Movement for an Open Web - Comments on the IAB Draft MSPA

This document sets out comments on the IAB draft MSPA on behalf of the Movement for an Open Web. It builds on our earlier comments for the Global Privacy Platform consultation.

Executive Summary

- **Agreement with aims of MSPA:** The MSPA has an important role to play in facilitating compliance with a variety of state laws, especially as these proliferate. MOW agrees with the aspects of the MSPA that simplify compliance with what is required on a jurisdiction-by-jurisdiction basis.

- **Concerns about overbroad limitations:** Concerns arise that the "National Approach" effectively requires all of the strictest rules to be combined. This risks effectively displacing the decision of all those states not choosing to regulate, which is also a valid choice and ought to be respected. Essentially, these jurisdictions have chosen to prioritise free content and business liberties relating to data processing on the basis that evidence of harm from personalisation of advertising is not strong and that free content may be more important than certain consumer opt ins and opt outs.

- **Evidence-based approach to application of regulation:** This decision not to regulate ought not to be overridden by an industry standard. The easiest way to account for this would be to use the national approach on an opt in basis and only in those cases where there is reasonable evidence of residency in some regulated states. Otherwise, there is a risk that an important use case will not be addressed: unregulated use of responsible low-risk data in the vast majority of states where that is still the law. Instead, the strictest law of any jurisdiction becomes the "longest pole in the tent" and businesses in all *other* states effectively have to apply it.

- **First- and third-party issues:** There are also some concerns about the definitional language relating to first and third parties and relating to purpose and use limitation. Particular concerns arise relating to the Schedule B "Additional Obligations" handling time and type limitations which would all apply to the residual "National Approach" despite there being no clear legal basis for this requirement.

- **Possible anti-competitive effects from data use limitations:** To the extent that IAB sets standards for sometimes very large parties, there is need for caution as to possible anti-competitive effects from de facto limitations on data use. These can easily be avoided through some small, suggested tweaks to the operation of the concept so that they do not mandate potential limitations to innovation and competition.

Concerns about the scope and content of the national approach

If applied, the MSPA effectively requires either (i) state-by-state compliance for the listed regulating states or (ii) the National Approach to be applied, even where not mandatory. This is because, where triggered, there is no third category of non-regulated use.

The definition of a covered transaction in 1.2 means that vendors can opt in to the application of the framework, but where it applies, there is thus no concept of an *unregulated state* of low-risk

responsible addressable data. This is the vast majority of states, but instead the National Approach applies, because 3.1(b) says that if there is a reasonable basis for US residence, but no information on which US state applies, then the National Approach is to be applied.

It would therefore be helpful to clarify that this is not mandatory and that the MSPA can be applied on a voluntary basis alongside taking a state-by-state approach to *non-regulated* as well as regulated states. Accordingly, the following sections could be helpfully revisited to clarify that non-regulated use remains available, unless there is evidence of presence in a regulated state:

- "Covered transactions" in 1.2.
- The description of the National Approach in 1.38.
- Specific references to "exceeding" legal requirements (1.38(a)) and treating non-residents of states "as if" they were residents of all of them (1.38(d)) should be trimmed.
- 3.1(b) should be broadened to include non-regulating states in cases where there is no reasonable evidence that the user is in a regulated state.

Several restrictions on competition and innovation result from National Approach treatment, as outlined in 4.4. Personally Identifiable Information (PII) is also broadened to the "longest pole in the tent". This sits in tension with the spirit of 1.45, which seeks to apply the law to PII definitions, yet National Approach treatment will mean that the single strictest jurisdiction becomes the de facto national standard. This means that it does not apply the applicable law in many jurisdictions.

It is noted that 1.45 does this deliberately, and it is appreciated that this is not an oversight but a choice. MOW's comment is simply that this is an undue limitation where there is evidence that the user is not in a specific regulated jurisdiction.

There is reference in 4.5 to warranting compliance with valid signals of meaningfully informed user choice. It would be very helpful to retain responsible use of interoperable personal data, and data no longer linked to specific individuals, unless there is some evidence a user is present in a regulated jurisdiction. This would be a more tailored approach and would still enable compliance with all state laws.

State laws not always followed exactly

MOW is concerned that the "OOPS" signal is effectively made mandatory for Californian cases, substituting out the plain reading of the law which states that alternative means of compliance are acceptable. Indeed other states currently also allow websites to provide their own choice mechanism as a valid alternative mechanism for providing users opt-out preferences. Moreover, adopting the current language would undermine IAB's written positions in favor of protecting websites' rights over interests of internet gatekeepers stated policies.

MOW preserves its position as to other state law points.

Party definitions

MOW notes that the concern in the summary box about first party data use being "too narrow insofar as it excludes the use of an advertiser's first-party data to target ads" is a significant concern about potentially lost innovation, undue limits to use cases, and harm to consumer welfare in cases where data use is innocuous and risks are low. There is no reason, in such cases, to restrict *either* first or third party data use, unless mandated by law. We note that state laws provide for "businesses" to be parties that are not brand or media owners to responsibly collect and process data, especially if appropriate privacy-by-design measures are in place.

Further limitations can be seen in the definitions, which would benefit from revisiting, especially 1.29 which defines "first party" with reference to "intentional interaction" on Signatory digital property.

- It is not clear that intentional interaction is the right standard. This is because intention does not align with consumer expectations. Consumers do not have decision making authority over the supply chain partners of the properties they visit, especially when such use relies not on user's declared data, but derivative data that often is no longer associated with a specific individual.. An intentional interaction standard does not map to risk, which is the true concern. The focus should thus be the risk of consumer harm – if present on evidence – and not the somewhat artificial concept of intention on visiting a website. This risk depends on *what* data is being collected and processed, rather than *whether* the organization processing data is a brand or media owner.

- Nor do Signatories' digital properties map to consumer expectations. By this standard, patterns of ownership would determine data use, rather than risk.

- This is not the law in many jurisdictions, and the position sits in tension with the correct application of law to the definition of Third Party in 1.61.

- First Party, to the extent relevant, should also be defined with reference to applicable law. If these definitions are lacking, then a reasonable risk-based approach should be taken, rather than an intentional interaction standard.

Vendor as business requirements

Vendors should not be relegated to having to be service providers. Vendors can be businesses under many state laws without being service providers. Therefore the draft misses the category where vendors are simply businesses that are not (also) providing business-to-consumer digital content or services.

This is an arbitrary requirement that harms smaller vendors and responsible data interoperation required for competitive digital markets. It also sits in tension with the application of law to the questions (e.g., the definition of third party in 1.62 as set by law) because this goes beyond the legal position.

PII and De-identification

There is a helpful reference to the use of law to define PII in 1.45, and we support the comment in the table that the intention behind now-deleted 4.6 so as to clarify that if PII is not involved, then the obligations do not bite. We also support the confirmation in the final table box to the effect that non-PII use is not caught.

However, this point is of wider importance. If the law is not clearly capturing something, as with the case of data not linked to identity by the organization possessing it, then obligations should not apply. Thus applying the same thought as that behind the deletion of 4.6, so as to safeguard cases of no PII from regulation, then logically unregulated use in those jurisdictions not regulating should also be exempt from obligations.

There are also cases where some data is used, but has undergone appropriate privacy-by-design measures to dissociate identity from the input data, such as through de-identification and aggregation. We note that merely temporarily storing data so de-linked is not sufficient to meet the definition of "de-identification," but also requires promises to keep the data in such a state with appropriate organizational measures and via contracts with external recipients.

As the legislatures have clearly articulated with this exemption, many De-identified data handling use cases can prove helpful in low-risk cases and does not present a clear case for regulation, as risks are then low. It may be helpful to re-emphasize the bright-line distinction between PII-based and non-identity-inked data from a risk point of view, especially in relation to the National Approach. If the National Approach applies, then it would be helpful expressly to calibrate it for risk to the extent that it may exceed the legal requirements in a non-regulating state.

There is also concern that a first hop fallacy is applied in 4.4 Comment A10 referring to inventory without personal data. Personal data would always be involved at the first point of collection, if present. The question is whether, from a risk point of view, PII risks are adequately addressed by a system. 4.4 Comment A10 seems to contemplate a total absence of PII as the only safe approach, but there is scope to use PII responsibly (e.g., identifiers) where the use case is low risk.

Overdefinition of some concepts

We support the tabular comment that "first party" and "downstream participants" are not defined terms in state law. Where they do not apply, the National Approach should not require them.

An example can also be seen in 1.62 which defines a use case (segment creation). There may be other uses, including future undefined uses, and it is unclear why use cases need to be restricted with definitions instead of simply allowing the market to operate, and for risk of harm (if any) to be addressed by regulation if it arises. For example, "businesses" should not be limited to "first parties" as defined by MSPA.

Towards this end it would be useful to generate a standard contract that could be used by businesses to facilitate compliance with state laws when relying on privacy-by-design interoperable data, rather than assuming all supply chain partners (implicitly referred to as "vendors" in MSPA) must be "service providers."

Purpose limitations

There are many purpose limitations under the national approach, e.g. 5.2 and 7.3(v). In some instances, these refer to proposed rules which are not yet law, and which may not become law. Thus, the terms expressly exceed the legal requirements. It would be preferable to simply refer out to legal requirements than to laws which have yet to pass, as this would encompass future laws.

7.3(c) refers to a "necessary and proportionate" approach reading on initial information collection consent. This rules out an important use case, which is where low-risk data use cases where data has been appropriately transformed from being linked to identity to provide useful insight even where such business processing, which would be too granular for consumers to understand (e.g., multi-touch attribution) or does not require consent (e.g., fraud detection) at the data collection point. As data repositories are often collected over time, this is a helpful use case as it avoids arbitrarily having to revisit the data collection procedure. So long as the data use is innocuous (e.g., weather-based adverts; restaurant reviews that do not rely on identity-linked information and have other appropriate privacy-by-design measures in place) it is unclear why re-permissioning is merited. Therefore, the "necessary and proportionate" test should depend on risk, rather than scope of permissions.

The Schedule B (ex G) "Additional Obligations" also include time and type limitations, which can amount to further unnecessarily limitations on time and type limitations in the National Approach, where risks are low. Regarding the tabular comments, MOW disagrees with the limitation of duration to campaigns and notes that some important use cases may have longer duration. The key here is the risk, and not the duration of data handling per se.

MOW supports the tabular comments about the importance of combining data sources, especially for smaller businesses.

Use of contractual compliance

MOW strongly welcomes the use of contractual compliance frameworks in 8.3 to ensure that a range of compliant vendors can be used for business purposes. However, the point can be expanded. There is scope to use contractual compliance more broadly in low risk cases. If a decision is taken to allow more use where it is known that the data comes from a non-regulating state, then it would be important to revisit the 8.3 definition to comport with this and to prevent there being undue limitation on the use of subcontracting in low risk use cases. It may also be the case that, even where engaged, the 8.3 language requires more Signal tracking than is required in low risk contexts. A helpful way to implement this would be to define audit rights with reference to risk-based audit parameters.

Potential forcing of National Approach

If the MSPA comes to be widely adopted, as is highly likely, then there are concerns that the deadline on full MSPA compliance in 14.6 raises a concern. As the document contemplates only (i) regulating state compliance or (ii) the National Approach, Covered Transactions must

implicitly be handled within those two categories. It does remain open to vendors not to elect to place a transaction within “Covered Transactions,” but practically, a great deal of data will pass via MSPA if successful, and individual vendors may not have a practical choice about this. This would then mean that the National Approach becomes a de facto standard, limiting competition in those instances where it is not required by state law.

For this reason, it would be helpful to clarify that MSPA does not intend to force adoption of the National Approach, but only to provide it as a framework on a purely voluntary basis with no opt in deadline. This avoids bundling of the entire MSPA menu and ensures that competition and innovation can take place around it, where helpful, without losing the benefit of the standardized approach of MSPA where desired by particular vendors.
