1 Introduction to the Me2B Safe Specification

Note: We highly recommend reviewing the Me2B 101 Flash Guides (#1-10 which can be found here) in order to familiarize yourself with Me2B terminology, principles and ethos.

2 Glossary

2.1 Attribute

One of 10 qualities (so far) determined to be minimal criteria for a Me2B Commitment being deemed safe and respectful.

2.2 Data Flow Analysis

Data Flow Analysis is the act of evaluating the flow of data into and out of the website/app/service. This refers to the independent evaluation, using network analysis and other tools to understand where and with whom data is being shared. Many of the tests in this specification require data flow analysis. Conducting data flow analysis requires a trained expert in data supply auditing.

2.3 Data Subject, Data Controller, Data Processor, Data Processing

We use the standard GDPR definitions for each of these terms. See https://gdpr-info.eu/art-4-gdpr/

2.4 Illustrative Controls

Illustrative Controls refer to unique tests that are run. A control must be satisfied in order to receive a passing score on a test. This document doesn't include every possible test that is included in the Core Requirements and thus, the controls are illustrative only (and not comprehensive).

2.5 User Experience Evaluation

User Experience Evaluation is the act of evaluating the user interface of the website/app/service. Many of the tests in the Me2B Safe Specification require evaluation of the user interface. Conducting user experience evaluation requires a trained expert in user experience design.

3 Introduction

The Me2B Safe Specification is a *safety* specification—in contrast to an *interoperability* specification. The Me2B Safe Specification is a structured list of tests, with clear passing and failing criteria.

The first version of the specification is considered the "minimum viable" definition for being "safe" technology—the most basic, fundamental measurements of safety. To compare it the full spectrum of digital harms (as described in our Me2B Digital Harms Dictionary), version 1.0 of the specification covers only a portion of the described harms.

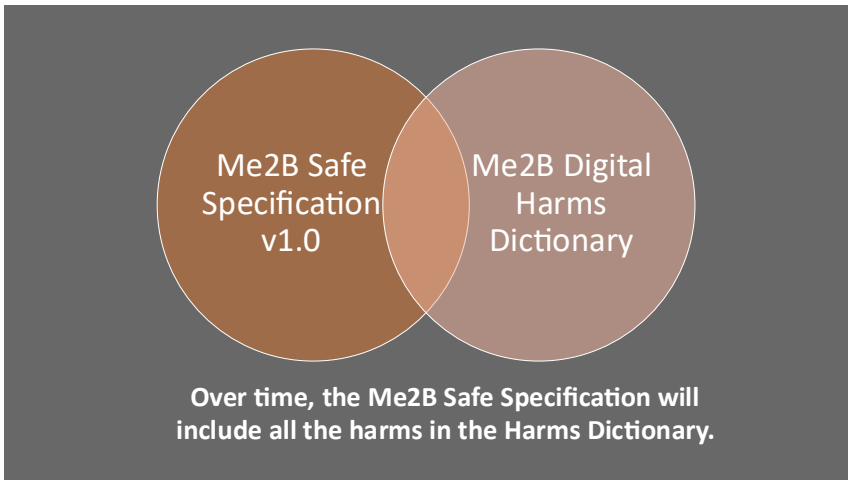

Figure 1 Relationship Between Spec v1.0 and Digital Harms Dictionary

Over time, subsequent versions of the specification will grow to include all of the harms defined in the Harms Dictionary.

4 Specification Architecture

Me2B Safe Specifications will be produced for each type of connected service and/or device such as:

- Websites
- Mobile Apps
- Wearables
- Medical Implants
- XR Devices/services
- Laptops / PCs
- Tablets
- Automobiles
- Smart Home Devices & Services

Version 1.0 of the specification covers websites and mobile apps.

All the specs would have the same fundamental structure (described below), with some differences unique to the type of service or device. In this way, there is fundamentally one baseline specification that is re-applied and customized as needed for each of the services listed above. The main set of tests will ultimately be stored in a database for easier reusability across services.

The specification is primarily a collection of spreadsheets:

1. Introduction/instructions
2. Data Controller Questionnaire
3. Core Requirements – this is the main body of delineated tests
4. Three files for use by the testers:
    a. Website Raw Data Collection worksheet – for testers to capture information about what data is being collected, shared and with whom,
    b. App Raw Data Collection worksheet – for testers to capture information about what data is being collected, shared and with whom,
    c. Raw Policy Info Collection worksheet – for testers to capture the key promises made in the privacy policy and terms of service, especially as it relates to data processing (collection, use, sharing, etc.)

4.1 Me2B Safe Specification Organization

Each specification tests each of the Me2B Commitments found in the service's user interface. Each Me2B Commitment represents a distinct value exchange (Me2B Deal), for which the user receives something of value (e.g., information) in exchange for providing something of value, typically in the form of information or online payment. Examples of Me2B Commitments are:

- Pre-Commitment or No-Commitment state (e.g., the state where the individual has opened an app/website/service for the very first time)
- Local Storage Commitment (e.g., Cookie commitment on websites)
- Location Commitment (e.g., providing location information to the service in order to receive location-relevant information)
- Promotional Commitment (e.g., signing up for newsletters)
- Contact Us Commitment(s)
- One-off Transaction (e.g., purchasing something as a guest)
- Loyalty Program
- Me2B Marriage (i.e., signing up for an account with the service)

Each of these commitments (including pre-commitment state) are tested against the 10 Attributes for Safe and Respectful Me2B Commitments. (See https://me2ba.org/library/recommendation-attributes-of-safe-respectful-me2b-commitments/) Each attribute has one or more unique tests.

Figure 2 below illustrates a simplified view of the testing flow—i.e., how the tests documented in the Core Requirements would be run in practice.

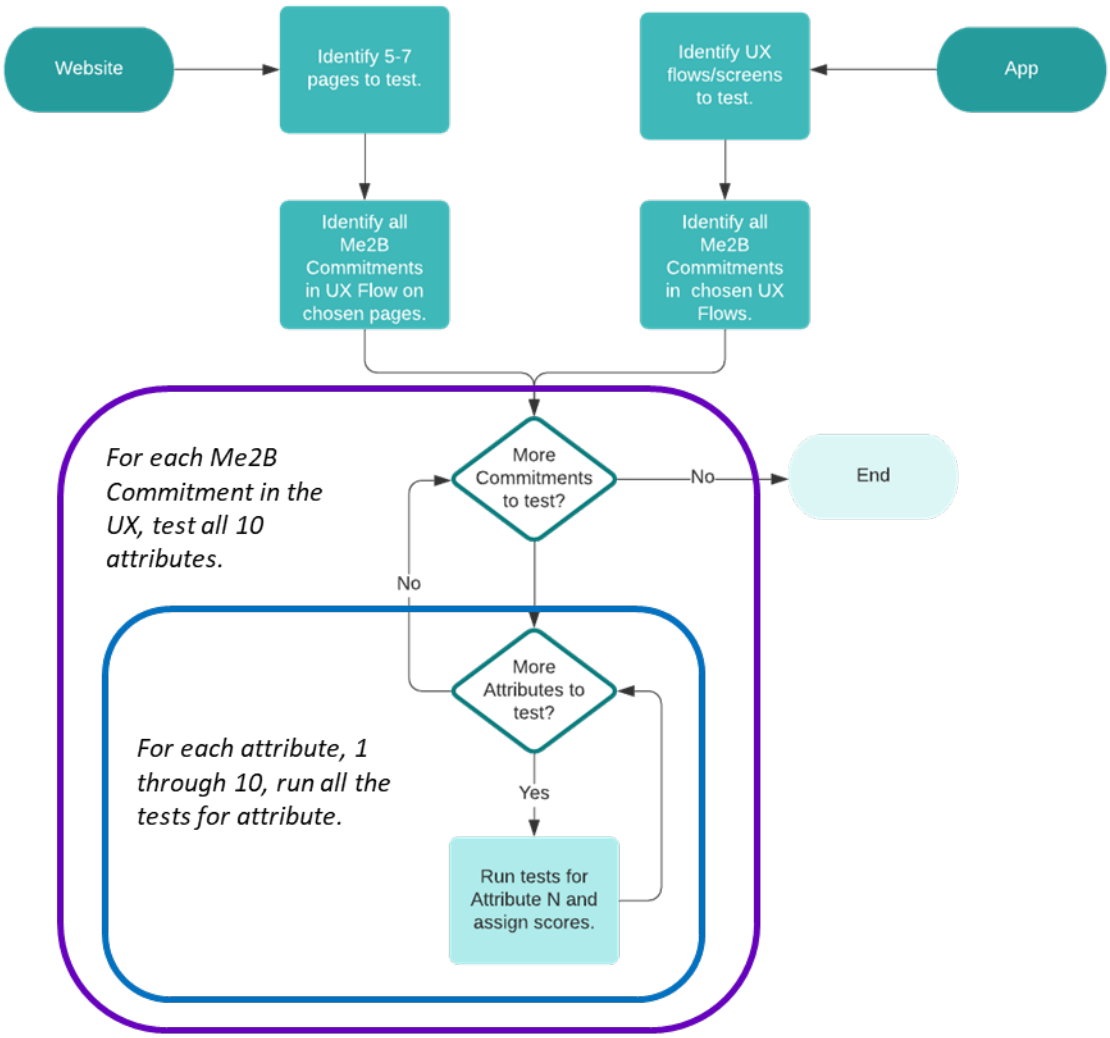

Figure 2 Specification Testing Flow

Note that it's impractical to test all the pages in a website—some websites are hundreds of pages in size. So, the first step of the website testing process is to identify the key 5-7 representative pages to test. A similar selection is made before testing a mobile app: determine the key UX flows and screens to be tested. Generally, the intention is to test all the UX flows and web pages that correspond to Me2B Commitments.

Each of those commitments would be tested against the 10 attributes of safe and respectful commitments.

Figure 3 provides more detail about the steps involved in using the specification materials to test a website or app.

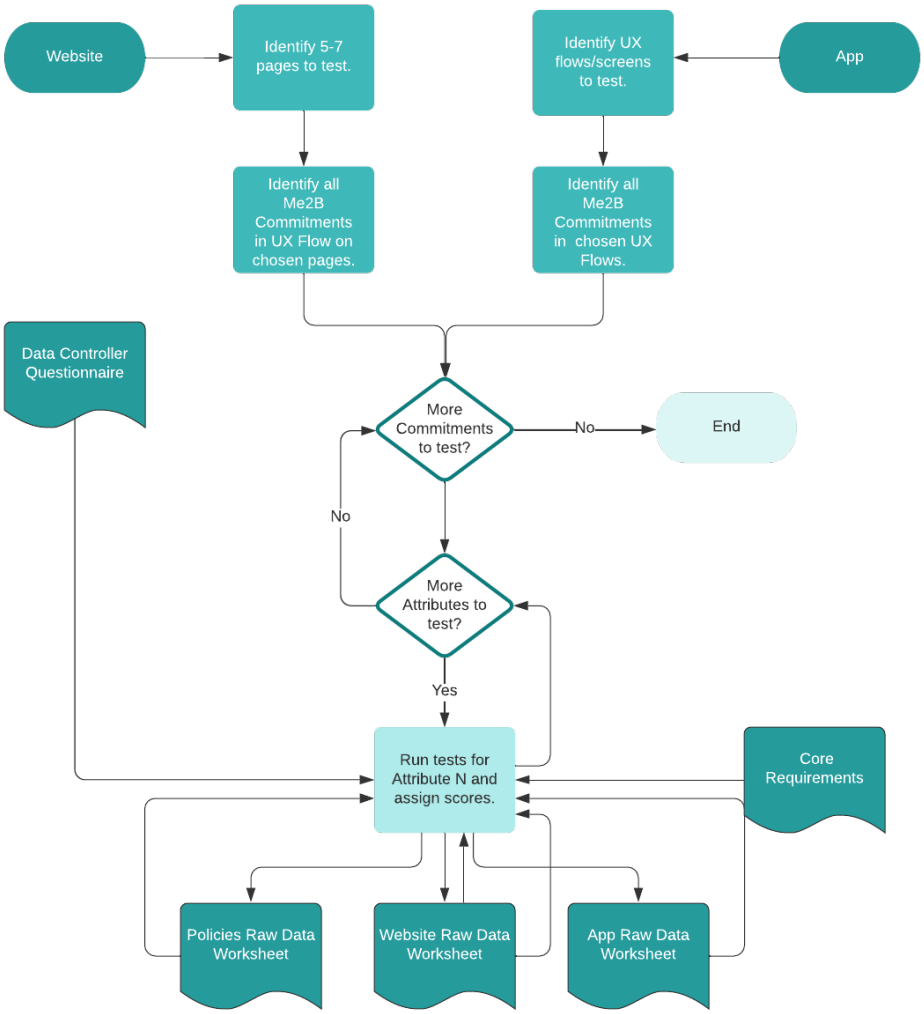

Figure 3 Website Testing Process & Spec Use

4.2 Me2B Commitment Context is Key

Why do we structure the testing in this way? Each commitment is a unique point in the overall Me2B Relationship lifecycle, reflecting a certain level of "intensity" of the Me2B Relationship. In particular, a Me2B Commitment is a transaction, with a unique value exchange between the Me and the B. We call this value exchange the “Me2B Deal”, **and for all Me2B Deals, the Me’s *information* is part of the currency of the deal.** It is this truth that creates many risks and

harms for Me-s, and thus, why it's such an important part of the Me2B testing structure; Me2B Commitments can be and often are *unsafe* and *disrespectful*.

Me2B Commitments represent unique points along the arc of the Me2B Relationship Lifecycle. As points on this lifecycle, they reflect not only the particular "behavioral economics" of the moment in time of the commitment, but also the trajectory of the arc—i.e., ascending or descending.

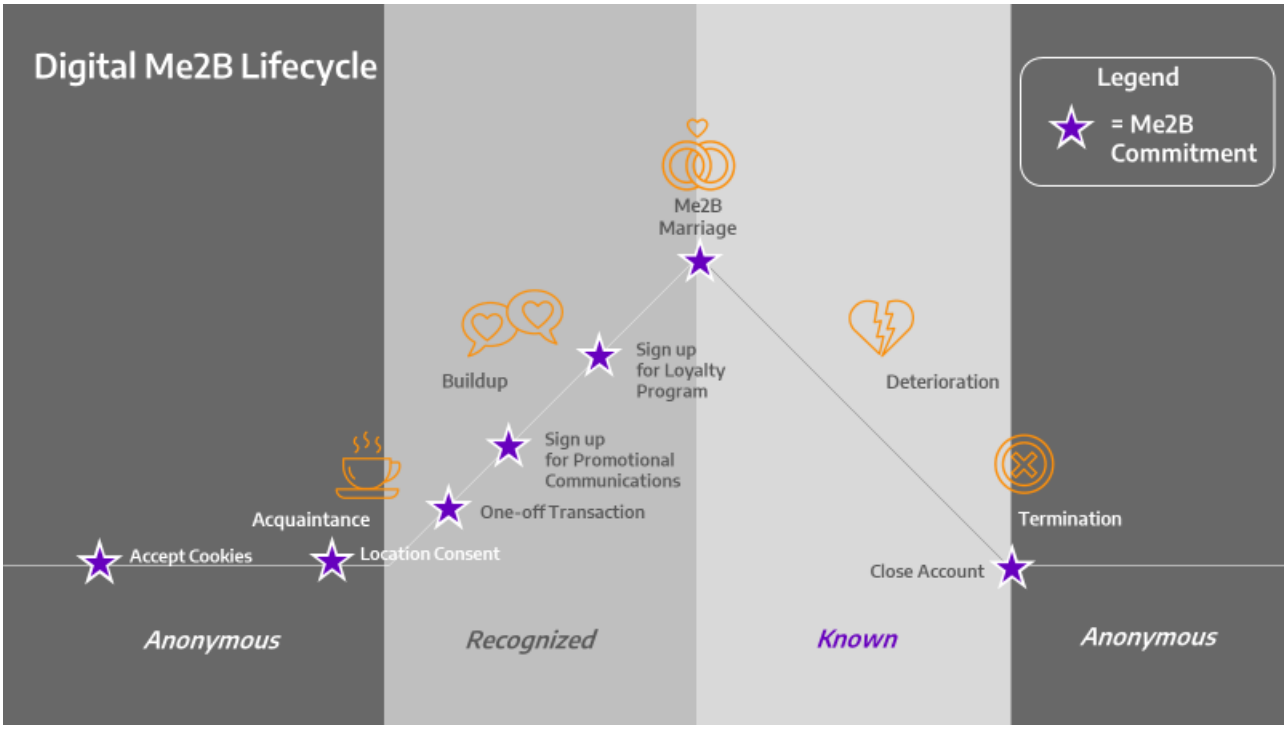

Figure 4: Me2B Lifecycle

A commitment is informed by and reflects three key things:

1. The Me's trust in the B and the B's product,
2. The Me's perceived value and expectations of the benefit to be received and if the cost is equitable, and
3. The vector/direction of the relationship—meaning, if the Me2B relationship is building and deepening, or if it's diminishing. If the Me is sharing yet more information, the relationship is necessarily deepening; if the Me is revoking the sharing of information, the relationship is necessarily diminishing. The only way a relationship vector remains neutral is if the commitment transaction is a virtual "repeat" of a previous transaction commitment.

This relationship lifecycle context mirrors the organic dynamics of our interpersonal relationships—where what we share reflects our trust in the other person, our expectations,

history, and perceived value of sharing. We may be so habituated to this kind of behavioral economic calculus that we no longer recognize that we're doing it. In our Me2B relationships in the digital world, the calculus is much more prominent, overt.

Take, for example, the Local Storage (including cookies) commitment. This commitment usually occurs very early on in the Me2B relationship and people's expectations of this particular commitment may be quite low, recognizing this is a kind of "entry gate" commitment. Whereas the so-called "Me2B Marriage" of creating a personal account reflects a much deeper--in fact, the deepest--stage of the relationship, and thus the user's behavioral economics in evaluating the costs/benefits of the deal (i.e., creating an account, being remembered, recognized, and personally responded to) are potentially (and hopefully) more thoughtful, meaningful.

To say it another way, each Me2B Commitment has tolerances that are unique to the level of the commitment and where it is on the Me2B Relationship arc. This "context sensitivity" is central to the Me2B Safe Specification. **Without this commitment-specific context, it's virtually impossible to derive objective scoring criteria.**

In addition to the tests that map to the commitments listed above, there is also a list of tests that are "commitment-agnostic" and apply unilaterally to every website, app or service being tested. These "commitment-agnostic" tests include high level security tests.

A note on security: The Me2B Safe specification is, by design, ***not*** a robust security certification. There are already many mature specifications for validating system security and practices. We chose not to duplicate those, but to confirm that some of the key best practices have been adopted.

5 How to Read the Tables in this Document

This introductory document communicates the high-level tests used to assess a commitment against the ten attributes for safe and respectful commitments. Each attribute has a summary table that includes:

- The attribute (high level principle) to be audited,
- The assessment criteria for the attribute, and
- Illustrative controls to measure the attribute; note that these are “illustrative” in that the list may not cover every test in every commitment.

6 ATTRIBUTE 1: Clear Data Processing Notice

ATTRIBUTE 1 - Clear Data Processing Notice (2 Criteria, 6 Controls)

This attribute assures that there is a clear Data Processing notice readily available to the user at the time(s) they need it. This attribute also ensures that the notice conveys full information surrounding the collection, use, and sharing of information.

ASSESSMENT CRITERIA	ILLUSTRATIVE CONTROLS
1.1 Existence of Notice	All of these controls are measured via User Experience (UX) evaluation. 1.1.1 The notice exists. It can be contained in the Privacy Policy, Terms of Service or other UX convention, but it must exist.
1.2 Understandability of Notice	1.2.1 The notice is easy to find, especially at the point of making the Me2B Commitment. 1.2.2 The data processing notice describes the data processing for the particular Me2B Commitment. 1.2.3 The notice accessible by machine readers (assistive devices). 1.2.4 The notice is complete. Notice includes minimally the following: - the Me2B Deal terms for the particular commitment (gives and gets) - how the collected information will be used - what "invisible information" (behavioral information, e.g.) is collected - how long information will be saved - who (what Data Processors, and specifically, company names) will receive information and what they use the information for, and how long they retain the information 1.2.5 The notice clear and easy to understand by the general population. Readable notice copy is at grade level 6 or better (lower) with additional explainer copy at grade level 6 or better as measured by: https://www.webfx.com/tools/read-able/flesch-kincaid.html

7 ATTRIBUTE 2: Viable Permission for Data Processing

ATTRIBUTE 2 - Viable Permissions for Data Processing (6 Criteria, 6 Controls) This attribute assures that no data is collected without viable permission. We use the Nancy Kim criteria for viable permission: (1) Understandability - the Data Subject readily understands the permissions being sought, (2) Freely given - the Data Subject is not coerced in any way including through dark patterns, and the permission is freely given, and, (3) Intentional action - the Data Subject provides an intentional action in order to signify permission; contracts of adhesion, for example, do not constitute intentional action.	
ASSESSMENT CRITERIA	**ILLUSTRATIVE CONTROLS**
	Controls 2.1.1 through 2.3.1 are measured via User Experience (UX) evaluation. 2.4.1 through 2.6.1 are measured through both UX evaluation and data flow analysis.
2.1 Understandability of requested permission	2.1.1 The information the Data Subject receives at the point of data collection and use is sufficient to provide informed permission.
2.2 Freely Given Permission	2.2.1 The Data Subject freely gives permission for the requested data (uncoerced, no dark patterns in UX).
2.3 Intentional Action	2.3.1 There is a required action the Data Subject must take in order to affirmatively provide permission for data processing, i.e., that data processing does not happen without the Data Subject's deliberate permission. For instance, contracts of adhesion, such as, "By continuing to use this website, you agree to our terms of service," do not constitute an intentional action and are unacceptable.
2.4 Permission Flow to Downstream Data Processors	2.4.1 The Data Subject's permissions flow downstream to all co-Data Controllers and Data Processors. This control is measured through data flow analysis and evaluation of self-reported answers provided by the Data Controller.

2.5 Appropriate Control	2.5.1 The data subject is afforded an appropriate level of control for the commitment parameters. E.g. If the service is collecting location information, depending on the nature of the service, the data subject should be given the option to share coarse- vs. fine-grained location information.
2.6 No Data Collection Prior to Data Subject Permission	2.6.1 The service does not collect commitment-related information prior to the data subject's explicit permission.

8 ATTRIBUTE 3: Identification Minimization

ATTRIBUTE 3 - Identification Minimization (2 Criteria, 2 Controls) This attribute assures privacy protection by ensuring that the level of identification [of the Data Subject] is proportional to the stage of the Me2B Commitment.	
ASSESSMENT CRITERIA	**ILLUSTRATIVE CONTROLS**
3.1 Assess whether or not the identification and data correlation performed by the data controller in the Me2B Commitment is appropriate and proportional to the Me2B Commitment.	*All of these controls are measured via data flow analysis.* 3.1.1 The identification in use reflects the stage of the Me2B Relationship, i.e., is proportional to the Me2B Commitment: COMMITMENT <--> IDENTIFICATION - None None - Local Storage Session ID (website); no cross-site IDs - Location Site + Session ID (website) - Promotional Comms Email - Customer Care Email - One-off Trans Unique Customer ID - Loyalty Program Unique Customer ID - Me2B Marriage Unique Customer ID See also Figure 4 below.

3.2 Assess whether or not the identification and data correlation performed by downstream co-data controllers and data processors is appropriate and proportional to the Me2B Commitment and Me2B Deal.	3.2.1 Data subject identification comports to appropriate state of Me2B Lifecycle, and the data subject "joinkey" isn't used to correlate behavioral data in an expected way by data processors & co-controllers. Data subject is not being actively tracked beyond the expected scope of this commitment per the Me2B Lifecycle.

Attribute 3: Identification Minimization - Me Experience

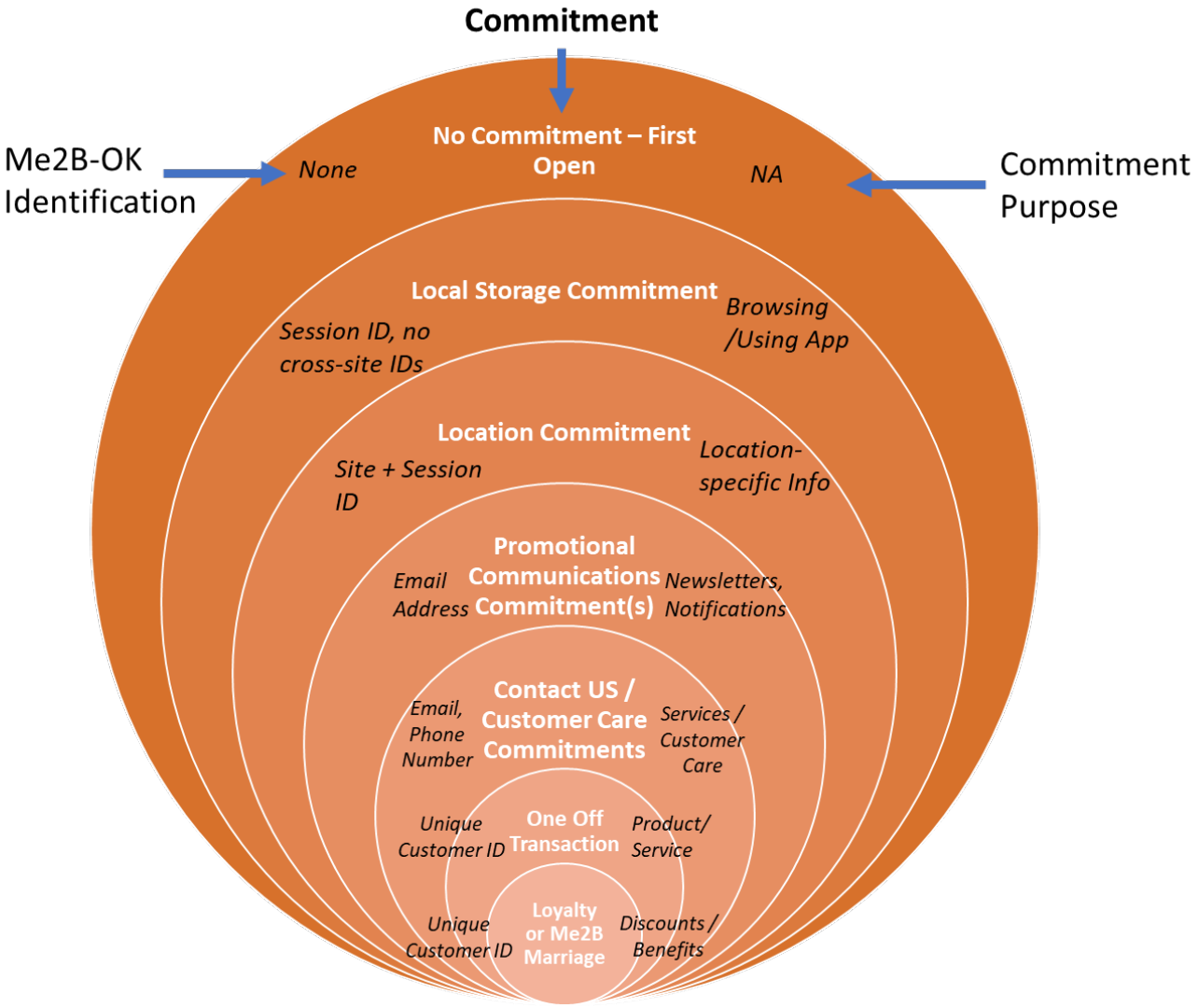

Figure 4 Identification Minimization

9 ATTRIBUTE 4: Data Collection Minimization

ATTRIBUTE 4 - Data Collection Minimization (1 Criteria, 4 Controls) This attribute assures that only the minimum amount of information is collected in order to provide the promised service.	
ASSESSMENT CRITERIA	**ILLUSTRATIVE CONTROLS**
	4.1.1 Each Me2B Commitment has a context-sensitive list of acceptable minimal data. Refer to Figure 5 for illustrative data collection minimization per Me2B Commitment. More details can be found in the detailed specification. (Measured via UX analysis.)
4.1 Assess whether the data being collected for the Me2B Commitment is reasonable for the Me2B Commitment.	4.1.2 Information volunteered by the data subject is appropriate for the particular Me2B Commitment. 4.1.3 Information observed by the data controller via data subject interaction is appropriate for the particular Me2B Commitment. 4.1.4 Information derived by the data controller is appropriate for the particular Me2B Commitment.

Attribute 4: Data Collection Minimization

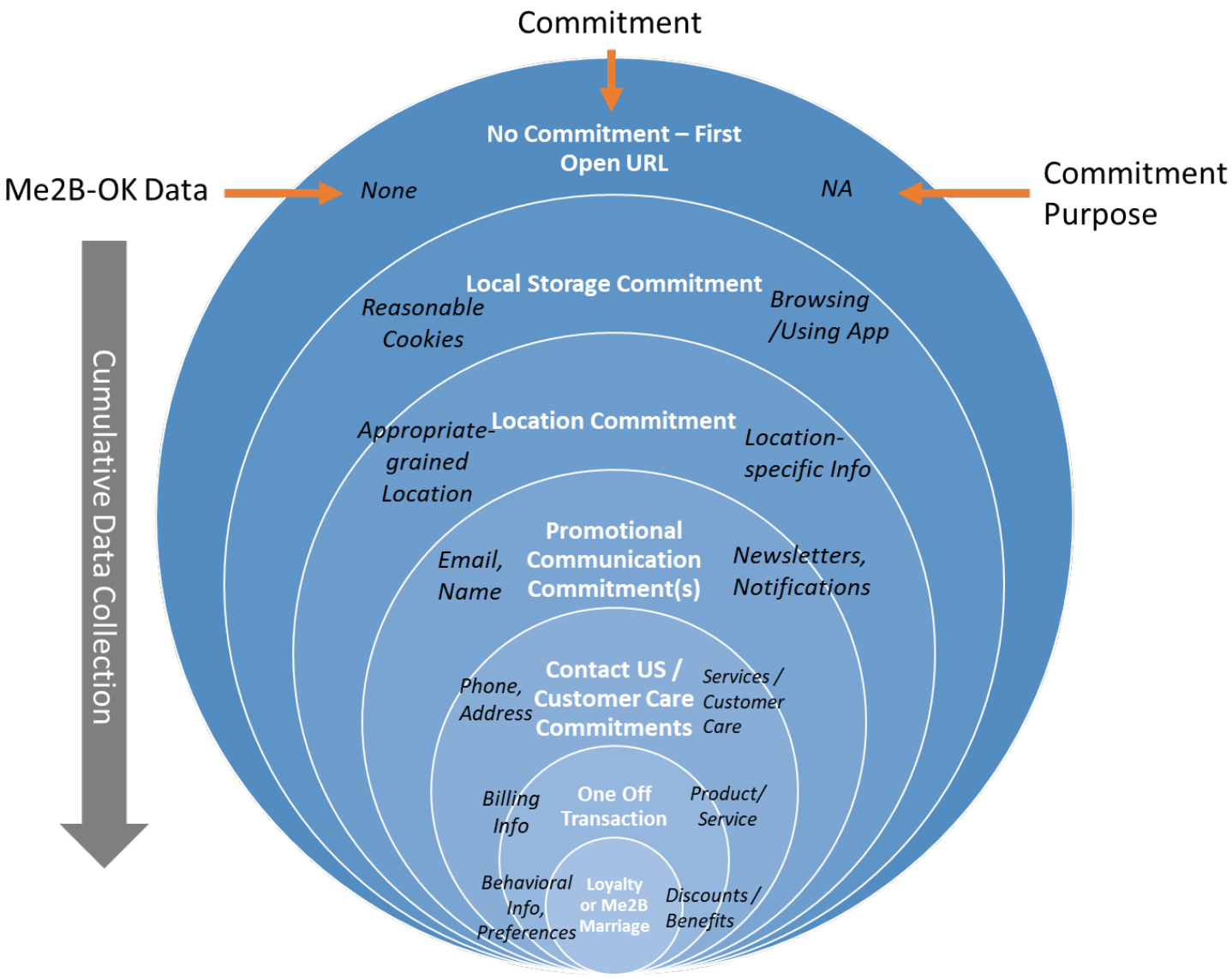

Figure 5 Data Collection Minimization per Commitment

10 ATTRIBUTE 5: Private by Default

ATTRIBUTE 5 - Private by Default (1 Criteria, 2 Controls) This attribute assures that the service (software) always defaults to the most conservative privacy settings and behaviors available, and that the Data Subject does not need to take any additional action in order to have a private experience.	
ASSESSMENT CRITERIA	**ILLUSTRATIVE CONTROLS**
5.1 Assess whether the information shared for the Me2B Commitment is automatically private by default, or if the Data Subject has to adjust settings in order to ensure privacy.	5.1.1 Each time the Data Subject enters a Me2B Commitment, no additional action is required in order to have a private experience. If there are privacy settings relating to the commitment, they default to the most private settings. (This control is measured via UX evaluation.) 5.1.2 Network traffic is evaluated in order to ensure that data isn't being automatically shared with Data Processors or co-Data Controllers in an inappropriate way. (This control is measured via data flow analysis as part of Attribute 6.)

11 ATTRIBUTE 6: Reasonable Data Use & Sharing Behavior

ATTRIBUTE 6 - Reasonable Data Use & Sharing Behavior (3 Criteria, 5 Controls) Similar to attributes 3 and 4, reasonable data use and sharing behavior is proportional to the Me2B Commitment under evaluation. This attribute assures that the data use and sharing behavior is proportional and appropriate to the particular Me2B Commitment.	
ASSESSMENT CRITERIA	**ILLUSTRATIVE CONTROLS**
	These controls are primarily measured via data flow analysis and evaluation of self-reported answers provided by the Data Controller.
6.1 Assess whether the collected data is being *used* in an expected and reasonable way.	6.1.1 Data Controller supplied information (questionnaire) matches observed data use behavior for the commitment.
	6.1.2 The UX doesn't indicate any unexpected (spurious) use of collected data. (This is determined by UX evaluation.)
6.2 Assess whether the Data Controller is reasonably *sharing* collected information with 3rd party co-data Controllers or Data Processors	6.2.1 Data Controller supplied information validates that collected data is only being shared with co-Data Controllers and Data Processors involved in fulfilling the commitment-specific services.
	6.2.2 Data flow analysis validates that data is only being shared with Co-Data Controllers and Data Processors involved in fulfilling the commitment-specific services.
6.2 Assess whether the level of data sharing is on par with industry norms.	6.3.1 Data sharing is equal or less than (better) than industry norms using the Me2BA industry benchmarks for similar services.

12 ATTRIBUTE 7: Data Processing Matches Data Subject's Permissions & Preferences

ATTRIBUTE 7 - Data Processing Matches Data Subject's Permissions & Preferences (1 Criteria, 3 Controls) This attribute assures that the observed data processing matches the Data Subject's permissions and preferences.	
ASSESSMENT CRITERIA	**ILLUSTRATIVE CONTROLS**
7.1 Assess whether or not the observed data processing (collection, use and sharing) matches the Data Subject's asserted preferences and permission.	All of these controls are measured via data flow analysis. 7.1.1 The observed data collection comports with the Data Subject's permissions & preferences. 7.1.2 The observed data controller data use and sharing comports with the Data Subject's permissions & preferences. 7.1.3 The observed data processor and co-data controller use and sharing comports with the Data Subject's permissions and preferences.

13 ATTRIBUTE 8: Data Processing Matches Policies

ATTRIBUTE 8 - Data Processing Matches Policies (1 Criteria, 6 Controls) This attribute assures that the observed data processing matches what is stated in the Data Controller's Privacy Policy and Terms of Service.	
ASSESSMENT CRITERIA	**ILLUSTRATIVE CONTROLS**
8.1 Assess whether the observed data processing (collection, use, and sharing) matches the Privacy Policy and Terms of Service.	These controls are measured by comparing the observed data processing behavior (UX and data flow analysis) to the promised data processing as described in the Data Controller's Privacy Policy and Terms of Service. 8.1.1 The observed data collection matches what's stated in the Privacy Policy. (Measured via UX analysis.) 8.1.2 The observed data collection matches what's stated in the Terms of Service. (Measured via UX analysis.) 8.1.3 The observed data use matches what's stated in the Privacy Policy. (Measured via UX and data flow analysis.) 8.1.4 The observed data use matches what's stated in the Terms of Service. (Measured via UX and data flow analysis.) 8.1.5 The observed data sharing matches what's stated in the Privacy Policy. (Measured via data flow analysis.) 8.1.6 The observed data sharing matches what's stated in the Terms of Service. (Measured via data flow analysis.)

14 ATTRIBUTE 9: Reasonable Commitment Duration

ATTRIBUTE 9 - Reasonable Commitment Duration (1 Criteria, 1 Control) This attribute assures that commitment duration is appropriate for the particular commitment.	
ASSESSMENT CRITERIA	**ILLUSTRATIVE CONTROLS**
9.1 Assess whether the observed Me2B Commitment duration (default) is appropriate for the Me2B Commitment.	9.1.1 Default duration for the commitment is appropriate for the commitment: **COMMITMENT <--> DEFAULT DURATION** - None NA - Local Storage Session duration - Location Session Duration - Contact Us Until the reason for contact has been completely fulfilled - Promotional Until Data Subject or Data Controller Terminates - One-off Trans As long as Data Controller legal obligations require - Loyalty Program Until Data Subject or Data Controller Terminates - Me2B Marriage Until Data Subject or Data Controller Terminates This control is measured via UX and data flow analysis.

15 ATTRIBUTE 10: Commitment Termination Behavior

ATTRIBUTE 10 - Commitment Termination Behavior (4 Criteria, 5 Controls) This attribute assures that the Data Subject can readily terminate commitments and that commitment termination behavior properly deletes any data and essentially "forgets" the Data Subject.	
ASSESSMENT CRITERIA	**ILLUSTRATIVE CONTROLS**
10.1 Assess the UX to determine if it's easy for the Data Subject to stop the Me2B Commitment.	10.1.1 The Data Subject can easily stop the Me2B Commitment. (Measured by UX analysis.)
10.2 Assess if the Data Subject receives a record of the change or termination of the Me2B Commitment.	10.2.1. The Data Subject receives a record of the termination of the Me2B Commitment. (Measured by UX analysis.)
10.3 Assess whether the Data Controller removes all collected data upon termination of the Me2B Commitment (as appropriate for the particular commitment and legal/tax requirements).	10.3.1 The Data Controller removes all collected data upon termination of the Me2B Commitment (except for data legally required to retain). (Measured by data flow analysis and UX analysis.)
10.4 Assess whether all downstream co-Data Controllers and Data Processors both receives and properly respond to changes to and termination of the Me2B Commitment.	10.4.1 All downstream co-Data Controllers and Data Processors receive notification that the Me2B Commitment has been terminated. (Measured via data flow analysis.) 10.4.2 All downstream co-Data Controllers and Data Processors delete Data Subject's data (except for data legally required to retain). (Measured via data flow analysis and self-reported information from Data Controller.)