



The Unanswered questions !

During Privacy week 2023 the Marketing Association hosted a panel discussion based on the theme ‘Balancing Privacy and Trust in Digital Marketing.’ The resulting discussion was so popular that it was impossible to answer all the questions online during the session.

We promised that we’d address all the unanswered questions and publish them. Panel members Mazen Kassis and Rali Andreeva have given their views with some comment from moderator Keith Norris.

If you missed the webinar, you can watch it in full on MA’s Resource Hub:

<https://marketing.org.nz/resource-hub/ma-privacy-week-webinar-2023>

- **How much does marketing need to contribute to helping draft the privacy policy of the company?**

Rali: The Privacy Statement is a customer facing document and Marketing should play a leading role in drafting the Privacy Statement. Working closely with the Legal team, the Marketing team should ensure that the privacy policy is written in simple and easy to understand language, it is presented in a way it is easy to read and to follow, use video, icons, even games if the target market is children .

Maz: I feel this should be addressed with the outcome in mind: how do we ensure that privacy policy works to engender trust amongst employees? In this light, whichever teams need to come together, should. Marketing is no exception.

- **Should the privacy officer and practices of a company be led by the marketing team?**

Maz: If privacy affected only the “customers”, which typically finds a home amongst Marketing teams in organisations, there may be a good argument for Marketing to play a lead role. However, privacy affects customers, employees, vendors, contractors, and other individuals equally – it doesn’t discriminate by job-type. Collaboration is likely required, with leadership ideally found in a dedicated privacy role (e.g., Chief Privacy Officer), depending on the size of the organisation.



Rali: Each organisation should decide what the appropriate governance is based on the maturity of the organisation and the business strategy.

The Marketing, Comms team should have a seat on the table. If appropriate the CMO should lead the privacy governance. Many organisations are changing the way they work and representatives of marketing, CX, digital or loyalty take a leading role in the privacy governance. When these teams get involved the conversation changes from meeting the legal requirements to building trust with customers and teams. I have seen first-hand how diversity of thinking makes a huge difference in the privacy practices and the organisation's culture.

- **How do you approach choosing digital tools when the legal terms are so difficult to understand?**

Maz: Some things to look for in the terms and conditions are that they reference the NZ Privacy Act and that the associated terms of service are clear and transparent. If the tools' terms are not easy to understand, it may be an indirect indication that privacy is not front of mind for the vendor. Vendors that take privacy seriously likely make this known in their marketing material, so consider using tools that tend to promote privacy in the tools design.

Rali: A good start is to work with the Legal teams and Technology partners to “demystify” the terms, establish principles and strategies. Unfortunately, some of the legal requirements can be interpreted differently which creates more complexity, for example when it comes to data retention the Privacy Act 2020 states that data need to be kept as long as required for the purpose collected. This is not very helpful when you need to decide what to do and what tools to use. In cases like this, you should work with the Legal, Data & Analytics, Tech partners and Strategy teams and establish the principles your organisation should follow.

Also, it is important that the business teams have appropriate privacy training, focusing not only on the legal requirements but on the business and customer implications.



- **Have you decided to not use tools simply because it's too vague about how they work?**

Maz: Yes. The primary focus should be whether a tool is fit to address the business purpose for which it's being considered. Meeting this critical criterion, with a sufficient focus on privacy, would be something else to look for.

- With governments banning TikTok from devices should marketers be worried how using the channel might affect perceptions about their privacy reputation and brand?

Rali. Yes. Marketing team should be clear on the potential implications and be prepared to change their strategy.

Maz: Yes. People are becoming increasingly aware of their privacy rights and conscious of privacy issues related to the collection, storage, use and deletion of their personal information. In this context, it seems reasonable to assume that, if a brand is seen actively promoting or endorsing their products or services through a platform that is perceived as having privacy risks, it may lead to a loss of trust. Furthermore, it seems reasonable that this can have a negative impact on a brand's reputation and the trust that customers may have with it.

- Thought experiment? Have you used YouTube with and without its trackers on? There is a stark difference in its recommendations' relevancy. Whilst we should focus on privacy, perhaps we should also focus on it generating value to the customer and not used to simply sell? Thoughts?

Rali. The focus should always be on generating value to customers and giving customers opportunity to make choices and control their data. Most of the organisations curate personalised journeys for customers, very few organisations ask customers if they want to see the personalised journeys and show them the implications. Customers should get value even if the privacy preferences are not applied.

Maz. Same answer as previous question!



- **We feel Meta pixels are poorly understood by the public - how well are businesses managing the privacy implications of this? Implications of the Privacy Act?**

Moderator. Neither panellist answered this question. Maz suggested that many people do not even know what a Meta Pixel is! My view is that the questioner is absolutely correct in saying that the public have very little knowledge about such tools. Facebook (now Meta) have had so many changes in their privacy policies that I believe the public are totally confused. In the end that will lead to a lack of trust and a loss of revenue. I fear that too many marketers are more concerned about response rates and KPI's than they are about information transparency.

- **What does the panel think about the use of ReCaptcha? It's commonly used on NZ websites, but Google's privacy policy is vague on how it uses info collected...**

Maz: I'm attracted to open-source technologies in this space. For example, hcaptcha markets itself as a privacy centric tool.

Moderator. I've made my views on the transparency of both Google and Facebook and their various subsidiaries known publicly. I believe that at times they are disingenuous.

However, here's what Google says on its ReCaptcha website *'reCAPTCHA's risk-based bot algorithms apply continuous machine learning that factors in every customer and bot interaction to overcome the binary heuristic logic of traditional challenge-based bot detection technologies.'* As a reasonably articulate anglophile I have no idea what that means!! Hands up everyone who can interpret it for me!

Moderator. I think that covers all the questions which went unanswered in the online session. May I remind you that these answers reflect only the views of the panellists and not necessarily those of the Privacy Commission or the Marketing Association. Thank you to all those participants who fired-in questions.