Global Privacy Platform ("GPP") Proposal of June 2022
Comments from the Movement for an Open Web

15 August 2022

Introduction

This document provides comments from the Movement for an Open Web ("MOW") on the Global Privacy Platform Draft in Request for Public Comment of June 2022 ("GPP" and "the proposal" respectively). MOW represents a broad cross-section of analytics companies, digital advertising providers, publishers, and broadcasters. MOW advocates for an open web in which organisations may continue to choose which partners they exchange legally compliant data with to operate and grow their business, allowing greater competition and innovation to the benefit of both small businesses and society. More information can be found at MOW's website: https://movementforanopenweb.com/

"Privacy by Design" has been accepted as a foundational principle by most democratic jurisdictions for many years. The fact that there have been differences of view on how that could be implemented does not invalidate the widespread acceptance of that principle. Pseudonymised and innocuous data can be used without breaching privacy laws. The data economy in which we live depends on it. Nor has Privacy by Design been rejected in favour of a user "Click Box" consent model of privacy protection in any jurisdiction. Indeed, the EU GDPR promotes both a Privacy by Design approach that can be adopted for innocuous and pseudonymised data alongside ***meaningful consent*** for Personal Data. This is needed to ensure that consumers exercise meaningful choice over sensitive personal data, which they cannot do under circumstances where they are coerced or faced with ***no meaningful choice*** by monopoly suppliers. Consumer consent through Click Box systems would be tend to favour the major worldwide and monopolistic platforms. This does nothing to protect end user privacy. It would undermine the competitive position and ability of those businesses who rely on only using innocuous data or pseudonymised data and a Privacy by Design approach. GPP may risk favouring Click Box Compliance over Privacy by Design unless there is more emphasis on the latter. This may limit the scope for legally compliant systems to be put in place and distorts competition in favour of the major platforms. These concerns are explored in more detail below.

Executive Summary

MOW appreciates that the IAB's proposal seeks to promote responsible data handling by creating mechanisms for transmitting necessary signals required for compliance with data protection law on a regional basis. However, MOW is concerned that the proposal as currently drafted may inadvertently give rise to issues that ought to be mitigated prior to proceeding to implementation. The concerns are:

I. **Applying unwritten norms for convergence, rather than engaging with diverse approaches to data protection in different jurisdictions.** The proposal seems to assume convergence in data protection norms, without citing supporting evidence to this effect. From MOW's perspective, there is current and anticipated future divergence in privacy norms, reflecting different jurisdictions' regulatory decisions. This creates risks of impeding even lawful data flows if the system obligates the transmission of unnecessary inputs into organisations' compliance processes or begins imposing interpretations of unclear regulations in ways that would negatively impact competitive market outcomes.

II. **Rethinking the unilateral user data control assumption, especially where this risks unintended harms to helpful B2B data flows.** The current draft states that users should have "transparency and control" over data as a general matter. MOW notes that consumer-friendly systems do not require control over all data, and that control over data can sometimes even harm consumers if taken beyond what consumers would reasonably want. If the data use is innocuous and follows privacy-by-design safeguards, as with mainstream commercial advertising, it seems unlikely that users want even more control over business decisions and it may even harm the consumer through increased costs, decreased ad-funded content, and poor user interfaces (e.g., excessive prompts). It is very unlikely that users would want to control the B2B advertising decisions made by publishers or marketers any more than they would want to control decisions relating to other complex products (e.g., auto supply chains or airline maintenance). The consumer interest seems to be in free content provided that advertising systems to fund it are responsible and do not harm them. This does not always depend on consent. Assuming control over all data fails to ask *what data* and *what is done with the data*, which seem to be the consumer-relevant questions. And these questions are best answered by data protection regulation, so that a targeted approach to proven consumer harm can be taken into account.

There is also a risk of inadvertently creating gatekeeper situations that impede lawful and pro-consumer data handling and undermine the interoperation of systems and the choice of vendors. Interfering with transfers of innocuous data by suggesting consumers should control the B2B decisions of the web properties they visit would fragment digital markets, benefiting walled gardens that do not rely on such partners and hence do not need separate consent for each B2B advertising process they operate inside their property.

III. **Competition risks.** As the GPP system would be deployed on a large scale by a range of vendors, this creates a risk of anti-competitive outcomes because, in effect, a very large data handling system could lock out new innovations offered by smaller start ups by creating additional complexity and cost beyond what is legally required for compliance. It is also unclear how competing alternatives could be combined with GPP (e.g., use of a rival compliance program in country X, but IAB's system in country Y). If the GPP is meant to be extensible and facilitate interoperation of required signals, it should not exclude such use cases.

IV. **Omission of privacy-by-design safeguards.** It is unclear whether the proposals apply, common privacy-by-design safeguards such as pseudonymisation and data minimisation. While the US and EEA may diverge on organisations' obligations (e.g., EEA opt-in regime under ePrivacy, but opt-out regime under CCPA) in relation to privacy norms, these disparate data protection regulations do harmonise their definitions on appropriate safeguards that factor into the likelihood and severity of risks to specific individuals when processing personal data. Where such safeguards are fully deployed, they remove the material risks identified by such regulations, including the risk of re-identification or use of special category sensitive information without prior informed, explicit consent. Given the current specification does not contain any signals associated with whether the recipient is prohibited from or intends to reidentify a specific individual, nor whether the data transmitted belongs to sensitive special category, it is unclear how the metadata described will help more organisations more easily comply with their regional data protection obligations.

V. **A need to focus on reducing the signals sent rather than increasing them.** The specification suggests businesses will reduce their cost of operations and compliance by adopting this framework. It would be helpful therefore to focus on sending fewer signals to justify the integration cost on all businesses. However, the current draft sends more signals by merely wrapping other frameworks rather working to harmonise and reduce the shared data they each contain.

VI. **Insufficient attention to commercial implications.** There are concerns that existing data handling systems would need an extensive redesign, despite no immediate benefits to justify the expense required to undertake this work. It is unclear why this extensive redesign is net beneficial, and it would be helpful to have analysis of the costs and benefits of the standardisation framework.

The report does not consider commercial implications beyond its tagline that the proposal "can adapt to… commercial market demands across channels." There is scope to consider incentives that would arise from a data handling system that could be abused by activists or internet gatekeepers in a pursuit to further fragment data-driven solutions markets.

While the report is correct to note that jurisdiction is a country-by-country matter, there is a risk of a spillover effect from the strictest rules if large data set handling is impeded. There are also possible risks from the existence of a global data handling layer if ever this came to be regarded as regulated in toto by one of the constituent elements to it (e.g., if GDPR were applied to the entire system on the basis that some GDPR-regulated information flows through the system).

This could affect the adoption of paywalls, or alternatively free riding on ad-funded markets because websites may not be able to alter their business models to align with the different jurisdictions (e.g., if unwilling to create multiple commercial presentations of a newspaper by jurisdiction). If the GPP layer were regarded as a regulated entity, e.g., under GDPR, then the websites using it would effectively have to comply with it and the benefits of divergence would be lost. So, there is also a need to ensure that those jurisdictions choosing *not* to regulate data as strictly – which is also a valid policy choice – are not inadvertently subject to "friendly fire" from an outsized effect from those jurisdictions choosing more regulation (a spillover sometimes called "the Brussels effect").

I. Applying unwritten norms for convergence, rather than engaging with diverse approaches to data protection in different jurisdictions

There is no single approach to "privacy" worldwide. Some jurisdictions have chosen, deliberately, *not* to regulate some data flows, or not to regulate them as strictly, because of a greater emphasis on the ability to handle data, and the pro-consumer innovations this can bring. Any global system would need to take care to preserve this diversity, and to avoid inadvertently applying rules that are stricter than a jurisdiction has chosen.

Differences are subtle but significant. A prominent example is the different treatment of pseudonymisation and re-identification risks under the GDPR and the CCPA. Whereas the GDPR takes a precautionary approach, providing jurisdiction to regulate even *potential* re-identification under the definition of Personal Data in Art 4(2), the CCPA takes a risk-based approach under which data is not regulated provided that reasonable *risk-based* safeguards are in place under the definition of exemptions in 1798.145. This reflects different underlying regulatory philosophies: in the predominantly civil law (also called code law) of the European Union, the focus is on empowering the state to monitor business on behalf of society; whereas in the predominantly common law United States, there is more emphasis on business liberty, provided that the business is taking reasonable care in context.

Examples of divergence on the data control assumption

CCPA

CCPA is a significant case in terms of different approaches to privacy: taking reasonable care is enough to discharge the duty on the business, thus being at liberty to handle the data provided that safeguards are used. Whereas in the EU there is always residual jurisdiction over "legitimacy" of data handling under Art 6(1)(f) GDPR, resulting in debates such as whether and when pseudonymised data remain regulated. These debates do not have clear answers, and compared with CCPA, the GDPR approach is more cautious. For a global system, it is necessary to respect and apply these differences, and it would be wrong to assume "more control" instead, which effectively assumes that one side of this debate is the correct one. Assuming "more control" on these facts would effectively apply GDPR and its assumption of control over data by the end user even to places which have chosen not to take that approach.

No general regulation of data handling in the USA

It remains the case that, for now, the US does not have a federal equivalent to GDPR, and this decision *not* to require user "control" should also not be assumed away. Proposals such as the Gillibrand and Klobuchar bills would apply different approaches than GDPR and do not necessarily mandate "control". For example, the Gillibrand bill regulates high risk activities but leaves processing liberty unless there is evidence of high risk, and the Klobuchar bill emphasises transparency (such as disclosures), and frames its opt out right so that a service provider can still condition access to a system on the provision of data if the system is otherwise "inoperable". This is not the same thing as necessarily giving end users "control" in all cases and chooses to prioritise the ability to run a data-driven business model over "control" in cases where this is necessary for "operability." It would not be the same thing as "control" in all cases and deliberately does not align to GDPR in this regard, reflecting emphasis on different prioritisation of consumer interests.

Examples of divergence on the data control assumption (continued)

UK rethink on GDPR after Brexit

Another significant example, also spanning the same philosophical divide, can be seen in UK proposals to alter the UK implementation of GDPR following independence from the European Union. It remains to be seen what form this would take, but the UK Government's consultation on the changes speaks to easier data handling for innocuous use and moves towards the risk-based approach seen under laws such as CCPA.

This builds on the Joint Statement by the UK Competition and Markets Authority and Information Commissioner's Office's (ICO) May 2021 Joint Statement, and the November 2021 ICO AdTech Opinion, which emphasise risk-based approaches rather than relying solely on control by the data subject.

This would move away from the EU's hazard-based approach to privacy regulation. This is a particularly striking example, as it shows that the democratic process sometimes moves towards *less*, rather than more, control over data flows.

It seems unlikely that deep differences reflecting such "norms" and the role of regulation would proceed towards inevitable convergence as asserted in the proposal. Indeed, it may be a feature rather than a bug that different societies and different regulatory systems can take different approaches to risk. This is seen in many areas of regulation and is an important aspect of legal and regulatory diversity. The existence of differences can support competition between regulatory systems, which can be pro-consumer by preventing regulation beyond what the consumer demands or needs.

GPP may have an important role to play in capturing these differences and giving them effect. If so, then the starting position in the proposal that the IAB framework (p.1) that "privacy and data protection norms [will] converge" seems to be wide of the mark. MOW agrees that data protection and privacy might logically coalesce, but application of rules to identical data inputs will mean different things in different jurisdictions, just as laws on all sorts of risks differ based on their societal context. Thus, the following sentence that "users, in countries previously uncovered by powerful digital advertising transparency and control tools, can see into and have a say over data uses for digital advertising" seems, with respect, to be fundamentally misplaced.

II. Rethinking the data control assumption, especially where this risks unintended harms to helpful B2B data flows.

With respect, MOW would observe that not all countries require the assumption that individuals ought to control business processing decisions, on purpose. Moreover, the recent criticisms of the Belgian Data Protection Authority suggest that presenting too much granularity in information or choices to individuals is overwhelming and hence cannot meet GDRP Article 7 requirements of presenting choices in simple, plain language to ensure users can be properly informed ahead of making their consumer decisions. It may be that the consumer does not always want such levels of control, as with innocuous commercial data uses. Some jurisdictions may validly choose to prioritise other elements of consumer demand,

such as free content, over increasing granular controls of data flows provided that appropriate safeguards are in place.

What does the consumer want?

There are concerns about GPP inadvertently second-guessing policy decisions by assuming that the consumer interest is always in "transparency and control." There are some very significant areas where this *is* certainly true: special category sensitive data calls for transparent handling and user control. But much internet advertising is not this sensitive and is most often completely innocuous. Knowing that a pseudonymised "User123" searched for a flight and might want travel insurance arguably does not call for "transparency and control" as there is no harm to the consumer. There is also a consumer upside associated with ad-funded content. The latest public estimates suggest that tailored advertising is worth at least 70% more to media owners and content producers, and for some uses such as specialist websites and back catalogue articles tailored advertising may be worth multiples of contextual approaches.[1] Inadvertent reductions in the interoperability of innocuous data would thus have not only disproportionate negative impacts on such smaller organisations, but also cause indirect harm to consumers by reducing the funding available to such niche properties that often tailor to minority interests.

It is a valid policy decision to omit user control for innocuous data handling, and to allow the market instead to provide ad-funded content without burdensome data regulation where there is no proof of harm. In the case of innocuous data deployed for innocuous uses, there is no harm, and the case for control is accordingly weak.[2]

The question of *when* control is merited does remain. Regulation often seeks to maximise consumer welfare,[3] and proxies for consumer welfare might be useful guides as to the correct level of "control." However, information on consumer demand as to data control is unclear. The noted "privacy paradox" observes that users express a demand for more privacy but continue to use online services which collect even higher risk personal data.[4] This is widely debated. It may reflect a lack of knowledge about systems. It is, however, also consistent with not suffering loss from the use of such systems[5] and expressing a strong privacy preference only because of framing effects in surveys: few would say that they would like "less privacy", and surveys do not ask about trade-offs where privacy-by-design safeguards are in place. As the UK Government has noted, there is very little data on what consumers want in terms of *specific* trade-offs between pseudonymised data handling and access to free content.[6] It may

---

[1] See UK CMA, "Mobile Ecosystems Market Study Interim Report," p.249 (reporting 71% reduction in CPM on Safari following the introduction of Apple's ITP data restrictions).

[2] Combinations of data might conceivably lead to harm, but this would be a case for regulating those data uses, and not the innocuous data use. There is logically always a category of innocuous data + innocuous use which should benefit from a safe harbour.

[3] See e.g., Cowen and Crampton (eds), *Market Failure or Success* (Elgar, 2002); Kahn, *The Economics of Regulation* (MIT Press, 1988).

[4] See e.g. Akman, "A Web of Paradoxes" 16 (2) *Virginia Law and Business Review* 217 (2022) on the complex and debatable pattern of consumer engagement with online platforms.

[5] A notable UK Supreme Court case, *Lloyd v Google LLC* [2021] UKSC 50, rejected a claim based on cookie placement on the basis that no loss had taken plaec. This is consistent with other analysis in common law jurisdictions requiring consumers to show loss from data handling before a claim is due. See the U.S. Supreme Court decisions in Spokeo, Inc. v. Robins, 578 U.S. 330 (2016) and TransUnion LLC v. Ramirez, 594 U.S. (2021).

[6] In its influential report on online markets, the UK CMA specifically notes a gap in the literature: "Few surveys examine what UK consumers perceive the specific benefits or harms of data processing and targeted advertising to be. Instead, consumer surveys tend to focus on the high-level benefits and harms resulting from all forms of online targeting." (CMA (2020) Appendix L: para 285. *Summary of research on consumers' attitudes and behaviour*).

well be that consumers *do not* want "more control" if this means less free content, provided that data handling safeguards are in place. This would suggest that control is not the correct starting point for analysis, and that the proposal is not correct in assuming that more data control spreading around the world over time is the aim of the system. This could, in fact, be quite harmful to consumers if the costs outweigh the benefits, or if clunky user interfaces are required to capture consent beyond what is necessary for consumer protection.

As to the more sensitive data uses, the balance between risk and regulation is appropriately set on a jurisdiction-by-jurisdiction basis and it a matter for compliance by vendors in each jurisdiction. It is also doubtful that consent or control alone is the answer to consumer protection in relation to complex systems because complex systems, like other complex products, are unlikely to be understood by consumers. What is needed is protection from proven harm where this intervention is net beneficial, and not an arbitrary assumption that control is the way forward. Therefore, it seems doubtful, and possibly harmful, to assume that there is a starting assumption of greater user control in a widely deployed data handling system to be applied across multiple jurisdictions.

Simplifying user to business signaling?

In principle, GPP could help with the simplification of metadata regarding the combination of certain data sets by allowing them to be combined to the extent legally permissible. However, this is a different aim from greater "control" over business decisions and should be expressed as such.

If this is the aim, then there should be more attention to how metadata associated with data transfers could be combined, rather than on compliance on a jurisdiction-by-jurisdiction basis since the latter is, in any event, possible without the additional GPP layer.

What would be useful is harmonising the signals to be sent, rather than sending more signals. It is not clear from the current specification that appending more metadata to existing signal frameworks accomplishes an immediately beneficial result. For example, if EEA and US both require the same signal, surely harmonising that into a consistent taxonomy and framework would be a much easier step than merely inserting an additional "wrapper" around existing frameworks' signals. This would also do more to allow interoperation of data sets, which seems to be the major advantage to the existence of a system like GPP. It would be helpful to understand more about how the system would result in cost savings and efficiencies of the types mentioned, which is not clear to MOW when compared with the current situation of simply deploying the existing toolkits.

III. Competition risks

MOW agrees that there are benefits to standardisation. However, standardisation does not necessitate centralised decision making, but instead greater interoperability. As currently drafted there seems to be a competition law risk in bundling in the IAB frameworks to GPP, and not providing access to competing alternatives signaling frameworks (e.g., AdChoices). It would be helpful to explore how other frameworks might be used within the Region IDs list. The proposal seems to assume that only IAB systems will be included, which is in tension with increasing emphasis on interoperation of responsible data sharing systems in several jurisdictions.[7]

[7] See e.g. the EU's Digital Markets Act; the UK proposals for a Digital Markets Unit; and the American Innovation and Choice Online Act, all of which seek to promote lawful and responsible interoperation of data systems.

Indeed, if the market share of IAB's proposed system is large, as seems likely, then existing competition law may well already require reasonable approaches to interconnecting different data handling systems,[8] but this is not substantively addressed in the current proposal.

IV. Omission of privacy-by-design safeguards

The proposal does not currently engage directly with the concept of unregulated, or lightly regulated, legal data use. Yet this exists where appropriate privacy-by-design safeguards are used. This is a significant oversight, because it results in the proposal assuming that "disclosures and control" are the right focus (e.g., p.4) in all cases. There are many cases where disclosures are not required, especially where risk is low or zero and privacy by design safeguards are used (e.g., pseudonymisation). For example, the UK DCMS and other regulators are interested in methods that would automate the signaling from users to businesses, rather than providing intrusive consent notices on each domain they interact with. While we realise the user experience may be beyond the GPP specification on encoding and transmitting such user-initiated signals, it seems prudent to ensure the specification does not inadvertently overstep by causing additional user prompts and extra data flows that are unnecessary for the digital advertising use cases in scope.

For example, where data use is innocuous (e.g., User123 searched for travel -- > travel insurance ad shown), GDPR does not require disclosing the list of intended recipients, but only the "categories of recipients" (which is more likely to meet Article 7 simple, concise plain language requirements).[9] Yet under the current specification, the intended recipients and other data are envisaged for encoding, which could add unnecessary complexity and cost to the detriment of the IAB's goal of facilitating digital transactions among players of all sizes. The same can be seen in p.3, with its assumption that control flows into the data repository. This may be true for some types of data, but control flowing into a pseudonymised data system seems neither necessary nor desirable and may come at significant cost to business and consumers, especially if the result is foregone valuable data handling.

A simpler approach might simply be for the data handler to verify legal compliance, as they do with other laws throughout their business. A "lawful data" flag could be applied. This would then mean that fraudulent certification would be a breach of contract and potentially subject to criminal penalties for fraud or misleading and deceptive conduct. If concerns about consumer harm were to arise, then the regulator could investigate and more easily intervene where there is unlawful processing, since the erroneous certification greatly expands the scope for action against a bad actor. The burden on lawful businesses abiding by the rules would be commensurately reduced.

At a more fundamental level, it is unclear how getting lawful businesses to state which exact processing pathway is being used in all instances of data handling in the data system itself aids enforcement, since a bad actor could always lie. Thus, if the system only increases costs and complexity on lawful actors, but does not help improve the detection of bad actors, this would not achieve the goals of this specification to improve the overall efficiency of responsible data handling among multiple parties involved in digital advertising transactions.

---

[8] Dominance duties re interconnection

[9] GDPR, Art. 13 (Information to be provided where personal data are collected from the data subject), Art. 14 (Information to be provided where personal data have not been obtained from the data subject) and Art. 15 (Right of access by the data subject). Indeed Art. 30 (Records of processing activities) ONLY requires "the **categories of recipients** to whom the personal data have been or will be disclosed including recipients in third countries or international organisations." (*emphasis added*)

V. Focus on reducing the signals sent rather than increasing them

The specification suggests businesses will reduce their cost of operations and compliance by adopting this framework. Indeed, if the framework focused on sending fewer signals this might be true. However, the current draft sends more signals by wrapping other frameworks rather working to harmonise and reduce the shared data they each contain.

Data minimisation concerns

It is not clear that the current proposals minimise data handling, which raises concerns to the extent that this is required in some jurisdictions. This can be seen in the recent blog post:

Global Privacy Platform: Explained – IAB Tech Lab

Example of TCF privacy string today:
CPXxRfAPXxRfAAfKABENB-CgAAAAAAAAAAYgAAAAAAAA

Example of USPrivacy string today:
1YNN

Example of GPP string that integrates TCF and USPrivacy strings:
DBABjw~1YNN~CPXxRfAPXxRfAAfKABENB-CgAAAAAAAAAAYgAAAAAAAA

It is concerning that the "new" string merely concatenates existing strings and adds more metadata. It might be more helpful to reduce the information sent as inputs to downstream recipients' own compliance programs.

There also appears to be a new set of signals such as "acknowledge" that seems like requiring notice with a soft opt-in or lack of ability to opt-out. Signal integrity is tracked, but this is not always necessary, as with innocuous data use.

There may be a need to revisit data minimisation principles in the specification of the GPP strings.

VI. Commercial implications

The need for cost benefit analysis

There are concerns that existing data handling systems would need an extensive redesign, despite no immediate benefits to justify the expense required to undertake this work. It is unclear why this extensive redesign is net beneficial, and it would be helpful to have analysis of the costs and benefits of the standardisation framework. This would be normal for many other standards and would help put to rest concerns that expensive redesigns, and increased complexity, will bring benefits to users rather than impeding them.

How would new systems be introduced?

There is a risk that this could effectively bake in the current generation of data handling frameworks, because they will all be present in GPP, and websites may struggle to differentiate on the basis of the different amounts of data permitted by the different systems. This could stymie helpful competition between paywalls and data-driven ad-funded models and mask the true consumer cost of restricting data flows under some regulatory frameworks.

The design and spirit of GPP seems minded to improve efficiency of legal data flows in its twin desire to lower compliance costs, but there is a risk of requiring more data in situations where it is not warranted would achieve the opposite result.

Suggestions for focus

Narrow the scope to legal compliance.
The scope of the work does not focus on compliance with law, but instead extends this to unstated "norms."
We have seen in the W3C and other trade bodies where internet gatekeepers often play a controlling role by

1. Sending more employees (see Don Marti, Adexchanger (July 8, 2022) https://www.adexchanger.com/the-sell-sider/googles-topics-api-picks-on-smaller-publishers: "Niche or independent publishers don't have the time or specific expertise to participate in web standards development like the big platforms do, so their priorities can often end up lost in the process."),
2. Subsidising special working groups focused on issues they prefer (e.g., Meta and Tech Lab PET Working group focused on IPA),
3. Using board influence to ensure standards favor their business (e.g., IAB TCF 2.0 was in large result due to Google's pressure, even though the ecosystem had agreed on TCF 1.0 - https://www.adexchanger.com/online-advertising/how-we-got-here-a-look-back-at-the-privacy-changes-that-reshaped-google/ "The IAB Europe released the Transparency and Consent Framework (TCF) last year as an industry solution for conveying consent signals across the digital supply chain. But the programmatic industry didn't have the one member it needed. Google was expected to integrate with the TCF by the end of the summer of 2018, but reset the timeline to 2019 and then to 2020…..Also, the TCF needed Google more than Google needed the TCF, since Google already serves the most publisher ads in Europe, and could still process consent for its consolidated ad tech stack.")

Accordingly, we need standards work to focus on the laws generated from more democratic processes than "norms" promoted by internet gatekeepers.

Focus on reducing the signals sent rather than increasing them
The specification suggests businesses will reduce their cost of operations and compliance by adopting this framework. Indeed, if the framework focused on sending fewer signals this might be true. However, the current draft sends more signals by wrapping other frameworks rather working to harmonise and reduce the shared data they each contain.

Incorporate open source and decentralised solutions over centralised registries
The current draft suggests that a Global Vendor List must be maintained by the IAB, which at least in Europe charges fees to be listed. However, this is not needed as each vendor operates a website and could host its identity key (such as public key) on a designated, well-known path (similar to ads.txt). While IAB could crawl such pages and charge an access fee to read the database, by decentralising the solution it lowers costs for businesses rather than increasing them.

Do not set user expectations that they will or should control businesses' B2B advertising decisions
The IAB sets display advertising standards to facilitate the programmatic digital ad market. Marketers pay media owners to display the advertising message to the marketers' desired audience. This content is thus "pushed" to the user, unlike search where users "pull" advertising related to their search query. Marketers rely on supply chain partners to facilitate their media buys across the diverse publisher landscape, helping to subsidise the diversity of content across the open web.

The document would be improved by signaling **what** data is being processed and **whether** the individual has consented to B2C choices (e.g., standard ad funded access, personalised ad funded access) and categories of B2B vendors that web properties will work with rather than suggesting individuals should select individual B2B vendors that web properties can work with. This simplification might also better address the concerns Belgium has raised with TCF, but we limit this feedback solely to GPP that ought to work towards meeting consumer expectations by phrasing choices in simple, plain language around B2C choices rather than requiring more user information and choices over even more granular business decisions related to B2B advertising processing.

Data on consumer impacts and compliance costs
There is no data on how compliance costs would diminish, or how consumers would benefit from the addition of GPP compared with the existing approach of applying jurisdiction-by-jurisdiction data handling frameworks. There is no clear data on what consumers want, and the current proposal assumes that they always want control and disclosures, but consumers may not want lots of prompts and in the case of innocuous data may not want control at all.

It would also be helpful to understand more about how compliance costs would materially diminish, since there is a need to apply the law of all the GPP frameworks if applying all the Region IDs.

There is a need to identify foregone ("unseen") lost data handling in relation to the application of consent requirements beyond those required by law, which may harm large scale data handling under privacy-by-design safeguards.
