Me2B ALLIANCE

Flash Guide #2

What is the Me2B Respectful Tech Specification?

Version 1.0 | July 22, 2021
Author: Me2B Alliance

#SafetyStandard #RespectfulTechSpec

IN A NUTSHELL

The Me2B Respectful Tech Specification is a sorely needed ethical and safety standard for the internet. It consists of a series of tests that objectively measure the behavior of a connected product or service. The Specification helps people ("Me-s") understand how technology is treating them, and helps businesses ("B-s") build technology that is safe and respectful for the people that use it.

The Me2B Respectful Tech Specification, produced by the Me2B Alliance's Respectful Tech Spec Working Group, is designed to provide an objective standard for measuring safe and ethical technology behavior. The Specification is intended to be a living document, to be updated regularly until it addresses all of the harms listed in our **Digital Harms Dictionary.** Each version is voted on and approved by the Alliance before publication. We anticipate that the first version of the Specification will be approved by the end of 2021.

The Specification consists of the following elements:

- The Core Respectful Tech Requirements,
- The Certification Application Questionnaire,
- Templates used to document the raw data being evaluated.

Our current Core Respectful Tech Requirements evaluate the behavior of websites and mobile apps, and are organized around Me2B Commitments. Me2B Commitments are the agreements a person can make when engaging with connected technology, such as agreeing to cookies or signing up for a newsletter.

The Requirements include multiple tests that assess a website or mobile app's behavior towards a user as they enter, engage in, and exit a Me2B Commitment. Each test includes a definition of Best Practice, Passing Behavior, and Failing Behavior, which map to a five-tier scoring system that ranges from -3 (riskiest) to +1 (exceptionally respectful):

Best Practice	Passing Behavior	Failing Behavior
+1 = exceptionally respectful behavior	0 = neutral / no detected risk or harm to Me	-1 = some risk to Me -2 = moderate risk to Me -3 = riskiest to Me

Conducting all of the tests described in the Core Requirements requires multidisciplinary expertise, including expertise in:

- **Data Integrity Testing:** Examining the flow of data out of the website or app and determining where the data is going.

- **Product Integrity Testing:** Examining the website or app functionality by exercising the user interface - i.e., using the service. This includes determining if individuals have an appropriate level of agency while using the service, as well as looking for other harmful usability patterns (often called “dark patterns”) in the user interface.
- **Legal and Policy Document Assessment:** Examining the Privacy Policy and Terms of Service to determine if they are understandable and appropriate. The Specification also validates if the product behaves as promised in these documents.
- **Security Assessment:** Security is a highly standardized discipline, and it would be redundant (and perhaps futile) to try to duplicate a full security evaluation. However, the Specification does include a small number of security checks, conducted by reviewing self-reported information from the service provider.

The majority of the Specification tests can be run independently of the service provider. The Certification Application Questionnaire addresses those areas that can’t be independently audited. These questions include, for instance, whether the business is sharing data at the back office - i.e. not directly through the website or mobile app.

Finally, the Specification includes a number of templates used to record the raw data observed during the evaluation.