PRIVACY FIRST

Postbus 16799
1001 RG Amsterdam
Tel. 020 - 8100279

Aan:
Tweede Kamer der Staten-Generaal
Vaste commissie voor Veiligheid en Justitie
Per email: cie.vj@tweedekamer.nl

Uw ref.	:	
Onze ref.	:	SPF-20160210
Datum	:	10 februari 2016
Betreft	:	Inbreng Privacy First t.b.v. hoorzitting wetsvoorstel Computercriminaliteit III

Geachte leden van de Tweede Kamer,

Morgen vindt een hoorzitting plaats over het wetsvoorstel *Computercriminaliteit III*. Door dit wetsvoorstel dreigt de overheid zelf de grootste cybercrimineel te worden. Privacy First zet hieronder kort uiteen waarom.

Pacemakers hacken

Onder het wetsvoorstel krijgt de politie de bevoegdheid om vrijwel alle computers die op internet aangesloten zijn te kunnen hacken, inclusief smartphones, televisies, fototoestellen, autonavigatie, boordcomputers, medische systemen, etc. etc. De politie wil zelfs *pacemakers* kunnen hacken, zo blijkt uit p. 86 van de Memorie van Toelichting bij het wetsvoorstel. Geen enkel apparaat wordt uitgesloten. Enige voorwaarde lijkt slechts te zijn dat het betreffende apparaat in verbinding staat met het internet. Met het Internet of Things in zicht (waarbij vrijwel de hele maatschappij op internet aangesloten kan worden, tot en met sportschoenen en koelkasten aan toe) is deze bevoegdheid ronduit totalitair. Het zal dan ook slechts een kwestie van tijd zijn voordat de hackbevoegdheden in dit wetsvoorstel voor allerlei onvoorziene doelen worden gebruikt en misbruikt. Het huidige wetsvoorstel beperkt dit totaal niet en laat er juist alle ruimte toe. Reeds op basis hiervan dient het wetsvoorstel verworpen te worden.

Disaster by legal design

In politiekringen wordt de doelverschuiving (*function creep*) die in dit wetsvoorstel ingebakken zit juist beoogd, zo weet Privacy First uit betrouwbare bron. Bijvoorbeeld om auto's op afstand te kunnen hacken en stilzetten (politiefuik op afstand). Technisch is dit prima mogelijk te maken en het wetsvoorstel verbiedt dit ook niet. De risico's hiervan voor de verkeersveiligheid (met name ook van onschuldige

inzittenden en omstanders) zijn echter enorm. Hetzelfde geldt voor computers in ziekenhuizen, industrie, vitale infrastructuur, etc. Waarom legt het wetsvoorstel in dit opzicht geen enkele beperking op?

Noodzaak ontbreekt

De internationaalrechtelijk vereiste “maatschappelijke noodzaak” en proportionaliteit van dit wetsvoorstel zijn ver te zoeken, zo heeft zelfs het doorgaans coulante College Bescherming Persoonsgegevens (nu Autoriteit Persoonsgegevens) begin 2014 terecht gesteld. Vervolgens lag dit controversiële wetsvoorstel enkele jaren stil, maar lijkt nu alsnog opeens door de Tweede Kamer heen te worden gejaagd. Vanwaar opeens deze haast?

Iedere burger vogelvrij

Door dit wetsvoorstel lijkt ieders computer, tablet, smartphone etc. (zelfs in het buitenland!) vogelvrij te worden verklaard. De hackbevoegdheid in het wetsvoorstel beperkt zich immers niet tot de apparatuur van verdachten, maar ook tot daarmee in verbinding staande apparatuur van onschuldige, nietsvermoedende burgers. Iedere burger als potentieel *target* van de overheid. Hadden we de laatste jaren nu juist niet geleerd dat dit geen heilzame weg is voor een democratische rechtsstaat?

Kruispunt

Nederland staat momenteel op een kruispunt. Welk voorbeeld willen we voor de rest van de wereld zijn? Ons land heeft alle randvoorwaarden om van Nederland een veilig Privacy Gidsland te kunnen maken. Het huidige wetsvoorstel vormt echter een typische bouwsteen voor een politiestaat, niet voor een democratische, op vrijheid en vertrouwen gebaseerde rechtsstaat. Bij de internetconsultatie van een eerdere versie van dit wetsvoorstel in 2013 heeft Privacy First dit ook al gesteld. Afgezien van de latere schrapping van het decryptiebevel uit het wetsvoorstel is het treurig om te moeten constateren dat er sindsdien weinig is veranderd. Privacy First pleit voor *privacy by design*, niet alleen middels techniek, maar ook middels privacyvriendelijke wetgeving en beleid. Door dit wetsvoorstel raakt de overheid echter gebaat bij suboptimale, door de overheid te kraken ICT-beveiliging. Daarmee zet de overheid koers richting een maatschappij waarin ieders privacy illusoir wordt.

Privacy Impact Assessment ontbreekt

Nog steeds is er bij dit wetsvoorstel geen sprake van een grondige en onafhankelijke Privacy Impact Assessment (PIA). De bijbehorende “PIA” is niet meer dan een oppervlakkig afvinklijstje en is de term PIA niet waard. Ook de privacyparagraaf in de Memorie van Toelichting is flinterdun en slechts bedoeld om het wetsvoorstel te legitimeren. Gezien de veiligheidsrisico’s van dit wetsvoorstel ligt bovendien een Security Impact Assessment voor de hand. Bij deze stand van zaken kan Privacy First dit wetsvoorstel dan ook überhaupt niet serieus nemen.

Tweede Kamer aan zet

Mocht het huidige wetsvoorstel ongewijzigd beide Kamers passeren, dan zal Privacy First niet aarzelen om het door de rechter onrechtmatig te laten verklaren. Het is nu aan de Tweede Kamer om het niet zover te laten komen.

Voor nadere informatie of vragen met betrekking tot bovenstaande punten is Privacy First te allen tijde bereikbaar op telefoonnummer 020-8100279 of per email: info@privacyfirst.nl.

Hoogachtend,

Stichting Privacy First

mr. Vincent A. Böhre,
director of operations