Me2B Safe Spec for Respectful Technology Websites & Mobile Apps - Core Requirements

Version 1.0

RTS WG

26-Apr-22

VERSION	DATE	PLATFORMS	EDITORS	CONTRIBUTORS	DESCRIPTION OF CHANGES
0.1	8/21/21	Websites	L. LeVasseur	RTS WG	Candidate Working Group Approval draft
0.2	10/10/21	Websites	L. LeVasseur	RTS WG	WG Approved Draft
0.7	12/28/21	Websites, Mobile Apps	L. LeVasseur	RTS WG	Simplified after lack of comments in two review periods.
1.0	4/25/22	Websites, Mobile Apps	L. LeVasseur	RTS WG	None. Ready for Publication.

This workbook constitutes the Me2B Safe Specification Core Requirements for Websites and Mobile Apps.

CONTRIBUTORS

At the time this specification was completed, the Respectful Tech Spec Working Group had the following membership:

Lisa LeVasseur, *Co-Chair*
Mary Hodder, *Co-Chair*

Justin Byrd
Haley Dahlberg
Zach Edwards
Jeff Orgel
Jim Pasquale
Noreen Whysel
John Wunderlich

The following members of the Me2B Alliance participated in the Respectful Tech Specification Working Group for any length of time since 2019.

James Aschberger
Andrea Ausland
Ted Barthell
Justin Byrd
Haley Dahlberg
Daniella Doern
Zach Edwards
Guy Gabriele
Cam Geer
Jane Gould
Iain Henderson
Mary Hodder
Corey Jackson
Lisa LeVasseur
Camille Nebeker
Kelsey Nordstrom
Jeff Orgel
Jim Pasquale
Michele Silverthorn
Shaun Spalding
Jay VanBuren
Richard Whitt
Noreen Whysel
John Wunderlich

Me2B Safe Specification for Respectful Tech Introduction

How to use this Workbook

As a website provider/maker and data controller, you can use the Website Rubric to evaluate your own websites, by running each test on your own prior to applying for a Pre-Pre-Certification Audit.

It is STRONGLY suggested that you familiarize yourself with the Me2B 101 series of Flash Guides that can be found here: https://me2ba.org/library/#flashguides

Please refer to the Me2B Alliance Glossary also for terminology: <Add Link ASAP>

There are data collection templates for the webiste audit <here add link when published>

In applying for a Pre-Pre-Certification audit, you will be required to complete the Pre-Certification Questionnaire <here add link when published>.

How to Scope a Website Pre-Certification Audit:

When performing a Website Pre-Certification Audit, the Auditor and the data controller will agree on the scope of the audit, and specifically which pages will be tested. The Auditor will prioritize pages based on:
- Page reach
- Sensitivity context of page,

An audit should cover minimally 5-7 pages, but varies depending on the size and nature of the website.

The Auditor shall first identify all of the Me2B Commitments that appear on the selected webpages.

The Audit shall consist of the following tests:

- All of the tests on the "All Commitments" tab,
- The "Per Commitment" tests shall be run for each Me2B Commitment found in the selected webpages (see list of Me2B Commitments below), and
- The "Location Commitment" specific tests found on the "Location Specific Commitment" tab.
- The "Me2B Marriage" specific tests found on the "Me2B Marriage Specific Commitment" tab.

How to Scope a Mobile App Pre-Certification Audit:

When performing a mobile app Pre-Certification Audit, the Auditor and the data controller will agree on the scope of the audit, and specifically which UX flows & "pages" of the app will be tested. The Auditor will prioritize flows based on trying to cover all of the Me2B Commitments that exist in the app.

The Auditor shall first identify all of the Me2B Commitments that appear in the app.

The Audit shall consist of the following tests:

- All of the tests on the "All Commitments" tab,
- The "Per Commitment" tests shall be run for each Me2B Commitment found in the app (see list of Me2B Commitments below),
- The "Location Commitment" specific tests found on the "Location Specific Commitment" tab.
- The "Me2B Marriage" specific tests found on the "Me2B Marriage Specific Commitment" tab.

List of Me2B Commitments

- First open / no commitment
- Local Storage Commitment -- covering cookies and all local storage.
- Location Commitment
- Promotional Communication Commitment
- One-off Transaction Commitment
- Contact Us Commitment
- Loyalty Program Commitment
- Me2B Marriage Commitment

SERVICE REQUIREMENTS

TEST #	Me2B COMMITMENT	WHAT'S BEING MEASURED	DATA USED TO MEASURE	EXPERTISE NEEDED TO EVALUATE	BEST PRACTICE (SCORE = +1)	PASSING BEHAVIORS (SCORE = 0)	FAILING BEHAVIORS (SCORES -1 to -3)
Test Scope: These tests apply to the overall service and are independent of the Me2B Commitments that appear in the service.							
AL1	*ALL*	Does data controller use the IAB's transparency and consent framework (TCF)?	Pre-Certification Questionnaire	Data supply expert	NA	Do NOT use the IAB's TCF. (TCF should stop generating an ID and sharing it, and every org that receives an ID, it's a version of the ID.) Or use the IAB's TCF and make sure that the data processors support opting out https://optout.aboutads.info/?c=2&lang=EN	Use of the IAB's TCF (-1), and data processors don't support opting out (-3)
AL2	*ALL*	Data controller use of information from data brokers.	Pre-Certification Questionnaire	Data supply expert	NA	data controller uses data broker obtained info for identifying known bad emails.	-3 == data controller uses data broker-obtained info for marketing, customer acquisition, advertising.
AL3	*ALL*	Data controller selling or sharing information with data brokers.	Pre-Certification Questionnaire	Data supply expert	NA	No use of data brokers.	-3 == data controller sends data to at least one known data brokers.
AL4	*ALL*	Whether data subject can request and receive a copy of Personal Data (definitions per GDPR Article 4 (1), and Article (15)) including data provided/input by the data subject, and behavioral information about the data subject.	Observed UX	UX Expert	NA	data subject can easily request a copy of Personal Data (definitions per GDPR Article 4 (1) and Article 15), and receives an electronic copy of all Personal Data including behavioral information within 30 days, in a format that is easy for the individual to understand.	-3 == No way for data subject to request copy of Personal Data, or data subject requested Personal Data but never received.
AL5	*ALL*	Whether data subject can request changes to Personal Data (GDPR Article 16).	Observed UX	UX Expert	NA	data subject can easily request changes to Personal Data and the changes take place within 30 days.	-3 == Either No ability for data subject to request changes to Personal Data, or data subject requested changes never took place.
AL6	*ALL*	Whether data subject can request to have Personal Data deleted (GDPR Article 17).	Observed UX	UX Expert	NA	data subject can easily request to have Personal Data deleted and the changes take place within 30 days.	-3 == Either no ability for data subject to request deletion of Personal Data, or data subjected requested deletion but it was never deleted.
AL7	*ALL*	Whether the privacy policy is for the actual data controller (business)?	Privacy Policy	Analyst	NA	If the privacy policy is for the actual data controller (business).	-3 == Privacy policy is not for the actual data controller
AL8	*ALL*	Whether the terms of service policy is for the actual data controller (business)?	Terms of Service Policy	Analyst	NA	If the terms of service policy is for the actual data controller (business).	-3 == Terms of service policy is not for the actual data controller
AL9	*ALL*	Service's use of advertising/ad related local storage.	Observed UX	UX expert	NA	Opt in consent to agree to personalized ads. Before consent, only contextual ads.	Personalized ads appear on website without consent. (-3)
AL10	*ALL*	If the service uses Facebook advertising.	Observed raw data	Data supply expert	NA	Not sharing with Facebook	Sharing with Facebook (-3)
AL11	*ALL*	If the service uses Google advertising.	Observed raw data	Data supply expert	NA	Not sharing with Google	Sharing with Google (-3)
Test Scope: this series of tests are performed on the information security controls/maturity of the product's and organization's identity, data protection, encryption, and security assessment/testing							
SE1	*All*	Whether personnel collecting, utilizing, and responsible for safeguarding sensitive/regulated data are briefed and trained	Pre-Certification Questionnaire; Summary results from Pre-Certifications mentioned in Column H.	Security Expert	**NIST Cybersecurity Framework (CSF)** Protect: PR.AT- 1, PR.AT-2, PR.AT- 3, PR.AT- 4 / **NIST SP 800-53 Rev.5** AT-3, PM-13, SA-9, SA-16/ **HITRUST** Control Category 01.c, 02e, 13.t/ **PCI DSS Requirement** 6, 9 / **FFIEC** Domain 1 Cyber Risk Management and Oversight - Strategies&Policies, Training/ **ISO 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2	Organization provides annual, and as mandated, training to applicable internal/contracted audit, privacy, information/cyber security and legal personnel in relation to data protection and privacy regulatory and compliance mandates.	-3== Organization has not met regulatory mandate to train personnel collecting, utilizing, and responsible for safeguarding sensitive/regulated data -2 == No awareness and training program defined per best/leading practices -1== Identified personnel not required to receive/report completed training
SE2	*All*	The capability and implemented security controls to securely provide access and to create, manage, and authenticate one's identity.	Pre-Certification Questionnaire; Summary results from Pre-Certifications mentioned in Column H.	Security Expert	**NIST Cybersecurity Framework (CSF)** ID.GV-4, PR.AC-1, PR.AC4, PR.AC-5, PR.AC-6, PR.AC-7 / **NIST SP 800-53 Rev.5** 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-7, AC, 12, AC-14, AC-16, AC-20, AC-24, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 PM-3, SA-2/ **HITRUST** Control Category 01.a, 01.c, 01.d, 01.e, 01.q, 01.u, 02.h, 02.i, 13.s /**PCI DSS Requirement** 2, 3, 4, 6, 7, 8, 10/ **FFIEC** Domain 1 Cyber Risk Management - Audit, Domain 3 Cybersecurity Controls - Infrastructure Management, Access and Data Management, Anomalous Activity Detection, Domain 5 Cyber Incident Management and Resilience - Detection, Response and Mitigation, Escalation and Reporting/ **ISO 27001:2013** A.6,A.7, A.9, A.11, A.13	Organization/product provides a secure process to create, store, and authenticate one's identity by utilizing secure communication/data transfer of credentials and securely storing Personally Identifiable Information (PII).	-3==Personally Identifiable Information (PII) entered by user is captured/stored in plain text -2==Passwords (PWs) are generated/captured/stored in plain text -1==Product does not offer secondary factor (2FA) for authentication.
SE3	*All*	The compliance and technical capability to protect sensitive or regulated data	Pre-Certification Questionnaire; Summary results from Pre-Certifications mentioned in Column H.	Security Expert	**NIST Cybersecurity Framework (CSF)** Protect: ID.GV 3, ID.GV-4, PR.DS- 1, PR.DS-2, PR.DS-3, PR.DS-5, PR.DS-7, PR.IP-6, PR.IP-12/ **NIST SP 800-53 Rev.5** AC-4, AC-5, MP-6, PE-19, PM-3, SC-8, SI-2, SI-4/ **HITRUST** Control Category 06.d, 0.6f, 0.9aa, 13.j,13.k, 13.q/ **PCI DSS Requirement** 3, 9, 10 / **FFIEC** Domain 1 Cyber Risk Management and Oversight - IT Asset Management, Audit; Domain 3 Cybersecurity Controls - Access and Data Management, Event Detection; Domain 4 External Dependency Management - Connections, Contracts; Domain 5 Cyber Incident Management and Resilience, Planning, Testing, Detection **/ISO 27001:2013** A.6, 7, 8, 9, 10, 11, 13, 14, A.16.1.6, Clause 9, Clause 10	Sensitive/regulated data is managed and protected in accordance with applicable regulatory mandates and compliance (e.g. GDPR, CCPA, PIPDEA, GLBA, etc.). Sensitive/regulated data should be safeguarded (encrypted or tagged/classified) to negate or minimize harm caused by data breaches/leakage).	-3== Verified successful data breach incident (<180 days or unresolved) -2== External Regulator/Auditor "data protection" material weakness noted -1== Absence of data protection policies or programs

SE4	*All*	Whether encryption standards/protocols are employed as data and information are entered (ingested), handled, processed, stored, or presented	Pre-Certification Questionnaire; Summary results from Pre-Certifications mentioned in Column H.	Security Expert	**NIST Cybersecurity Framework (CSF)** Protect: PR.PT-2, PR.PT-4, PR.DS- 1, PR.DS-2, PR.DS-3, PR.DS-5/ **NIST SP 800-53 Rev.5 AC-4,** SC-8, SC-11, SC-12, SC-13, SC-20, SC-21, SC-22, SC-23, SC-28, SC-38, SC-31, SI-4/ **HITRUST C**ontrol Category 06.d, 10.f/ **PCI DSS Requirement** 1, 3, 4, / **FFIEC Domain** 3 Cybersecurity Controls Access and Data Management/ **ISO 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2., A.8.2..1, A.8.2.2, A.8.2.3,A.8.3.1, A.8.3.2, A.8.3.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.11.2.5, A.11.2.7, A.11.2.9, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3	Session layer encryption and secure protocols (e.g. Secure Sockets Layer (SSL)), for sensitive and regulated data in transit is protected/encrypted at the web, mobile, etc. application level (production and non-production) per NIST best practices/guidance; to include personally identifiable information (PII) shared by user (form/field based entry). Sensitive and regulated data at rest (production and non-production) is protected by native or 3rd party encryption technologies.	-3== No implementation of secure protocols or encryption technology (application or data repositories) -2== Inaccurate or lesser standard encryption/secure protocols per data type (e.g., financial, govt., etc.) -1== Deployment of archaic/legacy secure protocols
SE5	*All*	Whether the application/product has critical or high vulnerabilities (security assessments) that could potentially lead to exposed or leaked sensitive information and defined remediation plan(s)	Pre-Certification Questionnaire; Summary results from Pre-Certifications mentioned in Column H.	Security Expert	**NIST Cybersecurity Framework (CSF)** Identify: ID.SC-4; Respond: RS.AN -5/ **NIST SP 800-53 Rev. 5** RA-5, SI-5, PM-15/ **HITRUST** Control Category 03.b, 08.d, 11.a, 13.q, 13.u/ **PCI DSS Requirement** 5, 6/ **FFIEC** Domain 3 Cybersecurity Controls: Secure Coding, Threat and Vulnerability Detection/ **ISO 27001:2013** A.15.2.1, A.15.2.2	Conduct initial and, at minimum, annual ongoing security assessments to include, where appropriate, but not limited to Static Application Security Testing (SAST)/Dynamic Application Security Testing (DAST), Penetration Testing, and continuous vulnerability management monitoring/scanning	-3== No testing/validation completed in the lifecycle of product development -2== No testing/validation completed in > 18 months -1== Lack of documented remediation/risk-based acceptance of identified High or Critical vulnerabilities
SE6	*All*	Whether data controller encrypts all Personally Identifiable Information at rest and in transport with the most respectful encrypted string and doesn't create a new persistent ID.	Pre-Certification Questionnaire	Security Expert	Data controller encrypts data at rest and in transport using optimal recommended methods for each type of info. Data controller doesn't create a new persistent ID.	Data controller encrypts data at rest and in transport using optimal recommended methods for each type of info. Data controller doesn't create a new persistent ID.	-3== No encryption in place on sensitive/regulated data (personally identifiable information) at any/all levels of the tech stack (e.g., data at rest, data in motion, etc.) -2== Lesser data standards and security/protection protocols (e.g., obfuscation/masking) used in lieu of encryption -1== Utilization of native encryption protocols vs. enhanced 3rd party encryption protocols and standards

SAFE & RESPECTFUL COMMITMENT TESTS - TEMPLATE

TEST #	Me2B COMMITMENT	SAFE & RESPECTFUL COMMITMENT ATTRIBUTE	WHAT'S BEING MEASURED	DATA USED TO MEASURE	EXPERTISE NEEDED TO EVALUATE	PASSING BEHAVIORS (SCORE = 0)	FAILING BEHAVIORS (SCORES -1 to -3)
Test Scope: These tests should be run (duplicated) for each Me2B Commitment that exists in the chosed audit scope (i.e. webpages or UX flows in an app).							
ATTRIBUTE 1: CLEAR DATA PROCESSING NOTICE							
A1-1	*<xxx> Commitment*	*(1) Clear Data Processing Notice - Existence*	If there is a data processing notice available to the user.	Observed UX	UX expert	There is a data processing notice available.	-3 == Data processing notice is missing
A1-2	*<xxx> Commitment*	*(1) Clear Data Processing Notice - Understandability - Accessible*	If the data processing notice is present/available on the same screen as the commitment.	Observed UX	UX expert	The data processing notice/information is available on the same screen as the commitment--without having to go to another page.	-2 == Data processing notice is not on the same screen.
A1-3	*<xxx> Commitment*	*(1) Clear Data Processing Notice - Understandability - Scope*	If the data processing notice explains (breaks out) data processing for each level of Me2B Commitment. E.g. the notice explains which information is collected for each type of commitment.	Observed UX	UX expert	The data processing notice is either specific to the commitment, or, if general for the whole website/app, contains sections for each commitment level.	-3 == Data processing notice does not clarify data process per Me2B Commitment.
A1-4	*<xxx> Commitment*	*(1) Clear Data Processing Notice - Understandability - Accessible*	If the data processing notice is accessible by assistive services.	Observed UX; Voiceover on Mac or NVDA on Windows	UX expert	The data processing notice/information is accessible and rendered by assistive services.	-3 == The assistive screen reader is unable to read any of the notice. -2 == The assistive screen reader is unable to read most of the notice. -1 == The assistive screen reader is unable to read part of the notice.
A1-5	*<xxx> Commitment*	*(1) Clear Data Processing Notice - Understandability - Complete*	If the data processing notice of the <commitment name> (Me2B Deal) that the data subject receives on the website is complete, providing details: (1) the Me2B Deal Terms (quid pro quo) including subsidization and data monetization; (2) list of information collected (covering volunteered, observed and derived information); and (3) for each item of information, (a) legal basis for collection, (b) purpose for collecting the information including how it's used, (c) all data processors & co-controllers who receive it, and (d) how long the information is retained (by all data controllers and co-processors).	Observed UX	UX expert	The information the data subject receives at the point of the commitment looks complete per cell 9E (i.e. includes all of the necessary categories/sections of information).	-3 == Processing notice is missing a section from the list in 9E.
A1-6	*<xxx> Commitment*	*(1) Clear Data Processing Notice - Understandability - Clear*	If the data processing notice of the <xxx> commitment is clear and easy to understand by the general population.	Observed UX	UX expert	The copy for the website notice for the <xxx> commitment is clear and easy to understand by the general population. Readable privacy policy for site is at grade level 6 or better (lower) as measured by: https://www.webfx.com/tools/read-able/flesch-kincaid.html https://datayze.com/readability-analyzer.php or other site.	-3 == Reading comprehension score is above Flesch Kincaid 8th grade level or similar readability score -1 == Reading comprehension score is above Flesch Kincaid 6th grade reading level or similar readability score
ATTRIBUTE 2: VIABLE PERMISSION							
A2-1	*<xxx> Commitment*	*(2A) Viable Permission - Understandability*	If the information the data subject receives at the point of the <xxx> commitment is sufficient to provide informed permission. (this is tested in Attribute 1--the rolled-up average scores for Attribute 1 satisfy this criteria.)	Attribute 1 Tests	Attribute 1 tests	If the roll-up average scores for Attribute 1 is between 0 and -0.49.	If the roll-up average scores for Attribute 1 are =< -0.5
A2-2	*<xxx> Commitment*	*(2B) Viable Permission - Freely Given*	If the data subject freely gives permission for the <xxx> commitment.	Observed UX	UX expert	No dark patterns detected in the commitment UX.	Harmful patterns detected in <xxx> Commitment UX. (range -1 to -3) Data subject is required to agree to terms of service prior to account creation. (-3)
A2-3	*<xxx> Commitment*	*(2C) Viable Permission - Intentional Action*	If the data subject performs an intentional action to enter the <xxx> commitment.	Observed UX	UX expert	There is a discrete, permission UX for the commitment.	No consent or permission mechanism for the commitment. (-3)
A2-4	*<xxx> Commitment*	*(2D) Viable Permission - Flow to data processors*	If the data subject's permissions for data related to this commitment are passed to all third parties - co-data controllers and data processors.	Pre-Certification Questionnaire; Observed raw policy data	Analyst	Data controller confirms that data subject permissions for commitment are passed to all co-data controllers and data processors.	Permissions are not passed to co-data controllers or data processors (-3)
A2-5	*<xxx> Commitment*	*(2) Viable Permission - Appropriate Level of Control*	If 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.	Observed UX	UX expert	Data subject has an appropriate level of control for the commitment parameters.	Data subject controls are are inadequate/insufficient/too coarse-grained. (-3) Data subject controls are somewhat inadequate/sub-optimal. (-1)
A2-6	*<xxx> Commitment*	*(2) Viable Permission - No Data Collection Before Permission Granted*	If the service collects commitment-related information before the data subject grants permission.	Observed UX, Observed local & network data	UX expert; Data supply expert	No commitment-related information is collected before the data subject grants permission.	Commitment-related information is collected before the data subject grants permission. (-3)
ATTRIBUTE 3: IDENTIFICATION MINIMIZATION							
A3-1	*<xxx> Commitment*	*(3) Identification Minimization - Data Controller*	Data subject identification comports to appropriate state of Me2B Lifecycle. Is the data subject "joinkey" being used to correlate behavioral data in an expected way by the data controller? Is the data subject being actively tracked beyond the expected scope of this commitment per the Me2B Lifecycle?	Observed local & network data	Data supply expert	Identification and data subject profiling performed by the data controller comports with the Me2B approved identification for the commitment.	Identification performed exceeds the Me2B-approved identification for the commitment (refer to Figure 4 in the Me2B Safe Specification Introduction). (-3)
A3-2	*<xxx> Commitment*	*(3) Identification Minimization - Data Processors and Co-Controllers*	Data subject identification comports to appropriate state of Me2B Lifecycle. Is the data subject "joinkey" being used to correlate behavioral data in an expected way by data processors & co-controllers? Is the data subject being actively tracked beyond the expected scope of this commitment per the Me2B Lifecycle? Note: testing the Local Storage Commitment covers advertising and analytics related cookies or other joinkeys.	Observed local & network data	Data supply expert	Identification and data subject profiling performed by data processors and co-controllers comports with the Me2B approved identification for the commitment.	Identification performed exceeds the Me2B-approved identification for the commitment (refer to Figure 4 in the Me2B Safe Specification Introduction). (-3) Service is using shared joinkeys with advertisers/analytics/data brokers outside of the expected Me2B Deal. (-3)
ATTRIBUTE 4: DATA COLLECTION MINIMIZATION							

A4-1	*<xxx> Commitment*	*(4) Data Collection Minimization*	The minimum **volunteered** information required for this commitment is (refer to Figure 5 in the Me2B Safe Specification Introduction for Me2B-approved data for this commitment). No other data is required.	Observed UX	UX expert	Website only collects the information described in Figure 5 and no additional information when entering this commitment.	Other lower-harm/lower-sensitivity information also collected. (-1, -2) Harmful/sensitive information also collected. (-3)
A4-2	*<xxx> Commitment*	*(4) Data Collection Minimization*	The minimum **observed** information required for this commitment is (refer to Figure 5 in the Me2B Safe Specification Introduction for Me2B-approved data for this commitment).	Data Supply Flow	Data supply expert	Website only collects the information described in Figure 5 and no additional information when entering this commitment.	Other lower-harm/lower-sensitivity information also collected. (-1, -2) Harmful/sensitive information also collected. (-3)
A4-3	*<xxx> Commitment*	*(4) Data Collection Minimization*	The minimum **derived** information required for this commitment is (refer to Figure 5 in the Me2B Safe Specification Introduction for Me2B-approved data for this commitment).	Data Supply Flow	Data supply expert	Website only collects the information described in Figure 5 and no additional information when entering this commitment.	Other lower-harm/lower-sensitivity information also collected. (-1, -2) Harmful/sensitive information also collected. (-3)
ATTRIBUTE 5: PRIVATE BY DEFAULT							
A5-1	*<xxx> Commitment*	*(5) Private by Default*	The individual doesn't have to modify any privacy settings in order for the data associated with this commitment to be used only in the context of this commitment and Me2B Deal.	Observed local & network data	Data supply expert	Data associated with this commitment is not shared to unnecessary data processors by default.	There are settings that the data subject must configure in order to assure shared data in this commitment is used only this commitment's Me2B Deal. (-3)
ATTRIBUTE 6: REASONABLE DATA USE & SHARING BEHAVIOR							
A6-1	*<xxx> Commitment*	*(6) Reasonable Data Use Behavior*	If the information use claims provided by the data controller match the observed data use [by the data controller].	Observed local & network data	Data supply expert	Observed data controller data *use* matches supporting information provided by data controller in the questionnaire.	-3 == Observed data *use* behavior for the commitment differs from information in the data controller provided questionnaire responses.
A6-2	*<xxx> Commitment*	*(6) Reasonable Data Use Behavior*	If the information use by the data controller is appropriate to the commitment.	Observed local & network data	Data supply expert	Service only uses <xxx> commitment information in order to provide <commitment name> services, as defined by the Me2B deal terms for the commitment.	-3 == Data controller uses data collected for this commitment outside of the bounds of the agreed-upon Me2B deal terms for this commitment, in a way that exposes the data subject to serious risks. -2 == Data controller uses data collected for this commitment outside of the bounds of the agreed-upon Me2B deal terms for this commitment in a way that exposes the data subject to moderate risks. -1 == Data controller uses data collected for this commitment outside of the bounds of the agreed-upon Me2B deal terms for this commitment in a way that exposes the data subject to low risks.
A6-3	*<xxx> Commitment*	*(6) Reasonable Data Sharing Behavior*	If the information sharing claims provided by the data controller match the observed data sharing [by the data controller].	Observed local & network data	Data supply expert	Observed data controller data *sharing* matches supporting information provided by data controller in the questionnaire.	-3 == Observed data *sharing* behavior for the commitment differs from information in the data controller provided questionnaire responses.
A6-4	*<xxx> Commitment*	*(6) Reasonable Data Sharing Behavior*	If the information sharing [by the data controller] with data processors and co-controllers is appropriate to the commitment.	Observed local & network data	Data supply expert	Service only shares <xxx> commitment information with mandatory data processors in order to provide <commitment name> services.	-3 == Service shares <xxx> commitment information with advertisers, OR with any data processor using a globally unique joinkey. -2 == Service shares <xxx> commitment information with analytics platforms without a globally unique joinkey -1 == Service shares <xxx> commitment information with other 3rd parties.
A6-5	*<xxx> Commitment*	*(6) Reasonable Data Use & Sharing Behavior*	If the information use & sharing is comparable to the industry norm.	Observed UX	Analyst	Number of data processors in the service is within 10% of industry average.	-1 == # data processors in the service is >11% and < 35% of industry average; -2 == # data processors in the service is >36% and < 50% of industry average; -3 == # data processors in service is > 51% of industry average.
ATTRIBUTE 7: DATA PROCESSING MATCHES DATA SUBJECT'S PREFERENCES & PERMISSIONS							
A7-1	*<xxx> Commitment*	*(7) Data Processing Matches data subject's Preferences & Permissions*	If the observed *data collection* matches the data subject's permissions and preferences.	Observed UX; Pre-Certification Questionnaire	UX expert	If the UX offers permission options in the <xxx> Commitment, changes pertaining to data collection are accurately reflected as soon as the data subject makes any changes.	For multiple options in the commitment: -3 == none of the options change the service's behavior in the expected way, -2 == 50% of the options change the service's behavior in the expected way, -1 == 20% of the options change the service's behavior in the expected way.
A7-2	*<xxx> Commitment*	*(7) Data Processing Matches data subject's Preferences & Permissions*	If the observed data controller *data use and sharing* matches the data subject's permissions and preferences.	Observed UX; Observed local & network raw data; Pre-Certification Questionnaire	UX expert; Data supply expert	If the UX offers permission options in the <xxx> Commitment, changes pertaining to data controller data use and sharing are accurately reflected as soon as the data subject makes any changes.	For multiple options in the commitment: -3 == none of the options change the data controller's behavior in the expected way, -2 == 50% of the options change the data controller's behavior in the expected way, -1 == 20% of the options change the data controller's behavior in the expected way.
A7-3	*<xxx> Commitment*	*(7) Data Processing Matches data subject's Preferences & Permissions*	If the observed data processor and co-data controller data use and sharing matches the data subject's permissions and preferences.	Observed local & network data	Data supply expert	If the UX offers permission options in the <xxx> Commitment, changes pertaining to data processor & co-controller data use and sharing are accurately reflected as soon as the data subject makes any changes.	For multiple options in the commitment: -3 == none of the options change the data processors'/co-controllers' behavior in the expected way, -2 == 50% of the options change the data processors'/co-controllers'behavior in the expected way, -1 == 20% of the options change the data processors'/co-controllers'behavior in the expected way.
ATTRIBUTE 8: DATA PROCESSING MATCHES POLICIES							
A8-1	*<xxx> Commitment*	*(8) Data Processing Matches Policies*	That the observed data collection matches what's described in the Privacy Policy as collected in the Policy Raw Data	Observed UX; Policy Raw Data	Analyst	Observed behavior mostly matches privacy policy.	-3 == Observed data collection behavior mostly doesn't match the privacy policy in substantial ways. -2 == Observed data collection behavior has one or more serious mismatch with the privacy policy. -1 == Observed data collection behavior has one or more less serious mismatches with the privacy policy.
A8-2	*<xxx> Commitment*	*(8) Data Processing Matches Policies*	That the observed data collection matches what's described in the Terms of Service as collected in the Policy Raw Data	Observed UX; Policy Raw Data	Analyst	Observed behavior mostly matches the Terms of Service.	-3 == Observed data collection behavior mostly doesn't match the terms of service in substantial ways. -2 == Observed data collection behavior has one or more serious mismatch with the terms of service. -1 == Observed data collection behavior has one or more less serious mismatches with the terms of service.
A8-3	*<xxx> Commitment*	*(8) Data Processing Matches Policies*	That the observed data use behavior of the data controller matches what's described in the Privacy Policy as collected in the Policy Raw Data	Observed UX; Policy Raw Data	Analyst	Observed behavior mostly matches privacy policy.	-3 == Observed data controller data use behavior mostly doesn't match the privacy policy in substantial ways -2 == Observed data controller data use behavior has one or more serious mismatch with the privacy policy. -1 == Observed data controller data use behavior has one or more less serious mismatches with the privacy policy.
A8-4	*<xxx> Commitment*	*(8) Data Processing Matches Policies*	That the observed data use behavior of the data controller matches what's described in the Terms of Service as collected in the Policy Raw Data	Observed UX; Policy Raw Data	Analyst	Observed behavior mostly matches Terms of Service.	-3 == Observed data controller data use behavior mostly doesn't match the terms of service in substantial ways -2 == Observed data controller data use behavior has one or more serious mismatch with the terms of service. -1 == Observed data controller data use behavior has one or more less serious mismatches with the terms of service.
A8-5	*<xxx> Commitment*	*(8) Data Processing Matches Policies*	That the observed data sharing behavior of the data controller matches what's described in the Privacy Policy as collected in the Policy Raw Data	Observed UX; Policy Raw Data	Analyst	Observed data controller data sharing behavior mostly matches privacy policy; and no data processors or co-data controllers are observed that AREN'T included in the privacy policy.	-3 == Observed data controller data sharing behavior mostly doesn't match the privacy policy in substantial ways, and shares data with data processors or co-data controllers who aren't included in the privacy policy. -2 == Observed data controller data sharing behavior has one or more serious mismatch with the privacy policy. -1 == Observed data controller data sharing behavior has one or more less serious mismatches with the privacy policy.
A8-6	*<xxx> Commitment*	*(8) Data Processing Matches Policies*	That the observed data sharing behavior of the data controller matches what's described in the Terms of Service as collected in the Policy Raw Data	Observed UX; Policy Raw Data	Analyst	Observed data controller data sharing behavior mostly matches terms of service; and no data processors or co-data controllers are observed that AREN'T included in the terms of service.	-3 == Observed data controller data sharing behavior mostly doesn't match the terms of service in substantial ways, and shares data with data processors or co-data controllers who aren't included in the terms of service. -2 == Observed data controller data sharing behavior has one or more serious mismatch with the terms of service. -1 == Observed data controller data sharing behavior has one or more less serious mismatches with the terms of service.

ATTRIBUTE 9: REASONABLE COMMITMENT DURATION							
A9-1	*<xxx> Commitment*	*(9) Reasonable Commitment Duration*	If the default commitment duration is reasonable & appropriate for the commitment and the type of service. For ongoing/long-lived commitments: The <xxx> Commitment is expected to end when either the data subject unenrolls from it, or the data controller discontinues the service (or ends the commitment per the Terms of Service).	Observed UX; Pre-Pre-Certification Questionnaire; Policy Raw Data	UX expert	The default commitment duration matches the Me2B approved duration for the commitment.	The default duration for the commitment exceeds the Me2B Approved duration for the commitment (-3): COMMITMENT <--> Me2B APPROVED 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
ATTRIBUTE 10: COMMITMENT TERMINATION & CHANGE BEHAVIOR							
A10-1	*<xxx> Commitment*	*(10A) Commitment Termination & Change Behavior - Easy to End/Change Commitment*	If it's easy to stop or change the commitment.	Observed UX	UX expert	Easy to stop or change <xxx> commitment.	-3 == No way to change/end <xxx> commitment; -2 == Difficult to find and change/end <xxx> commitment; -1 == Difficult to find OR change/end <xxx> commitment.
A10-2	*<xxx> Commitment*	*(10B) Commitment Termination & Change Behavior - Record*	If the data subject receives or has access to a record of requested changes.	Observed UX	UX expert	Data subject can view online or separately receives a confirmation of changes.	Data subject neither has a way to view online NOR receives a separate confirmation of changes. (-3)
A10-3	*<xxx> Commitment*	*(10C) Commitment Termination & Change Behavior - Data Removal*	If the data controller removes or changes commitment-related data upon request.	Observed raw data; Pre-Certification Questionnaire	Data supply expert	Data controller removes all data relating to the commitment.	Data controller retains personally identified information relating to the <xxx> commitment. (-3)
A10-4	*<xxx> Commitment*	*(10D) Commitment Termination & Change Behavior - Permissions Flow to data processors*	If all co-data controllers and data processors receive notification and change/delete data upon commitment end/change.	Observed raw data; Pre-Certification Questionnaire	Data supply expert	All co-data controllers and data processors receive notification and delete data upon commitent end/change.	Co-data controllers and data processors do not receive notification of commitment change/termination and do not delete data. (-3) Co-data controllers and data processors do receive notification but don't delete data on commitment termination. (-3)

LOCATION COMMITMENT

TEST #	Me2B COMMITMENT	RESPECTFUL COMMITMENT ATTRIBUTE	WHAT'S BEING MEASURED	DATA USED TO MEASURE	EXPERTISE NEEDED TO EVALUATE	PASSING BEHAVIORS (SCORE = 0)	FAILING BEHAVIORS (SCORES -1 to -3)
LC1	*Location Commitment - Browser Level*	*All*	If the website uses browser level location tracking & consent	Observed UX	UX Expert	No use of browser level location tracking & consent.	Use of browser level tracking & location consent. (-3)
LC2	*Location Commitment - data controller Level*	*(5) Private by Default*	If the site automatically determines location without data subject permission.	Observed UX	UX Expert	Site does not automatically calculate location, and asks for consent to use location information.	Site automatically calculates location without asking for permission (-3).

ME2B MARRIAGE

TEST #	Me2B COMMITMENT	WHAT'S BEING MEASURED	DATA USED TO MEASURE	EXPERTISE NEEDED TO EVALUATE	PASSING BEHAVIORS (SCORE = 0)	FAILING BEHAVIORS (SCORES -1 to -3)
SCENARIO: ACCOUNT CREATION						
MM1	*Me2B Marriage*	Plain text fields in password /pin creation	Observed UX	UX Expert	Not collected as plain text.	Collected as plain text (-3).
MM2	*Me2B Marriage*	Plain text fields in password security questions	Observed UX	UX Expert	Not collected as plain text.	Collected as plain text (-3).
SCENARIO: USER LOGGED IN - "REMEMBER ME" OPTION						
MM3	*Me2B Marriage*	"Remember Me" option presented to data subject.	Observed UX	UX Expert	Option only presented for high-frequency interaction relationships, and only for low-risk transactions.	Option presented for low-frequency interaction relationships, and for high-risk transactions. (-3)
MM4	*Me2B Marriage*	"Remember Me" enabling.	Observed UX	UX Expert	Easy to understand exactly what gets remembered and for how long; shouldn't be too easy to turn on; Defaults to disabled.	Defaults to enabled. (-3) Harmful patterns manipulating data subject to turn on Remember Me. (-2)
MM5	*Me2B Marriage*	"Remember Me" disabling.	Observed UX	UX Expert	Easy to find and disable "Remember Me"	-3 == No way to disable Remember Me, -2 == Hard to find and disable Remember Me, -1 == Hard to find or disable Remember Me.
SCENARIO: USER HAS ACCOUNT BUT NOT LOGGED IN, N						
MM6	*Me2B Marriage*	Validates that no personal information is displayed when not logged in and "not remembered"	Observed UX	UX Expert	Website behaves exactly as in the "Local Storage consent" state, before an account was created.	Website continues to remember, recognize and personally respond to data subject (-3).
SCENARIO: USER HAS ACCOUNT, IS LOGGED IN & REMEA						
MM7	*Me2B Marriage*	If too sensitive information is displayed/exposed when "remembered".	Observed UX	UX Expert	Website doesn't allow for extremely sensitive personal information to be displayed or exposed on the device.	Website displays extremely sensitive personal infromation on the device without being logged in. (-3)