L'ORÉAL

L'OREAL AUSTRALIA'S SUBMISSION TO THE DISCUSSION PAPER: STRENGTHENING AUSTRALIA'S CYBER SECURITY REGULATIONS AND INCENTIVES

The Hon. Karen Andrews, MP
Minister for Home Affairs
Department of Home Affairs
Australian Government

27 August 2021

L'Oréal Australia's Submission

1. Introduction

L'Oréal Australia Pty Ltd ("**L'Oréal**") welcomes the opportunity to provide a submission to the Department of Home Affairs discussion paper, *Strengthening Australia's cyber security regulations and incentives*. Robust and effective cyber security has never been more important and L'Oréal is pleased to have the opportunity to contribute to that outcome.

As a global leading consumer goods company and the largest beauty group in Australia, L'Oréal is a consumer focussed business that has rapidly adapted its business model to succeed in the digital age. L'Oréal seeks to be a "digital first" company, putting digital at the service of our consumers, which gives rise to a responsibility to help create a trustworthy online environment for our consumers. We believe cyber security is essential to business operation and risk management in order to protect our consumers, business partners and stakeholders.

We agree that cyber security is a shared responsibility between government, businesses and the community and appreciate that large enterprises, including L'Oréal, play a role in protecting Australia from privacy and online security threats. In addition, we welcome the government's acknowledgement that the protection and education of consumers regarding cyber security is essential. L'Oréal believes that robust cyber security is critical for economic prosperity and international competitiveness and that this will only become more important as Australia continues to embrace the fourth industrial (technology) revolution.

To maintain our consumer focus, we regularly talk to our consumers regarding their experiences with L'Oréal brands (currently 30 brands in the Australian market). Globally, we speak with over 100,000 consumers every year, 15,000 of whom are enrolled in programs in Australia. They welcome us into their homes and their online communities to understand their needs and views on a variety of topics, including data protection and security. These conversations have helped us understand the concerns of our consumers in relation to this critically important topic. We would be delighted to discuss how our consumer insights could assist the government in understanding the needs and expectations of this community.

While L'Oréal does not seek to address all of the questions posed in the discussion paper, we can offer some insights and recommendations related to those of the consultation's most significant proposals and points for health and beauty businesses.

We believe that these recommendations will better achieve the policy objectives of this consultation in a manner that strengthens the cyber security standards of all digitally enabled businesses and improves the cyber security awareness and protection of consumers. Importantly, we believe that appropriate incentives

L'Oréal Australia
564 St Kilda Road, Melbourne 3004
Tel. +61 (0)3 8680 0000

ABN 40 004 191 673
www.loreal.com/australia

L'ORÉAL

can also enable Australian business to invest in cyber security and associated technologies. This will allow cyber security to become more effectively embedded into Australian business and society.

2. Recommendations and insights

L'Oréal supports the government's aim of enabling Australia to be a leading digital economy by 2030 and agrees that effective cyber risk management by businesses, as well as increasing consumer education in the area of cyber security, are important drivers in uplifting the cyber security of the economy at scale.

Our concern is ensuring that any measures introduced can achieve the above aim without causing significant unintended negative consequences, in particular for Australian businesses that are already appropriately acting and investing in cyber security. Importantly, cyber-attacks have now become a matter of "when" not "if", notwithstanding adequate and reasonable cyber security practices. We believe that the policy responses to this threat should seek a "whole-of-society" response, including education, guidance, local skill development and appropriate incentives, rather than penalizing organisations that are themselves victims of crime.

Recommendations

We recommend that the government:

1. Carefully considers whether to introduce any additional compliance obligations into primary legislation relating to the duties or obligations of companies and their directors and officers in relation to cyber security, especially given the rapidly evolving nature of the threat.

2. Considers the introduction of safe harbour laws for directors and officers of companies where a ransomware attack create conflict between their duty to act in the best interests of shareholders and the company and potential illegality through the payment of ransoms.

3. Carefully assesses the potential negative consequences of any mandatory codes in terms of cost and effectiveness in achieving the consultation's aims, when suitable frameworks are already in existence and are adequate if implemented appropriately.

4. Ensures any consumer protection measures such as compulsory labelling are soundly demonstrated to achieve the aim of increasing cyber security protection for consumers in a manner that is balanced against the actual risk, cost and operational impact of managing and providing such labelling, as well as any potential negative consequences where a risk based approach is appropriately taken.

5. Investigates the opportunity for government policy and investment in educating and upskilling consumers regarding good cyber security practices.

6. Considers promotion and investment in the development of Australian cyber security capabilities, skills and careers to generate the critical workforce skills necessary to meet the threat in the future.

7. Investigates the use of additional policy levers to incentivise investment and innovation in cybersecurity by Australian companies.

We will discuss our recommendations in more detail below.

Recommendation 1

That the government carefully considers whether to introduce any additional compliance obligations into primary legislation relating to the duties or obligations of companies and their directors and officers in relation to cyber security, especially given the rapidly evolving nature of the threat.

L'Oréal Australia
564 St Kilda Road, Melbourne 3004
Tel. +61 (0)3 8680 0000

ABN 40 004 191 673
www.loreal.com/australia

Cyber security threats are constantly evolving. Threat actors continuously adapt, modify and hone their weapons to exploit weaknesses. In such a dynamic threat environment, obligations enshrined in legislation may not be flexible and adaptable enough to ensure businesses can respond appropriately and efficiently in real time where needed, or to keep pace with technological change over time.

Further, increased regulation would inflate costs for businesses and potentially stifle innovation without necessarily increasing cyber security. This is especially so for businesses that already have mature and effective cyber risk management processes in place to protect consumers. Utilising increased regulation across corporate Australia, rather than focusing on identifying and regulating companies that are not already taking appropriate steps to manage this risk, could increase compliance costs that may cause businesses to decide between funding those compliance activities versus investing and innovating in cyber security and associated technologies that would better protect, and thereby benefit, its consumers. We believe alternate options should be evaluated before enacting such legislation.

Recommendation 2

That the government considers the introduction of safe harbour laws for directors and officers of companies that are the victim of a ransomware or similar attack and decide not to pay any ransom, where the company has acted reasonably with regard to its cyber security position.

We believe that any measures taken by the government in relation to cyber security should consider the impact of penalizing companies that are themselves victims of a cyber-incident. Directors and officers are often placed in conflicting positions, whereby the crush of time pressure may push an interpretation of their duty to the company to force the payment of ransoms to avoid potentially disastrous consequences. We acknowledge that from a moral, ethical and long-term perspective, the right choice may be to refuse to pay the ransom to discourage further attacks. This can happen even to organisations that have carefully invested in and appropriately managed their cyber security postures.

By providing directors and officers with certainty that any decisions to refuse to pay a ransom will not result in personal liability, the government can help elevate the public policy imperative of not paying ransoms. This will remove the incentive for ransom attackers to continue operating by limiting the potential negative consequences for those companies that have behaved appropriately and yet were still the unfortunate victims of a criminal attack.

Recommendation 3

That the government carefully assesses the potential negative consequences of introducing mandatory codes to achieve the government's aims when suitable frameworks already exist, and if appropriately implemented, address the same concerns.

The consultation paper suggests that a mandatory standard could be onerous and expensive, and we agree with that finding. As cyber threats are constantly evolving, it is preferable that any regulatory framework is flexible and of a voluntary nature. Relevant cyber security frameworks already exist, such as CIS or NIST, and if implemented appropriately can provide for adequate, risk-based management of cyber security threats.

Mandatory codes or similar required standards could lead to unintentional consequences, such as restricting adaptability and reactivity in the face of new emerging threats by requiring companies to consistently refer back to ensure any actions, activities or decisions are compliant. This is especially unhelpful when a quick response is critical.

Mandatory codes or similar standards may also cause Australian cyber security practice to diverge from other countries – potentially resulting in Australia being seen as a difficult place to do business and affecting inward investment, and/or impacting the operations of large multinational corporations who seek to manage these risks in a uniform manner across multiple jurisdictions. Over time, to the extent that such codes may become

L'Oréal Australia
564 St Kilda Road, Melbourne 3004
Tel. +61 (0)3 8680 0000

ABN 40 004 191 673
www.loreal.com/australia

outdated, it could result in Australia being adversely affected in terms of the perception that data and information might be less secure if stored here.

If regulatory reform is required, targeted, specific regulatory guidance from appropriate sector regulators would be an appropriate mechanism (such as APRA's CPS234 for financial institutions). This approach would result in an updated regulatory framework that is adaptable and more flexible and thus better suited to manage and respond to emerging cyber threats as they are tailored to relevant actors.

Recommendation 4

That the government ensures any consumer protection measures such as compulsory labelling are soundly demonstrated to achieve the aim of increasing cyber security protection for consumers in a manner that is balanced against the actual risk, cost and operational impact of managing and providing such labelling, as well as any potential negative consequences where a risk based approach is appropriately taken.

The ongoing costs associated with a labelling proposal could see manufacturers reconsider supplying to the Australian market, especially with products that generate small margins that these requirements could render unprofitable. In this regard, we would welcome greater clarity on the scope of consumer-connected products to which such a requirement would apply.

Our experience is that consumer education is more important (see **Recommendation 5** below) as it enables consumers to understand the risks and choose more secure products regardless of labelling. Without this knowledge and understanding, any labelling will ultimately be irrelevant to consumers.

Recommendation 5

That the government investigates the opportunity for government policy and investment in educating and upskilling consumers with regards to good cyber security practices.

We believe that consumer education in the area of cyber security is critical. A coordinated Government-led education campaign to raise consumer awareness and increase the cyber literacy of all Australians would have the greatest impact in combatting this risk to consumers and directly addressing the issues of information asymmetry and a lack of competition between manufacturers based upon good cyber security practices. Without prioritising education, the government, companies and their information security teams will always be fighting an uphill battle.

Recommendation 6

That the government considers promotion of investment in the development of Australian cyber security capabilities, skills and careers to generate the critical workforce skills necessary to meet this threat in the future.

For Australia to succeed in its mission to improve cyber security, it needs investment in the creation of a highly skilled local workforce with capabilities in technical cyber security and cyber-risk management and governance. In light of the Covid-related impacts on the ability for international workers to access the Australian market, as well as the already highly competitive international market for employees with cyber security capabilities, without this focus on developing a locally-based workforce, Australian companies will struggle to achieve the necessary cyber security status in a timely and cost-effective manner.

By developing this workforce, Australia can avoid missing out on the investment and innovation opportunities to develop new cyber security products, technologies and services that it could export internationally for the benefit of the Australian economy.

Recommendation 7

That the government investigates the use of policy levers to incentivise investment and innovation in cyber security by Australian companies.

The discussion paper suggests that there are insufficient incentives for companies in Australia to adequately and appropriately invest in good cyber security and that this is the reason additional regulations are being considered. We believe that a more effective tool for solving this problem could be the use of tax policy to incentivise and reward investment and innovation in cyber security by Australian companies. Such an approach could be used in conjunction with voluntary cyber security codes or other guidance, to provide a balanced regulatory framework that is targeted to achieve uplift in this area. Whilst clearly a complicated solution that would require investment from the government and industry to identify the right areas for tax incentives to be applied, we believe that the nature and scale the problem and the need for a long-term solution justify this investment of time and effort.

Conclusion

L'Oréal remains committed to supporting the government's aims in improving cyber security across Australia and protecting Australian consumers. We believe our recommendations build on and improve the proposals raised in the discussion paper and will help deliver the outcomes sought by the Department and government.

We would welcome the opportunity to discuss our recommendations with you. Please let us know if you would like to do so.

Yours sincerely,

Jessica Amos
Legal Counsel – Privacy and Data Protection
L'Oréal Australia Pty Ltd