Google Australia Pty Ltd
[redacted]
Australia
google.com

25 October 2021

Director, Online Safety Reform and Research Section
Department of Infrastructure, Transport, Regional Development and Communications
[redacted]

BY EMAIL: OnlineSafety@infrastructure.gov.au

Google and YouTube welcome the opportunity to contribute to the Draft Online Safety (Basic Online Safety Expectations) Determination 2021 consultation.[1]

The draft Basic Online Safety Expectations Determination (the "draft Instrument")[2] addresses a number of issues that have widespread implications for how Australians use the Internet, and online service providers, and we welcome the clarification provided by the Draft Online Safety (Basic Online Safety Expectations) Determination 2021—consultation paper (the "Consultation Paper")[3] and the Frequently Asked Questions (the "FAQs").[4]

At Google, we build tools that are a force for creativity, learning, access to information, and much more. We believe that the Internet has had an immensely positive impact on society. Today, Australians use the Internet to learn, shop, work, and particularly during the pandemic, stay connected with friends and family. We recognise, however, that the Internet is exploited by bad actors, and it is imperative for everyone, including Google, to work together to better protect and empower people online.

To that end, we work to anticipate and respond to harmful content and behaviours online. We build transparent, fair, and effective processes to help address harmful content and behaviour,

[1] https://www.communications.gov.au/have-your-say/draft-online-safety-basic-online-safety-expectations-determination-2021-consultation.
[2] https://www.communications.gov.au/file/52396/download?token=g5mtd5WJ
[3] https://www.communications.gov.au/file/52336/download?token=S0nlJI7G
[4] https://www.infrastructure.gov.au/sites/default/files/documents/frequently-asked-questions--basic-online-safety-expectations.pdf

including to help ensure that content that violates the law or our terms of service is addressed as quickly as possible. We have made significant investments in technology and human resources, and we regularly engage with policymakers in Australia and around the world on appropriate steps to protect users of our services. In fact, the draft Instrument, in many respects, aligns with Google's existing efforts to minimise the availability and impact of illegal content on our services.

We acknowledge that many of the reasonable steps discussed in the draft Instrument provide helpful guidance to online service providers, codifying best practices for the core expectations specified in the Online Safety Act. Similarly, the "additional expectations" described in the draft Instrument are generally helpful. However, such additional expectations should avoid going beyond the scope of the Online Safety Act by addressing other topics such as encryption and identity verification. These issues, while important and worthy of consideration, should be addressed through separate mechanisms that are better suited to consider the broader impact they may have on the Internet ecosystem.

Our feedback in this submission focuses on selected portions of the Instrument where changes would strengthen and improve the framework. Specifically:

- The Instrument should encourage practical best efforts and sound processes to address the harms covered by the Online Safety Act, without being overly prescriptive.
- The Instrument is not the right forum to address issues relating to encryption, which should be considered in a separate, holistic context.
- Online Service Providers should not be expected to proactively monitor all user activity or content.
- Children's safety expectations should account for variations in age and maturity among children.
- The access of services in a signed out state, without providing additional identification data, is a valid route to interact with services. Identity verification should not be the only route to prevent abuse of services for users who choose not to provide additional identification information.
- The Commissioner's guidance should be transparent and, to the extent possible, publicly available.
- Industry cooperation, while helpful to protecting users in some contexts, should not require that online service providers share proprietary information, including intellectual property and trade secrets and should not require coordination on removals or make mandatory the sharing of Personal Identifiable Information or other data that would risk user privacy.
- Any framework should focus on clearly defined, unlawful content.
- Complaint resolution expectations should be flexible and clear and focus squarely on complaints that impact online safety, acknowledging the diverse relationships between online services and content creators.
- Online service providers should retain the flexibility to determine when to remind users of applicable terms and policies, especially when such terms and policies have not changed since the user last agreed to them.

We also want to highlight a key principle that, while not addressed directly in the draft Instrument, is important to the implementation of the Online Safety Act: any assessment or enforcement relating to the Online Safety Act should focus only on systematic failures. As the draft Instrument rightfully highlights, tools such as complaint mechanisms can be effective for identifying those harms. However, when considering new regulation or enforcement actions, it is important to focus not on isolated examples of harmful activity that may slip through despite good-faith efforts to protect users, but rather on supporting transparent, fair, and effective processes and systems that successfully sift through extraordinary volumes of user activity daily. While supporting good faith actors, enforcement should focus instead on bad actors (both corporate and individual) who continue seeking to engage in harmful activity online.

Google thanks the Department for its attention and welcomes the opportunity to work with the Department to address these important issues going forward.

Division 2—Expectations regarding safe use

Expectations—provider will take reasonable steps to ensure safe use

Online Service Providers Should Not Be Expected to Proactively Monitor All User Activity or Content

The draft Instrument states that a "provider of the service will take reasonable steps to proactively minimise the extent to which material or activity on the service is or may be unlawful or harmful."[5] We are supportive of online service providers voluntarily implementing robust systems to identify and address illegal or harmful content. We are concerned, however, about the implications of a broad legislated expectation to "proactively minimise" unlawful or harmful material or activity. Such a provision is likely to result in over-removals which will impact users' rights to provide and access information.

In particular, we caution against provisions that could force companies to over-rely on automated content moderation tools. While existing automated systems can be a vital tool for detecting and blocking content at scale, such systems often struggle with the application of nuanced, context-dependent definitions of illegal content, such as those in the online safety space. Similar difficulties extend, as well, to fully lawful content that is prohibited by content policies or Terms of Service, especially in cases that rely heavily on context to determine meaning and intent. Codifying an expectation that online service providers proactively minimise certain categories of content would likely lead to the blocking of large amounts of legitimate content and undermine Australians' access to valuable information.

[5] Draft Instrument Sec. 6(2).

We encourage the removal of "proactively" from the draft Instrument, to make clear that although online service providers should take reasonable steps to minimise unlawful or harmful material or activity, proactive measures such as automated detection and blocking systems should remain voluntary. An alternative approach would be to align the Instrument with the European Union's Digital Services Act ("DSA"). The DSA calls for annual risk assessments for significant systemic risks, including the dissemination of illegal content, followed by "reasonable, proportionate and effective mitigation measures….". Adopting a similar approach for Australia would further protect consumers online by enabling online service providers to engage in tailored, service-specific risk mitigation efforts.

Children's Safety Expectations Should Account For Variations in Age and Maturity Among Children

The draft Instrument recommends that, for services targeted or used by children, that "the default privacy and safety settings of the children's service are robust and set to the most restrictive level."[6] The draft Instrument could be more effective if it drew a distinction between services that are aimed at -- and marketed specifically -- to child users, as contrasted with those services which are useful to the general population (e.g. maps, online encyclopedias, etc.), but which may include users under 18.

We share the Government's objective to protect children from online harms. When designing our products and services, we consider the online harms children may face and have developed a number of special features to enhance the safety of children online. However, we are concerned that the reasonable steps to set privacy and safety settings to the *most restrictive* settings possible are both too blunt and inconsistent with the approach used in other markets.

There are circumstances where the most restrictive default settings are appropriate, and we have applied such settings in some of our own products - see our recent blog, explaining our approach to giving kids and teens safer experiences and the specific measures on YouTube. For example, when a user has signed-in as a minor, their uploaded videos in YouTube are set to the most restrictive privacy settings available by default and wider wellbeing features are enabled, such as autoplay off by default and bedtime and take a break reminders on by default.

And for Search, one of the protections we offer is SafeSearch, which helps filter out explicit results when enabled and is already on by default for all signed-in users under 13 who have accounts managed by Family Link. In the coming months, we'll turn SafeSearch on for existing users under 18 and make this the default setting for teens setting up new accounts. SafeSearch will also be on by default for users with Google Workspace for Education accounts.

Furthermore, Location History is already off by default for all accounts, and children with supervised accounts don't have the option of turning Location History on. Taking this a step further, we'll soon extend this to users under the age of 18 globally, meaning that Location History will remain off (without the option to turn it on). Lastly, with regard to Search, we have recently given minors more control over their digital footprint by introducing a policy that enables anyone under the age of 18, or their parent or guardian, to request the removal of their images from Google Image results.

[6] Draft Instrument Sec. 6(3)(b)

We also develop products specifically for kids and families, meeting parents' needs to enable their children to enjoy experiences online while helping their children to be safer. Examples include:

- Family Link: Family Link is a downloadable app, now available by default in the latest Android operating system and Chromebooks, that helps parents guide their child's experience as they explore online. The app lets parents set digital ground rules for their family, such as managing the apps their child can use, keeping an eye on screen time, or setting a bedtime and daily limits for their child's device. SafeSearch, a default Family Link supervision feature, helps filter out explicit search results like pornography on Google Search.
- YouTube Kids: YouTube Kids is an app that provides a separate YouTube experience designed especially for children that parents can customise. The app uses a mix of filters, user feedback, and content moderation to keep the videos in YouTube Kids age-appropriate, allowing children to explore a catalogue of content in a safer environment. YouTube Kids offers a set of parental controls to customise their child's experience. Parents can decide what content to make available for their child to watch, set a timer to control screen time, block videos or channels, and more.
- YouTube supervised experience: As of March 2021, parents using Family Link can also allow their child to access YouTube with a supervised account, with three content settings for parents to choose from. The YouTube supervised experience looks much like YouTube's flagship app and website, but with adjustments to the features children can use and ads protections. For example, comments and live chat are disabled, as well as the ability to upload content and make purchases. Additionally, automatic reminders will appear for breaks and bedtime, which they can adjust to reinforce healthy screen-time habits.

While these product specific measures are appropriate, a "one size fits all" approach, as proposed by the draft Instrument, is overly restrictive and will have unintended negative effects. For example, the proposed Instrument does not consider that children of different ages may require different settings. The draft Instrument would set an expectation that a 17 year old's default settings would be the same as those of a five year old -- the most restrictive, regardless of the product or the risk to the child. Default settings need to respond to the evolving capacity and developmental needs of children and the risks associated with the services. Settings should also consider other rights at stake, including children's rights to access information and freedom of expression.

It is also important to recognise the role that parents and caregivers have to play in supporting younger children as they discover and explore the online world. Tools like Family Link allow families to set the digital ground rules that are best for them, helping parents choose what is appropriate for their children.

The impact of a blunt restriction would likely be to limit access to significant amounts of age-appropriate information and experiences. Teenage users, for example, may find it difficult to research the topics they read about in school or content that allows them to explore their identity and their sexuality.

Expectations—provider will consult with Commissioner and refer to Commissioner's guidance in determining reasonable steps to ensure safe use

The Commissioner's Guidance Should Be Transparent and Publicly Available, Consistent with the Principles Laid Out in the FAQs

The core expectation to consult with the Commissioner[7] and refer to the Commissioner's guidance[8] is important because it requires that all online service providers consider the same factors when determining how to meet the Basic Online Safety Expectations. It is helpful to clarify that online service providers need not contact the Commissioner in each instance, but rather may look to any relevant guidance material that has been made available.[9] However, this is not supported by the current wording of the draft Instrument which suggests service providers must have regard to guidance material *in addition* to consulting the Commissioner.

The Commissioner's guidance should, wherever possible, be made public, as suggested by the FAQs. While it is important for online service providers to consult confidentiality in certain circumstances (e.g., regarding unreleased products), there should be a general presumption written into the Instrument that the Commissioner's position in evolving issues impacting online safety will be equally accessible to all stakeholders. Doing so will promote transparency and better protect Australians by helping to ensure that the Commissioner's guidance is applied consistently across services.

Additional expectation—provider will take reasonable steps regarding encrypted services

Access to Encrypted Communications Should Not Be Addressed via this Instrument

The Instrument includes an additional expectation that, if the service uses encryption, the providers "will take reasonable steps to develop and implement processes to detect and address material or activity on the service that is or may be unlawful or harmful."[10]

Encrypted communications are recognised by the UN as a fundamental component of free expression in the digital age,[11] and provide the highest level of security to users. According to cryptographers and security engineers, even well-intentioned efforts to provide a lawful intercept solution in E2EE undermines security benefits by making all users of such services more vulnerable to malicious attacks. That said, we are mindful of the risks that encrypted communications can be misused and abused by bad actors to facilitate the sharing of illegal content. We believe that there are appropriate tools to fight the spread of illegal content even in encrypted environments. Those tools include using behavioural information and metadata signals, which can be deployed to detect behaviours that may be putting children at risk, and we are committed to working constructively on innovation in this area. Whatever measures are undertaken, further research, refinement, and technological innovation is required in this space

[7] Draft Instrument Sec. 7(1).
[8] Draft Instrument Sec 7(2).
[9] Consultation Paper, p3
[10] Draft Instrument Sec. 8.
[11] UN (2015) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

in order to attain public safety benefits without engineering vulnerabilities into products and services in ways that weaken security for all users.

Should encryption nevertheless be addressed by the Instrument, we recommend a clear statement, consistent with the FAQs, that the expectations can be met using behavioural information and metadata, and explicitly stating that backdoors or other measures that would undermine the security of user data or user privacy are not expected or required.

Additional expectation—provider will take reasonable steps regarding anonymous accounts

Listing Identity Verification as One of Two "Reasonable Steps" To Address Repeated Abuses May Inhibit The Development of Alternative Mechanisms

The draft Instrument includes an expectation that services that "permit anonymous accounts will take reasonable steps to prevent those accounts being used to deal with material, or for activity, that is or may be unlawful or harmful"[12] and describes "having processes that require verification of identity or ownership of accounts" as one of two reasonable steps to address that expectation.[13] We acknowledge and appreciate the Government's clarification that this expectation is not intended to impose a verification requirement. Nevertheless, we recommend that the Instrument include additional, specific examples of reasonable steps that an online service provider may take, short of account termination, to meet this expectation.

Online service providers should take steps to limit accounts that engage in illegal activity or violate applicable Terms of Use regardless of whether an account is directly tied to an individual's identity. Rather than impose an additional expectation with respect to anonymous accounts, the Instrument should focus on measures that discourage abuse of all kinds, regardless of anonymity.

We are concerned that expressly including and highlighting identity verification as a reasonable step implies that identity verification can act as a safe harbour. Even after the Government signalled a more nuanced approach through the FAQs, we expect that many companies will offer users a choice between identity verification and account termination, rather than other reasonable steps that could address bad behaviour by anonymous accounts.

To encourage online service providers to advance users' legitimate interests in access to information while maintaining privacy and protecting against the real harms that can be caused by bad actors, we recommend exploring further what additional reasonable steps are feasible and can be implemented to make it more difficult for users who have previously been banned from an online service to regain access.

[12] Draft Instrument Sec. 9.
[13] Draft Instrument Sec. 9(2)(b).

Additional expectation—provider will consult and cooperate with other service providers to promote safe use

Industry Cooperation Expectations Should Account for Differences Across Services, IP, and Trade Secret Protections, as well as Data Privacy

The additional expectation to "take reasonable steps to consult and cooperate with providers of other services to promote the ability of end-users to use all of those services in a safe manner"[14] is helpful. Cooperation among online service providers can be a helpful tool to address harmful online activity and Google takes measures to cooperate today with other online service providers on a range of safety and security measures.

For example, we are an active member of several coalitions, such as the Technology Coalition, the ICT Coalition, the WeProtect Global Alliance, and INHOPE and the Fair Play Alliance, that bring companies and NGOs together to develop solutions that disrupt the exchange of CSAM online and prevent the sexual exploitation of children. Together we fund child safety research and share tools and knowledge, such as our insights into transparency reporting, in-product detection, and operational processes. We also use our technical expertise and innovation to detect child sexual abuse material and support others to do the same. We offer our cutting-edge technology free-of-charge for qualifying organisations to make their operations better, faster and safer, and encourage interested organisations to apply to use our child safety tools, like the Content Safety API, to help detect not previously seen CSAM, and the CSAI Match, hash matching technology to detect CSAM in video format.[15]

We also recognise the importance of taking a multi-stakeholder approach to tackling violent extremism and terrorism. We are proud to be part of the Christchurch Call Community and a founding member of the Global Internet Forum to Counter Terrorism. We are pleased to offer our support to building the Call community including expanding and diversifying its members and strengthening the critical role of civil society.

Safe Browsing, which helps protect more than four billion devices every day by showing warnings to users when they attempt to navigate to dangerous sites or download dangerous files. This service is not limited to Google products - we've made Safe Browsing services free and publicly available for developers and other companies to use in their applications and browsers via publicly documented APIs.

While this approach works well for Safe Browsing, it can be more difficult for content takedowns and account removals. For example, different platforms have different terms of service and community guidelines, such that activity that is inappropriate for one platform may be permitted by another. Requiring coordination could also lead to abuses where one platform could intentionally seek to pressure others to remove lawful content or account activity. Therefore, we recommend that the Instrument clarify that online services providers are not obligated to coordinate on these and similar activities.

[14] Draft Instrument Sec. 10(1).
[15] https://protectingchildren.google/

In addition, while information sharing can be an important tool, it is important that such sharing protects user privacy. For example, if a user is posting content on one online service, providing the user's IP address could improperly reveal the user's otherwise private identity or expose connections between the user and other individuals who use that IP address.

Finally, we note that our processes for identifying and responding to users that violate our terms of service or otherwise cause harm on our services reflect significant investment in intellectual property over many years. We also rely on trade secret protections to preserve the integrity of our methods, including spam filtering and fraud detection. These efforts are some of the many reasons that our users actively engage with our services every day, and we recommend that any expectations to cooperate not impinge upon providers' IP and trade secret investments.

While there are circumstances where it is appropriate to cooperate with other online service providers to promote safe use, the Instrument should explicitly note that cooperation is not required.

Division 3—Expectations regarding certain material and activity

Core expectation—provider will take reasonable steps to minimise provision of certain material

Core expectation—provider will take reasonable steps to prevent access by children to class 2 material

As mentioned above, online service providers should not be expected to proactively monitor user activity or content.

Any Framework Should Focus on Clearly Defined, Unlawful Content

Google agrees with the comment in the draft Consultation Paper that online service providers are "best placed to identify emerging forms of harmful end-user conduct or material and to react to them."[16] In fact, this principle should be applied broadly in the draft Instrument, providing online service providers with broad flexibility to react to the ever-changing Internet landscape, including by updating community guidelines, acceptable use policies, and terms of service to limit the availability of content that online service providers view as harmful to their communities.

Any framework should focus on unlawful content, such as child sexual abuse material and illegal terrorist content, with such content clearly defined to support consistent application across online services. "Other harmful material" referenced in the Consultation Paper,[17] and material or activity that is or may be unlawful or harmful[18] as used in the draft Instrument, should be precisely defined to focus on material that is illegal or otherwise subject to governmental regulation.

[16] Consultation Paper, Pg. 3
[17] Consultation Paper, Pg. 3.
[18] Draft Instrument Sec. 6(3)(a).

Similarly, with respect to reasonable steps to prevent access by children to Class 2 material (i.e. content classified as mature), we recommend that the Instrument account for both protecting children from online harms and preserving the right of children to access information and participate online. As we recently wrote to the Commissioner regarding an implementation roadmap for a mandatory age verification regime relating to online pornography, not all online spaces present the same level of risk of exposure to harmful materials. This is particularly true where platforms have policies and user settings in place to address and remove or restrict access to harmful content. Furthermore, not all online spaces have the same level of risk, in terms of access to information, when it comes to the removal or restriction of fully legal content.

The Instrument should not seek to set new rules for what lawful content should remain online and what platforms should remove. Service providers should have clear terms for harmful content, including how "harmful" is defined and determined. If the Government believes that a category of content is sufficiently harmful that it should not be available online, we believe it should make that content illegal directly, through transparent, democratic processes and not based on private entities' interpretation of the applicable framework. Absent clear, carefully considered expectations, the practical effect will effectively be that online service providers are encouraged to deny Australians access to valuable legitimate content out of an abundance of caution to avoid regulatory penalties.

As a general principle, we believe platforms that host content should be free to set their own guidelines on the legal content they will and won't host. Regulation should not seek to set the rules for what lawful content should remain online and what platforms should remove – what is legal offline should remain legal online. Platforms should have clear terms for harmful content, including how "harmful" is defined and determined. For example, YouTube's community guidelines prohibit content that threatens other individuals or that targets an individual with prolonged or malicious insults based on intrinsic attributes. And YouTube's community guidelines prohibit explicit content that is meant to be sexually gratifying or that endangers the emotional and physical well-being of minors.

We recognise the concerns that the Department has on specific categories of lawful content. We haven't waited for legislation; we have developed our own guidelines and taken action. We understand the sensitivity and importance of these areas and have devoted careful attention to developing an approach that limits harm while protecting users' ability to express themselves online.

We think that it is vital that the Instrument retains an approach that is based on encouraging platforms to clearly set out how they deal with harmful content, and that holds them accountable for delivering on their commitments.

Alternatively, If the Government determines that a category of content is sufficiently harmful, the government may, in a necessary and appropriate manner, make such content illegal through democratic processes.

Division 4—Expectations regarding reports and complaints

Online Service Providers Should Have Sufficient Flexibility to Address Complaints About Certain Material

We agree that complaints regarding the material laid out in the Online Safety Act should be addressed in an "accessible, fair, responsive and effective" manner, as described in the Consultation Paper[19] and outlined in the draft Instrument.[20] An accessible, fair, responsive and effective manner is a qualitative standard, and the Instrument should acknowledge that different types of complaints may merit different treatment.

For example, some complaints may require more careful review or vetting, which can take a longer period of time. We regularly receive complaints that may impact ongoing law enforcement investigations, and we closely scrutinise complaints that may implicate the rights and freedoms of individuals. And the relationship between online service providers and content creators will vary. For example, not all online service providers have a contractual relationship with content creators, which can make it more difficult to resolve complaints in certain cases.

Online service providers should also have sufficient flexibility to dismiss malicious or otherwise improper complaints. Complaint mechanisms can be a channel of abuse by bad actors, who can seek to suppress legitimate content and viewpoints or advocate for the suspension of accounts that have not violated an online service's terms of use, much less the law. Complaint mechanisms can also encourage unfounded or bad faith complaints. For example, bad actors will sometimes "brigade" together, submitting a high volume of unfounded or bad faith complaints, which can be quickly dismissed. While we understand the importance of handling complaints in a responsive manner, it is important that responsiveness not require a level of detail in response that would compromise the effectiveness of existing controls to fight bad actors.

In addition, as with tools to combat spam on the Internet, online service providers need flexibility to respond to unfounded complaints without harming the integrity of their services or disclosing information that could be used to circumvent existing controls. For example, in services for which we voluntarily offer users the ability to flag content, our experience is that the user-submitted flags are often inaccurate and can be used as a tool to harass and infringe on the expression of other users. The YouTube community guidelines flagging tool illustrates this risk. We receive hundreds of thousands of content flags on a daily basis. While many are good-faith attempts to flag problematic content, large numbers of them represent mere disagreement with views expressed in legitimate content or are inaccurate.

Given the high risk of inaccurate user flags, the Instrument should provide online service providers wide latitude to determine how to respond to complaints, including flexibility with respect to time. Any expectation that implies a limited time period to respond to complaints will likely have the effect of encouraging online service providers to take down content—even when such content is legal or the complaint is not meritorious—in order to meet the expectations.

[19] Consultation Paper, Pg. 3
[20] Draft Instrument Sec. 13.

The standards-based approach in the draft Instrument appears to provide the requisite level of flexibility. We encourage the Government to adopt the proposed language and confirm that rigid deadlines or specific procedures would undermine good-faith efforts by online services providers to tailor complaint mechanisms to the nature of the services they offer.

Division 5—Expectations regarding making certain information accessible

Online Service Providers Should Have Flexibility to Determine When to Remind Users of Applicable Terms and Policies

The draft Instrument calls for online service providers to "ensure that end-users receive regular reminders of, and updates in relation to material changes in" the terms of use, policies and procedures and standards of conduct, and information regarding online safety and parental control settings, including those published by the Commissioner.[21]

We offer numerous services throughout the world and have taken great care to ensure that our terms of service, procedures and standards, and settings are transparent and accessible to our users.

Just in time notice, commonly used with privacy policies, presents users with the relevant information when they are making the decision whether to proceed. Presenting information about what information will be shared, for example, when a user chooses to log in to a third party service with their Google Account, gives that user an opportunity to consider the implications of their choice at the moment in which they are asked to choose. We also provide annual reminders to users who have opted into Location History to make sure they are aware of that choice and have an opportunity to confirm their settings.

We recommend that the Government reconsider the additional expectation to provide "regular reminders of… the information specified in subsection 17(2), including through targeted in-service communications." Online services generally make their terms accessible to users at any time already and proactively notify users of any changes to the terms. Providing "regular reminders" can be helpful in some contexts. For example, Google's Privacy Checkup and Security Checkup help users confirm that their privacy and security choices are up to date. However, providing forced reminders of terms of service are likely to be less effective and could hinder user experience. Consider for example, a user who needs to quickly check their email prior to a meeting. She opens her email app, only to be greeted by a popup encouraging her to rereview the terms of service, which are unchanged. She would likely find the reminder annoying. More importantly, she would probably click through it quickly, so as to get to her emails.

Users who receive an undue number of prompts develop click fatigue. Rather than carefully consider dialogue boxes or warnings, they see these tools as barriers to be struck down by selecting "OK," "continue," or "I agree." This expectation would, if implemented, likely contribute to click fatigue and reduce the effectiveness of existing mechanisms to notify users of policies, terms and conditions, etc.

[21] Draft Instrument Sec. 18.

We also recommend that online service providers not be expected to provide updates regarding the Commissioner's publications. We recognise that the Commissioner has an important role to play in providing Australians with information about online safety, but do not believe that online service providers should be required or expected to amplify or publish those messages on behalf of the Commissioner.

Google thanks the Commissioner for the diligent effort to address this important topic and careful consideration of our contribution. We look forward to continuing working together and providing our perspective as the Basic Online Safety Expectations are finalised and are more than happy to address any questions the Commissioner may have or share our technical expertise.

Yours faithfully

Samantha Yorke
Government Affairs and Public Policy