To the Australian Attorney-General's Office:

Our submission relates to the office's review of the Privacy Act.

The New York Times is committed to fostering better privacy standards in our digital ecosystem. With this in mind, we write to support this review. We believe that it is vital for governments to continue to improve laws in relatively quick iterations as our understanding of the internet and its multifarious impacts evolves. There is an inherent need to establish a better social understanding of privacy in the modern world. If done properly, it can help remove the burden from individuals and stop allowing businesses to create arbitrary privacy policies that suit their economic interests over the interests of the people interacting with them.

We are aligned with the Australian Competition and Consumer Commission's (ACCC's) Digital Platforms Inquiry (DPI) final report and agree with the majority of their recommendations on how to update the Privacy Act.

The objects of the Act, set out in Section 2A, are an adequate framework for investigating the questions of user privacy. At the same time, we agree with the DPI report's suggestion that framing user privacy as something which should be balanced against 'interests of the entities carrying out functions' can lead to an imbalance of power. We believe that the user is frequently unable to properly understand how business entities process their data, and would suggest that the objects be rephrased to ensure that entities are required to act in accordance with the user's expectations of how their data will be processed as opposed to in the interest of the entity itself.

As much as possible, we suggest grounding expectations of privacy in what they would be outside of the digital realm as that makes it easy for individuals to reason about the usage that may be made of their data. If visiting a site is akin to visiting a shop, then users can readily understand who may recognise them, what kind of information may be collected, with what retention period, to which third parties it may be shared, and so forth. The mapping is imperfect, but producing a well-documented digital equivalent to people's existing expectations of privacy in their physical interactions is a powerful tool with which to frame reasonable data processing and to obviate the need for much of "notice and choice." We have written about this approach in greater detail elsewhere.

We believe that technical information must be categorised as personal information when it is generated by a user's action, including inferred information. We are in agreement with the ACCC on Recommendation 16(a), and encourage specific language to be added to the Privacy Act. Aligning the definition of personal data with the GDPR will ensure consistent and thorough

protection for users as well as make it easier for businesses to comply with multiple international privacy laws.

We believe that journalistic exceptions should be continued under any revised version of the Privacy Act. Journalists should be empowered to make use of information that may be private so long as it is used with newsworthy goals. For example, The New York Times Opinion section's 'Privacy Project' would not have been able to publish a groundbreaking piece on the ability to re-identify and spy on individuals from log-level data that is publicly available for purchase without such an exception.

However, the commercial business that supports the journalistic mission should not be exempt from privacy regulations. Naturally, the reader expects different things from the journalistic product and the business entity, and we should honour reader expectations when defining journalistic exemptions.

Regarding consent, we believe that it is necessary in some cases but it should ideally be relied upon as rarely as possible. People have limited resources in time and energy to dedicate to understanding the specifics of a business's data processing. These resources should be treated with respect and called upon sparingly. We agree with the DPI report's findings that "click-wrap agreements with take-it-or-leave-it terms that bundle a wide range of consents … leverage digital platforms bargaining power and deepen information asymmetries, preventing consumers from providing meaningful consents to digital platforms' collection, use and disclosure of their user data." An approach such as the GDPR's that normalises consent as the first thing one does when visiting a site or app pays superficial lip service to transparency and agency while producing neither.

Our preference is instead to default to permissible data processing that matches pre-digital expectations of privacy as described above (limited collection, only by the first party and its processors with no further reuse, safe processing, limited retention, etc.) and to require consent to anything beyond that to be slow, difficult, specific, and temporary.

This set of permissible defaults, so long as it matches a reasonable digital mapping of user expectations, would effectively be pro-consumer — far more so than the status quo — while still enabling businesses to access enough data that they can reap the benefits specific to the digital era in terms of efficiencies and product development.

The relative merits of consent and reasonable defaults are particularly salient when it comes to children. Companies claim they act transparently by listing out all of their collection practices but they do so in a way that leaves parents unaware of the risks and consequences involved, and

parents rarely understand the potential risks of data processing to their children. Parents are made to grant consent to companies to collect their children's data without fully understanding who is seeing it, what they are doing with it, and the impact it could have on their children's lives.

Because children are vulnerable data subjects, it is important to remove the incentive for parents to give away their personal information; for children's data too, consent should not be the end-all-be-all but rather should be rare. If parents refrain from granting consent to the collection of their children's personal information, the child should not be excluded from accessing the site.

For children as for adults, rather than focusing on consent, the default should be safe as should be the maximum consentable option. While we believe this is true for all users, it is especially important for children.

We agree with recommendation 18 from the DPI report, and are heartened to know that the Australian Government is pursuing this question separate to the review.

We would like to thank the Attorney General's office for conducting this review, and will make ourselves available if there are any clarifying questions.

Contacts:

Rebecca Grossman-Cohen
Vice President, Audience and Platforms

Robin Berjon
Vice President, Data Governance

Shushana Jachobov
Vice President, Assistant General Counsel