

To: (10)(2e)] (10)(2e) @minvws.nl]
Cc: (10)(2e)] (10)(2e) @minvws.nl]
From: (10)(2e)
Sent: Thur 7/2/2020 7:30:39 AM
Subject: Re: Escalatieverzoek
Received: Thur 7/2/2020 7:30:58 AM

Niet of nauwelijks. Dat is het lullige....

On 2020-07-02 09:14, (10)(2e) wrote:
 > Dank! Een zelfde gesprek was er ook al bij de wetgeving. Maar: hoe
 > bruikbaar is de data überhaupt en zouden ze daar dan niet op een
 > andere manier al aan gekomen zijn?
 >
 > Gr
 >
 > (10)(2e)
 >
 > -----Oorspronkelijk bericht-----
 > Van: (10)(2e) <(10)(2e)> <(10)(2e)>
 > Verzonden: woensdag 1 juli 2020 22:24
 > Aan: (10)(2e) <(10)(2e)> @minvws.nl>
 > Onderwerp: Escalatieverzoek
 >
 > Hol (10)(2e)
 >
 > Zojuist heb ik onderstaand risico voor de DPIA opgetekend. Het gaat
 > erom dat in theorie politie/om of inlichtingendiensten bij de data van
 > de app kunnen komen. Los van het privacyrisico is dit een groot ding
 > in de perceptie die mensen hebben bij het gebruik. Dus al weken terug
 > heb ik gestuurd op het offlimit proberen te krijgen van deze data. Dat
 > zou veel critici de mond snoeren en een groot privacyrisico wegnemen.
 >
 > De AIVD ziet dat niet zomaar zitten 'want als er een aanslag kan
 > worden voorkomen'. Het OM gaf vandaag aan het ook niet te zien zitten,
 > want 'als je er een moord mee kunt oplossen'. Ik baal hiervan omdat ik
 > beide zaken bij succes van de app echt zwaar ondergeschikt vindt (op
 > een juist moment een dreigende uitbraak stoppen kan miljarden kosten
 > en tientallen levens redden).
 >
 > Ik kom dus niet verder. Mijn vraag: zou er een kans bestaan dat de
 > minister zijn collega's spreekt en bovenlangs probeert dit te regelen?
 > Of ben ik nu aan het dagdromen en moet ik het laten schieten? Ik vraag
 > het even direct langs iedereen heen om het niet een ding in het team
 > te laten worden. Als het wel kan, wat heb je dan van mij nodig of hoe
 > regel ik dat?
 >
 > Groet,
 >
 > (10)(2e)
 >
 >
 > 24. Toegang door OM/Politie of inlichtingendiensten
 > Fase: Validatiefase
 > Categorie: Gegevens
 > Incident: Via een vordering van het OM, een inbeslagname door de
 > politie of ingrijpen van een inlichtingendienst valt een mobiele
 > telefoon in handen van deze instanties. Zij kunnen in theorie bij de
 > TEKs komen als zij de beveiliging van Apple/Google doorbreken.
 > Impact: Hoog. Als de data wordt gebruikt om in te zetten tegen een
 > betrokkene dan kan dat verstekkende gevolgen hebben voor deze
 > persoon.
 > Kans: Laag. De kans dat de API van Google/Apple te kraken is en dat
 > een mobiele telefoon in handen van de partijen op een moment dat ze
 > relevante data bevat is klein door de 14-dagen retentieperiode. Het is
 > daarnaast een kleine kans, omdat de mobiele telefoon, de operator en
 > clouddienstverleners meer informatie bevatten die een dergelijk
 > onderzoek kunnen helpen.
 > Risico: Midden.

- > Maatregelen:
 - > • Sterke versleuteling om daarmee de kans op succes van het benaderen van de gegevens te verkleinen
 - > • Retentie. Door gegevens na twee weken weg te gooien is de kans op het bestaan van nuttige informatie fors verminderd
 - > • In het nationaal belang vragen om deze data off limits te verklaren voor informatie op de mobiele telefoon en de infrastructuur.
- > Dit ook om weerstand bij gebruik weg te nemen. Dit uit oogpunt dat het bestrijden van COVID-19 een groter belang is dan het belang van een individueel onderzoek en het ondermijnen van het vertrouwen van het systeem.
- > • Het uitvoeren van onderzoek op de cryptografie.
- > Beperking/Uitdaging: Zowel de inlichtingendiensten als het Parket
- > Generaal hebben aangegeven niet open staan voor het off limits verklaren van de app.
- > Impact na maatregelen: Laag. Bij het off-limits verklaren van deze data verdwijnt de impact.
- > Kans na maatregelen: Laag.
- > Risico na maatregelen: Laag-Laag
- >
- >
- > --
- >
- > (10)(2e)
- >