Från: Eva Ljungbert
Skickat: den 1 februari 2022 09:36
Till: 'Maija Corinti Salvén' <mcorinti@apple.com>
Kopia: Berfin Eken <berfin.eken@regeringskansliet.se>; Marion Ghaffarnejad
<marion.ghaffarnejad@gov.se>; Håkan Hillefors <hakan.hillefors@regeringskansliet.se>
Ämne: Sv: Updated Material & Exchange of Views DMA

Dear Maija,

Thank you for your answer. Wednesday the 9th of February 10h-11h suits us well and the Webex platform should work for us. Thank you for the link.

We look forward to meet you next week.

Best regards,

Eva Ljungbert

Eva Ljungbert
Kansliråd
Näringsdepartementet
Enheten för marknad och konkurrens
103 33 Stockholm
Tel. 08-405 46 26
Mobil 070-486 50 46
eva.ljungbert@regeringskansliet.se
www.regeringen.se

Från: Maija Corinti Salvén <mcorinti@apple.com>
Skickat: den 31 januari 2022 15:48
Till: Eva Ljungbert <eva.ljungbert@regeringskansliet.se>
Kopia: Berfin Eken <berfin.eken@regeringskansliet.se>; Marion Ghaffarnejad
<marion.ghaffarnejad@gov.se>; Håkan Hillefors <hakan.hillefors@regeringskansliet.se>
Ämne: Re: Updated Material & Exchange of Views DMA

Thank you Eva!

I would then propose Wednesday 9 February 10h-11h.

If Webex works for you, then I directly enclose a link for this slot
https://appleinc.webex.com/appleinc/j.php?MTID=m9e2dd8ec5e19802e4fb5eab35cca51c2

Please feel free, of course, to propose an alternative platform.

Thank you also for the update on the DMA team on your side!

Maija

On 28. Jan 2022, at 16:21, Eva Ljungbert <eva.ljungbert@regeringskansliet.se> wrote:

Dear Maija,

Thank you for your e-mail and the enclosed paper and report.

We would be open to listen to your views regarding the proposals from EP that you mention below and others that is relevant for you. The ministry of Infrastructure and the Ministry for Foreign Affairs are also interested to participate in a meeting with you. For your information, Berfin Eken has replaced both Linn and Marcus as contact person regarding DMA from the Ministry of Infrastructure. We would like to suggest dates for a meeting at Tuesday the 8th of February before lunch or Wednesday, whole day. Would any of these times be suitable for you? Please let us know if they are or we will try to find another time.

I hope that you will have a nice weekend.

Best regards,

Eva Ljungbert

Eva Ljungbert
Deputy Director
Ministry of Enterprise and Innovation
Division for Market and Competition
103 33 Stockholm
Tel. + 46 8 405 46 26
Mobil + 46 70 486 50 46
eva.ljungbert@gov.se
www.government.se

<image001.png>

Från: Maija Corinti Salvén <mcorinti@apple.com>
Skickat: den 24 januari 2022 13:50
Till: Eva Ljungbert <eva.ljungbert@regeringskansliet.se>

Kopia: Linn Berggren <linn.berggren@regeringskansliet.se>; Marcus Boklund <marcus.boklund@regeringskansliet.se>
Ämne: Updated Material & Exchange of Views DMA

Dear Eva, I hope you had a good start into 2022!

The year starts by keeping us busy on the DMA, with the trilogue now on the agenda. Especially the European Parliament's latest extension of interoperability requirements in Art 6.1.f is concerning to us; and also the security concerns around side-loading remain.

My colleague Marc and I would be very happy to exchange views with you on these points, or any others that might be relevant to you. Please feel free to propose time slots for a call over the next weeks.

Please also allow me to send you some material - incl. summaries - which you may find insightful.
As this included an MSC paper, I wanted to ask whether you might be attending the Munich Security Conference event now in February? This could be an opportunity to catch up in person, if you were interested.

With kind regards,
Maija

 MAIJA CORINTI SALVÉN

HEAD OF GOVERNMENT AFFAIRS • NORDIC • BALTIC • SUISSE •
+49 (0)151 6186 9310 • maija@apple.com

Munich Security Conference Discussion Paper:

The MSC issued a paper on the need to cyber-security proofing EU digital legislation.
It explicitly mentions the DMA's sideloading has unintended consequences on security as it may "*open the door to malware and ransomware attacks at a time when malicious (state or non-state) actors, whether their goal is infiltrating governments for intelligence or businesses for financial gain, increasingly target individuals and their mobile devices*."

Oxera Report on DMA Amendments
https://ddei5-0-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fwww.oxera.com%2fwp%2dcontent%2fuploads%2f2022%2f01%2fOxera%2dReview%2dof%2dDMA%2damendments%2dFinal%2dreport%2d2022%2d01%2d10.pdf&umid=F5E43B16-D6E1-E005-827D-74BB364FC8DA&auth=b32f7072cb1370b7b119b85843019516260d8fac-a99a661dcbadfc40ad00effb411372c3cdfa1d92
This report, commissioned by the CCIA, includes a number of concrete examples, case studies and recommendations, e.g.

On Platform Governance:
- The emphasis should be on limiting user exposure to unsafe software and content, inline with the DSA's objectives.

- A sole focus on integrity and end-user's ability to protect themselves will lessen existing protections.
- 6.1.c will reduce the gatekeeper's ability to identify and manage security threats and may increase the chances of malware infection.

On Interoperability Requirements:
- The definition of interoperability proposed by Parliament risks forcing disproportionate levels of third party integration across the board, by precluding an API approach which is more suitable to 6.1.f requirements. Full interoperability of specific services might not be necessary, and instead may have an impact on communication services and end-to-end encryption in particular.
- Free of charge access to functionalities would lead to expropriation and reduce incentives to innovate.
- Compliance timelines are too short to deliver effective third party access requirements while minimising governance issues. Longer compliance timelines should be an option within the specification process and regulatory dialogue.

Nokia's 2021 Threat Intelligence Report

Nokia's yearly Threat Intelligence Report finds that Android was responsible for over 50% of malware infections in 2021.
In contrast, iOS's percentage was so small in 2021 that it was lumped into the category of "other".
Additionally, if you look at the top 10 of the 20 most common types of Android malware listed in the report you find that 5 of the top 10 were installed directly via sideloading.