contract is not extended to the user.

Centering on the Human Perspective to Find an Improved Model

For all of these reasons, we explore a third option, licenses – specifically licenses that may be offered by the individual to the service provider. We begin by centering on the human perspective, as in the practice of human-centered design, and asking what it is the individual seeks out of human-service provider relationships.

Introducing a “Me2B Relationship” Perspective

We propose using a “Me2B” perspective to find a more successful model that improves on today’s consent and permission model. A *Me2B relationship* is a relationship that an individual has or seeks to form with a business or other institution.

Relationships of any kind are characterized by the simple act of sharing between two parties. In the case of a Me2B relationship, sharing takes the form of mutually agreed-upon value exchange – a *Me2B deal.* This is a *quid pro quo* agreement that defines the scope of sharing.

In the past, sharing in such relationships was relatively static and interaction was not as pervasively tracked and remembered by the serving institution. Today, it’s the norm for connected products and services to observe, remember, and utilize every human interaction in an ongoing fashion.

A digital Me2B relationship has a lifecycle as follows, adapted from psychologist George Levinger’s five stages of interpersonal relationships [4]:

1. **Acquaintance** (discover and window shop): I want to do X online.
2. **Build Up** (try): I explore Website or download App and play with it. I like it, so I create a Me2B Relationship by allowing myself to be remembered by the service provider.
3. **Continuation** (habit): I regularly use the service.
4. **Deterioration** (problems): I’m using the service less.
5. **Ending** (end use): I no longer use or even open Website or App.

Digital Me2B relationships are established at the point where the individual is remembered, which is currently dictated by the service provider, and happens in multiple ways.

Enabling individuals to have agency throughout the relationship lifecycle will require new thinking and technologies acting on behalf of the individual, the most important being a Me2B *relationship manager.*

Privacy frameworks and regulations typically discuss relationships among the *data subject*, *data controllers*, and *data processors*. The Me2B perspective starts with the individual and works outward. Figure 3 illustrates how these parties can map to each other in the different perspectives. A Me2B relationship manager is shown where it might appear in future.

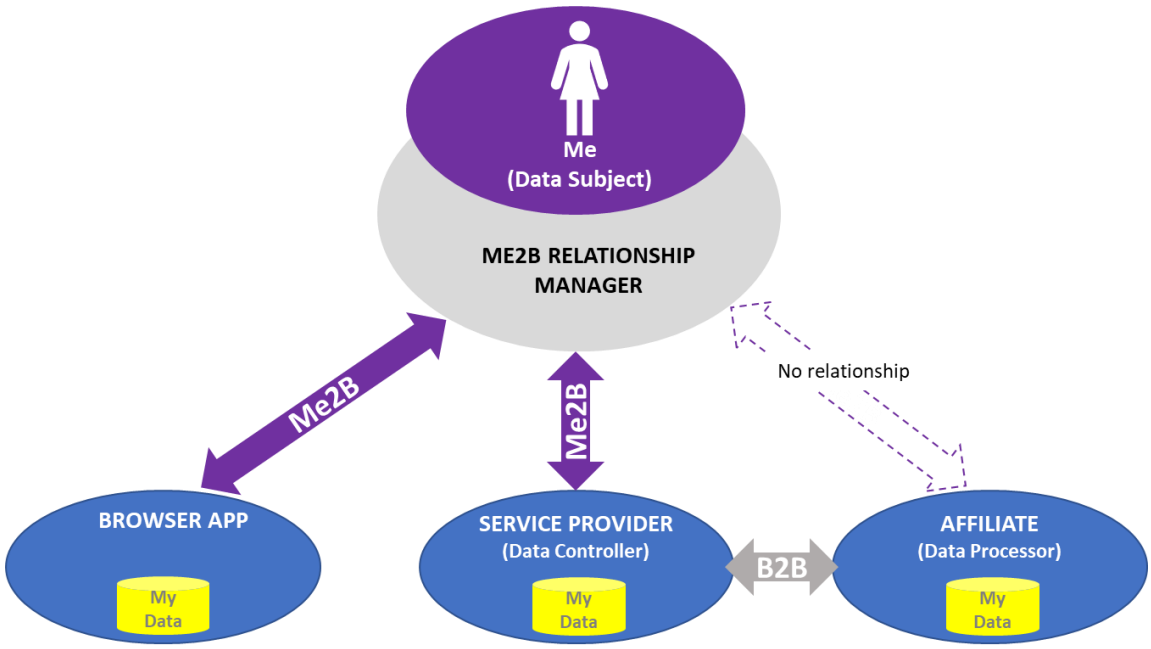

Figure 3. Relationships and Mappings Among Me2B, Privacy, and Service Provider Concepts

Criteria for a Human-Centered Permission Model

From a human-centered perspective, a robust permission model for data sharing must align more closely with real-world Me2B transactions. This includes the following capabilities:

1. **Individual Asserts Terms:** The individual can assert their own data sharing terms to the service provider. They can also modify and revoke their terms.
2. **Proactive Terms Specification:** The individual can specify data sharing terms *before* supplying any data (for example, authentication data used for the purpose of setting up an account).
3. **Choice About Being Remembered:** The individual can navigate to and begin to use a website without having to be known or tracked at all, until they're ready to be remembered (for example, no cookie browse-wrap).
4. **Terms Usability:** The data sharing terms are highly usable in both a legal and a technical sense – easy for the individual to choose and understand and for the service provider to adopt.

Proposal: Right-to-Use Licenses

Given that consent as practiced and contracts of adhesion fail to work properly in a digital context and frequently fail to meet a legal definition for consent, we propose instead for users to assert right-to-use licenses.

Motivations for Licenses

Right-to-use licenses best meet the criteria for digital Me2B relationships (assuming appropriate implementation).

A right-to-use license functions as a reverse EULA, a “vendor license” whereby the user licenses personal data collection, use, disclosure, and so on to a service provider. A license also enables frequency of change and revocation by the individual, and greater volition than the alternatives we have analyzed. These properties allow it to meet the Individual Asserts Terms criterion.

The choice of a right-to-use license as a *reverse* EULA also allows it to meet the Proactive Terms Specification criterion and the Choice About Being Remembered.

Finally, since a license is designed to have its details packaged up for the party needing to adhere to it, it meets the Terms Usability criterion.

Permission Scenarios with Right-to-Use Licensing Opportunities

Several permission scenarios, to date less common than those described above but variously increasing in usage, may align in interesting ways with right-to-use licensing.

UK Open Banking

An arm of the UK Government has created a set of regulatory and technical standards called Open Banking to oversee how banks as digital service providers share digital data out to third-party apps and arrange payments to them on customers’ behalf.[5] Thus, it is a species of the third-party permissions scenario described above. Currently, the UK’s nine largest banks and building societies are required to offer Open Banking. The standards are intended to achieve greater security, privacy, data portability, and interoperability than users sharing bank account passwords with third-party apps.

Open Banking connects the app with the user’s bank account in order to provide, for example, an aggregated view of bank data across several accounts, or to enable a payment to the app for a purchase of goods or services.

To satisfy a regulatory requirement, Open Banking has built in a technical mechanism using the OAuth and OpenID Connect protocols that has two parts, “consent” and “authorization”. The third-party app seeking permission takes the following actions:

1. Collects the particulars of the user’s “consent”, including which bank the customer uses and other relevant information
2. Bundles these consent details in a standardized data structure called the customer’s “intent”
3. Sends them to the bank and receives an “intent ID” in return
4. Redirects the customer to the bank service, along with the just-received ID, so the user can log in to the desired account there and “authorize” (confirm) their previously expressed intent

Note that the user’s intent is expressed prior to any exchange of data; it is “pushed” to the service before the user logs in there and the user confirms it after. This flow meets the Individual Asserts Terms and Proactive Terms Specification criteria. The fact that the intent data structure has been standardized for this sector and jurisdiction suggests the Terms Usability criterion could be met piecemeal. Though consent and authorization terminology are used, this scenario presents opportunities to align with a right-to-use license approach, at least (in its current form) with the third-party permissions scenario.

User-Managed Access

The User-Managed Access (UMA) protocol also builds on OAuth and OpenID Connect. UMA enables an individual to control the delegation of access to their digital data, content, services, and devices with other parties from a unified control point, even if the digital assets reside in multiple locations. [6]

UMA has been designed to provide greater security, privacy, and interoperability to the peer-to-peer sharing scenario described above (along with a variety of other scenarios). One typical user experience pattern is a “Share” button, where the user can configure different access constraints for different recipients, much as in Google Docs. Another is a “Pending Requests” interface, where the user can field collected requests for access and decide how much access to grant.

The authorization server role in UMA is a service provider that centrally protects a user’s digital assets on their behalf and their instructions. It maps to a Me2B Relationship Manager. This pair can support a user in controlling access for UMA sharing and delegation use cases. Figure 4 shows a mapping of Me2B relationships to UMA concepts.

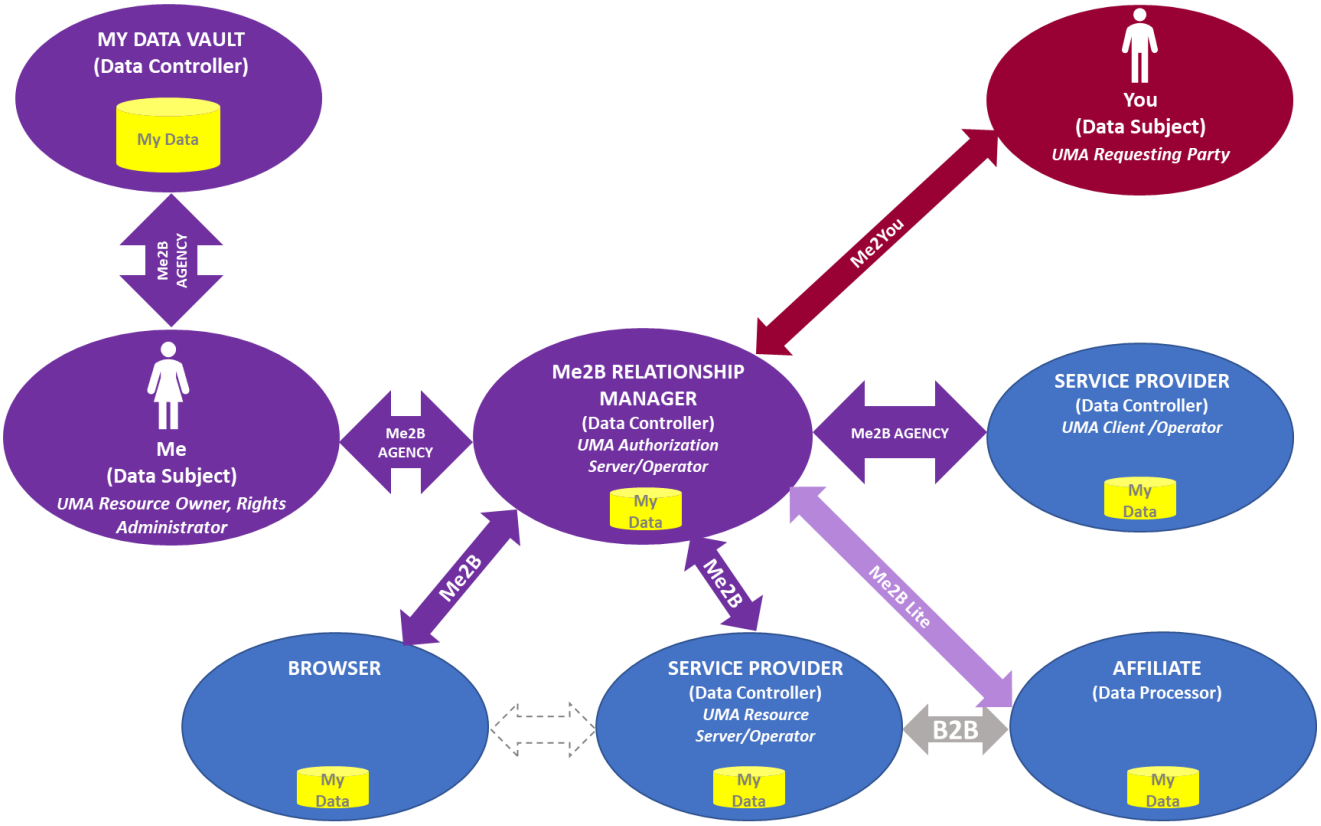

Figure 4. Me2B Relationships Mapped to UMA Concepts

UMA enforces constraints on access to an individual's resources in a manner somewhat akin to enterprise access control using authorization policy. This enables alignment with the Individual Asserts Terms and Proactive Terms Specification criteria because the user – rather than an enterprise – is in the "resource owner" role.

Further, the Kantara Initiative's UMA Work Group has produced a report proposing a business-legal framework that ties machine-readable licenses to various artifacts produced by the protocol, such as tokens and permission structures within them.[7] This work suggests opportunities for standardizing right-to-use license terms.

Decentralized Identity

Past iterations of decentralized identity work have suggested two concepts and technologies to be used for data sharing permissions. These are suggestive of two respective legal permission constructs: [8]

- **"Consent receipt ("consent"):** a receipt record that records proof that an identity owner has shared data with another party.

- **“Link contract:** A record of who is sharing data with whom, for what purpose and with what controls on its usage.”

However, current specifications for decentralized identity technologies do not cite these technologies, and do not have sufficient detail with respect to data sharing permission flows to allow us to make a sufficient analysis, either of type(s) of permission scenarios implemented, or of which of our criteria may be met.

Proposal for a New Permission Framework

A user-empowering permission framework must support the regulatory complexities and business needs of the digital service provider, and at the same time recognize the user’s right to agency and desires for convenience and value while in a Me2B relationship.

Right-to-Use License Components

Figure 5 illustrates the fields in the proposed right-to-use license. Several of the fields in the license are standard for licenses, such as Issuer and Grantee. [9]

RIGHT-TO-USE LICENSE											
WHO			*WHAT* RIGHT TO USE LICENSE PARAMETERS (What I Give)								*WHY* What I Get
PARTIES	**RELATIONSHIP TYPE**	**RELATIONSHIP ROLES (Me2B Example)**	**DATA ACQUISITION METHODS ALLOWED**	**DIGITAL ASSETS**	**GRANTEE(S)**	**DELEGATION**	**LEGAL DUTIES OF GRANTEE**	**ACTIONS**	**DESIGNATED PURPOSE /USAGE**	**LICENSE DURATION - excepting SP data retention requirements**	**VALUE**
Issuer - Data Subject (natural person)	Me2B* - Individual to Service Provider and beyond	Data Subject Roles (Customer-of, User-of, Patient-of, Benefactor-to, Student-of, Client-of, etc.)	Volunteered by DS	Specified Digital Assets	Service Provider (SP) Only	SP is assigned as Delegate, bounded by:	For PII: Dependent on Service Provider Type and Relationship; Fiduciary Duty, Duty of Care, Duty of Loyalty	Industry or Category Norms / Standard	Basic Service	1: this transaction only 2: as long as I have a relationship with you	Basic Service
Licensee - recipient of License (Natural or Legal Person)	Me2You* - Individual to Individual and beyond	Licensee Roles (Healthcare-Provider-to, Service-Provider-to, Product-Provider-to, etc.)	Unvolunteered by DS / Surveilled and/or derived inferred by SP		Specified 3rd Parties	(1) specified distribution	For non-PII: Duty of Care	Custom	Personalized Service	1: this transaction only 2: as long as I have a relationship with you	Personalized Service
	B2B - business to business; Service Provider to Affiliate, e.g.		Obtained by SP from 3rd Parties			(2) Subset of SP's rights			Altrusitic/Academic Purposes	3: I transfer rights permanently	Warm fuzzies
	Me2B - Individual to Employer					(3) custom Right-to-Use License parameters			Loyalty	1: this transaction only 2: as long as I have a relationship with you	Personalized Service + Monetary Value
	Me2G - Individual to Government					Unlimited Delegation Rights			Authentication Only	2: as long as I have a relationship with you	Being Remembered

Figure 5. Right-to-Use License

Data Use Templates

Achieving the Terms Usability criterion requires winnowing vast numbers of options. Therefore, for scalability from a business and legal perspective, as well as for human comprehension and usability, we propose providing data use templates as indicated in Figure 6. (Note that “data use” could refer to controlling a smart device or inserting data into a server-side repository as well as downloading data.)

DATA USE OPTION	**USER GIVES**	**USER GETS**	**EXAMPLE**
Me2B Deal Options			
Basic Service Only	Only enough information for the service to function properly.	Basic service	A music service plays music but has no capacity to make or retain playlists.
Personalized Service	Enough information to provide personalized service.	Personalized service	A music service plays music and can make and retain playlists.
Loyalty	What’s needed for personalized service, plus what’s wanted for service provider alternate revenue streams.	Personalized service plus monetary or equivalent value	A music service plays music, can make and retain playlists, can make AI-based recommendations, and can use personal data for other disclosed purposes.
Academic/Altruistic Add-On			
Altruistic/Academic Use	Can be added to any of the above three options.	Warm fuzzies about helping mankind	A music service can additionally use personal data to build a geographical map of music genre preferences for anthropological musicology studies.

Figure 6. Templated Data Use/Me2B Deal Options

These data use choices can map to industry- and/or company-specific templates.

Conclusions

We have examined today's consent and data sharing paradigms through the Me2B relationship lens and found that they are structurally and experientially flawed. This lens makes clear that digital technology – along with its business and legal underpinnings – has a long way to go to eliminate the power asymmetry and provide mutual agency between individuals and service providers.

It is difficult to fine-tune ecosystems. As one of us (Maler) noted in 2009:[10]

> All of the stakeholders — human beings, the manufacturers of the hardware and software tools they use, RPs, and IdPs — have different stakes, in an intricate mix. Along with "new-relationship energy", efficiency, and self-revelation habits, the parties might be influenced by privacy desires and regulations, legal liability, security vulnerabilities (each party having a dramatically different attack surface), enjoyment or productivity, profit motives, application flexibility, and more. Some goals sit in uneasy tension with others.

In these regards, little has changed in the intervening decade, though tension has increased as regulatory forces have attempted to shift the fulcrum of agency and control closer to the user. This will necessarily bring growing pains to many stakeholders.

We have discovered that cookie consent reflects the fundamental mismatch of consent to a user's requirements for service provider relationship management, in that it has a poor capacity for individual identification when desired by the user and an overcapacity for same when the user desires anonymity.

A key tension in resolving this mismatch relates to the use of cookie consent in the context of Me2B relationships – that is, meeting the Choice About Being Remembered criterion. In an ideal world, cookie consent would be supplanted by the combination of a service provider default that admits the setting only of cookies that are necessary for a service to function (cookies that might come under a strict interpretation of a "legitimate interest of the controller" GDPR personal data processing rationale), followed by the establishment of a long-term Me2B relationship within which the user is able to license further cookie use.

This, however, has the likely effect of further motivating service providers to a) provide deliberately thin user experiences in "strictly necessary cookie" environments and b) push more aggressively for the early creation of strong unique user identification where there is only heuristic user identification through cookies today. As noted earlier, users should be able to window-shop anonymously on the internet. The full reconciling of

cookie technology (and similar, such as browser fingerprinting) with window-shopping anonymity is a difficult challenge and beyond the scope of this article.

Progress is being made; both market and regulatory forces are driving implementation and adoption of capabilities such as Open Banking and UMA and facilitating the path toward mutual agency. The single greatest challenge will be to arrive at highly usable solutions for everyday people.

We have proposed a license-based framework that corrects the identified weaknesses and offers benefits to both service users and service providers by minimizing decision-making for the individual while allowing specificity when desired. This framework is only the starting point of a longer journey to explore, test, and eventually arrive at empowering yet effortless user-controlled permissions that support a mutually valuable ecosystem of digital services.

Future Work

The following areas of future work are suggested:

- Exploration of the Open Banking intent registration flow, UMA, IETF Internet-Drafts Rich Authorization Requests [11] and Transactional Authorization [12], and decentralized identity developments, for their opportunities to aid Me2B relationship setup in additional permission scenarios.
- Development of Me2B relationship manager prototypes to test the usability of the data use defaults for permissions. Testing could potentially leverage existing UMA authorization servers.
- Detailed analysis and evaluation of data use templates against real-world variations such as app type, sector, jurisdiction, user wishes. Some users will want the ability to fine-tune their right-to-use data licenses beyond the proposed templated choices. Some will want to negotiate the license real-time with the service provider. The proposed framework allows for variation.
- Detailed analysis of all stakeholder needs of the permission system.

References

[1] N. S. Kim, *Consentability*, Cambridge, UK: Cambridge University Press, 2019. [E-book] Kindle Edition.

[2] J. A. Obar,. and A. Oeldorf-Hirsch, “The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services, *TPRC 44:*

The 44th Research Conference on Communication, Information and Internet Policy, 2016, June 1, 2018. [Online],
Available: https://ssrn.com/abstract=2757465 or http://dx.doi.org/10.2139/ssrn.2757465.

[3] C. Utz, et al., "(Un)informed Consent: Studying GDPR Consent Notices in the Field," *CSS '19 Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security,* page 973-990, November 11-15, 2019. [Online], Available: https://www.syssec.ruhr-uni-bochum.de/media/emma/veroeffentlichungen/2019/09/05/uninformed-consent_Yl7FPEh.pdf.

[4] M. Spiegelberg, "Can Psychology Help Us Understand Our Changing Relationships with Brands?", April 6, 2011. [Online]. Available: http://popsop.com/2011/04/can-psychology-help-us-understand-our-changing-relationships-with-brands/. [Accessed Nov. 16, 2019].

[5] Open Banking Limited, "What Is Open Banking?", *Open Banking Limited*. [Online]. Available: https://www.openbanking.org.uk/customers/what-is-open-banking/. [Accessed Nov. 16, 2019].

[6] E. Maler et al., "User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization," *Kantara Initiative, UMA Working Group,* January 7, 2018. [Online]. Available: https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html. [Accessed Nov. 16, 2019].

[7] T. Reiniger, ed., "A Proposed Licensing Model for User-Managed Access," *Kantara Initiative, UMA Working Group,* Jan. 2018. [Online]. Available: https://kantarainitiative.org/file-downloads/uma-business-model-0-7e-2018-02-01-pdf/. [Accessed Jul. 5, 2019].

[8] Sovrin Foundation, "Sovrin Glossary," *Sovrin Foundation*, September 29, 2016. [Online]. Available: https://www.evernym.com/wp-content/uploads/2017/07/Sovrin-Glossary.pdf. [Accessed Nov. 10, 2019].

[9] This analysis was informed in part by E. Maler, "Designing a New Consent Strategy for Digital Transformation," *RSA Conference*. [Online]. Available: https://www.rsaconference.com/industry-topics/presentation/designing-a-new-consent-strategy-for-digital-transformation. [Accessed Nov. 7, 2019].

[10] E. Maler, "The design of everyday identity," *Online Information Review*, vol. 33, no. 3, 2009 pp. 443-457.

[11] T. Lodderstedt et al., “OAuth 2.0 Rich Authorization Requests”, *IETF, draft-lodderstedt-oauth-rar-03*, November 3, 2019. [Online]. Available: https://tools.ietf.org/html/draft-lodderstedt-oauth-rar-03. [Accessed Nov. 16, 2019].

[12] J. Richer, “Transactional Authorization”, *IETF, draft-richer-transactional-authz-03*, November 1, 2019. [Online]. Available: https://tools.ietf.org/html/draft-richer-transactional-authz-03. [Accessed Nov. 16, 2019].

Biographies:

Lisa A. LeVasseur (BS'88–MBA'00) received dual B.S. degrees in Computer Science and Philosophy from the University of Michigan, Ann Arbor, MI, USA, in 1988, the MBA degree in High Tech from Arizona State University, Tempe, AZ, USA, in 2000. From 1988 to 2003, she was with Motorola Corporation, Schaumburg, IL, USA. From 2004 to 2005, she was with the Kyocera Corporation, San Diego, CA, USA. From 2005 to 2006, she was with Amp'd Mobile, Los Angeles, CA, USA. From 2007 to 2009, she cofounded three startups. Since 2010, she has been designing privacy and agency enabling products. She is currently Vice President of Research and Technology in a not-for-profit foundation, Wrethinking the Foundation. She is the vice chair of the IEEE P7012 working group, she is actively involved in several Kantara working groups, and is co-creating the Me2B Alliance.

Eve Maler received a B.A. in Linguistics from Brandeis University in 1985. She is VP of Innovation & Emerging Technology in ForgeRock's Office of the CTO. She founded and leads the Kantara User-Managed Access (UMA) Work Group and is co-chair of the OpenID Foundation Health Relationship Trust (HEART) Working Group. Eve has provided expert advice to forums such as Open Banking, as well as the U.S. Office of the National Coordinator for Health IT for its API Security and Privacy Task Force and its "National Health IT Priorities to Advance Research" technical expert workshop. Eve co-invented the SAML and XML standards. Eve contributes to the rock 'n' roll outfit ZZ Auth and the Love Tokens.