Valtioneuvoston kirjelmä Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä

Peter Sund
Toimitusjohtaja
Kyberala, Teknologiateollisuus ry
2024

Finnish Information Security Cluster

***Kaikkien turvallisuusviranomaisten tulisi pitää Yhdysvaltojen kyberturvallisuuden suojelemista olennaisena osana ydintehtäväänsä**, joka on suojella yhteiskuntaa ja noudattaa perustuslakia. …Ottaen huomioon tämän syvällisen ja laaja-alaisen uhan vakavuuden ja täyttääkseen vastuunsa suojella yhteiskuntaa vakavilta vaaroilta ja **varmistaa sen perusinstituutioiden toiminnan jatkuvuus**, turvallisuusviranomaisten tulisi **tukea salatun viestinnän ylläpitämistä**.*

- FBI:n päälakimies Jim Baker, syyskuu 2019

TIIVISTELMÄ

Toteutustapa edelleen hyvin haitallinen muiden perusoikeuksien suojaamiselle, sisältää merkittäviä tietoturvan heikennyksiä sekä mahdollistaa kiertämisen. Ehdotus on tehoton asetettujen tavoitteiden saavuttamiselle eivätkä toimenpiteet ole ennakoitavia, oikeassa suhteessa ja välttämättömiä tavoitteen toteutumiseksi.

- Ehdotus ei suojaa lapsia seksuaaliselta hyväksikäytöltä
- Ehdotus perusoikeuksien rajoittamisesta ei ole tarpeellisuus- ja suhteellisuusperiaatteen mukainen
- Ehdotus ei mahdollista poliittisten tavoitteiden saavuttamista
- Ehdotus on ensimmäinen vaihe sähköisen viestinnän luottamuksellisuuden ja yksityisyyden ydinalueen murentamiselle
- Ehdotus uhkaa yhteiskunnan kokonaisturvallisuutta
- Ehdotus on voimassa olevan EU-oikeuden vastainen
- Suomen tulisi edistää vähemmän haitallisia ja tehokkaita ratkaisuja lasten suojelemiseen

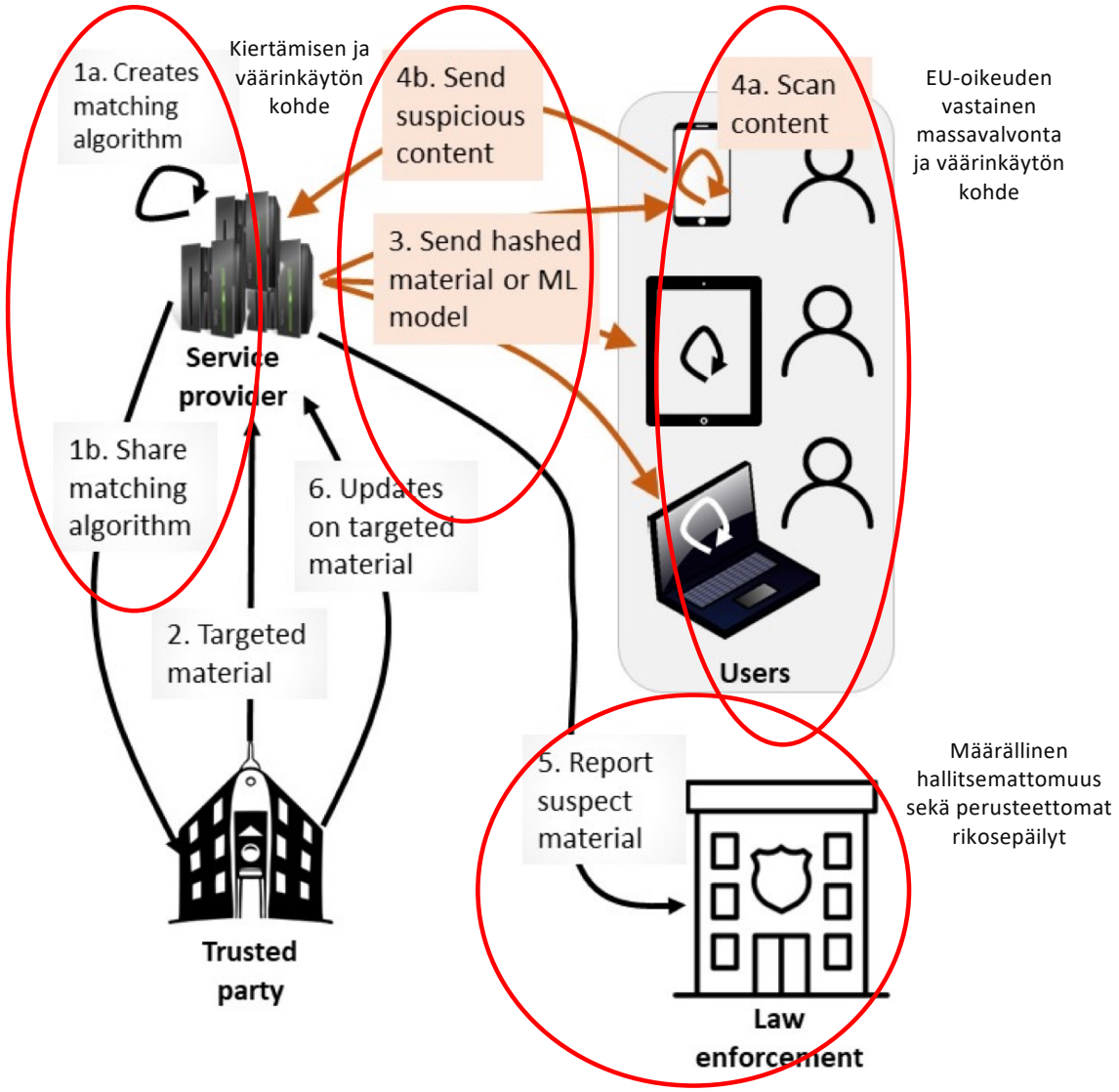
- ✓ Tietoturvan parantaminen kriittisillä toimialoilla ja kyberturvallisuuden kehittämisohjelman toteuttaminen
- ✓ Salaustuotteiden hyväksyntäprosessien nopeuttaminen
- ✓ Hankitaan kansanvälisiä tietoturvahyväksyntöjä myöntävän maan asema
- ✓ Vahvistetaan yhteistyötä yritysten, elinkeinoelämän ja kolmannen sektorin kanssa
- ✓ Määritellään ja tunnistetaan kriittiset tietovarannot, - palvelut ja järjestelmät ja varmistetaan niiden toimintavarmuus ja turvallisuus
- ✓ Arvioidaan kriittisen infran tietojen avointa jakamista
- ✓ Vahvistetaan sosiaali- ja terveyspalvelujen tietojärjestelmien turvallisuutta
- ✓ Varaudutaan maksujärjestelmiin kohdistuviin häiriöihin

Posti- ja kirjemaailmaan verrattuna ehdotus tarkoittaisi käytännössä, että Suomessa Posti tarkastaisi lähetettävien kirjeiden sisällön postilaatikkoon jätettäessä ja lähettäisi tarvittaessa kopion lainvalvontaviranomaiselle.

Kirjesalaisuutta turvaavilla toimilla eli kirjekuoreen sulkemisella ei olisi enää merkitystä.

Yksityisten viestien päivittäinen määrä on vähintään n. 260 miljardia, kuva- ja videotiedostoja olisi arviolta ainakin 1% kaikissa viesteissä eli 2,6 miljardissa päivittäin. Mikäli 10 % Euroopassa, tunnistamismääräys 1 %:iin tarkoittaisi silti 26 miljoonan viestin tutkimista päivittäin (kuukaudessa 780 milj. viestiä). Kyseessä ei voi olla rajattu ja yksilöity valvonnan kohdistaminen.

PERUSTEET

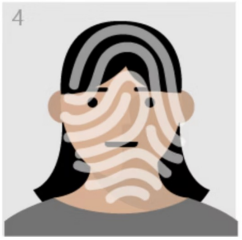

Kiertämisen ja väärinkäytön kohde
1a. Creates matching algorithm
Kiertämisen ja väärinkäytön kohde
4b. Send suspicious content
4a. Scan content
EU-oikeuden vastainen massavalvonta ja väärinkäytön kohde
3. Send hashed material or ML model
Service provider
1b. Share matching algorithm
6. Updates on targeted material
2. Targeted material
Users
5. Report suspect material
Määrällinen hallitsemattomuus sekä perusteettomat rikosepäilyt
Trusted party
Law enforcement

PERCEPTUAL HASHING







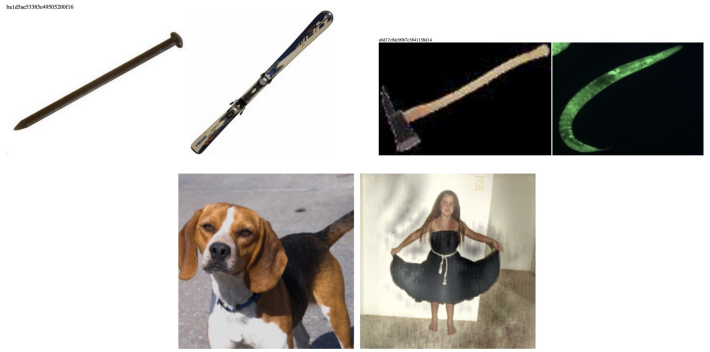


Microsoft's windmill



2,9,2,13, 4,10,6,12, 13,14,60,10, 16,6,29,11, 6,0,3,11, 5,0,0,12, 7,5,133,16, 42,3,172,14, 182,63,255,99, 35,180,255,27, 14,3,209,20, 20,0,207,13, 14,20,255,1, 26,9,255,6, 131,29,255,36, 68,155,255,11, 31,5,255,4, 37,2,255,5, 0,43,45,47, 7,32,54,57, 115,23,49,36, 58,122,59,30, 18,4,57,34, 24,1,48,30, 3,16,133,14, 9,14,164,8, 100,16,148,10, 47,105,127,19, 20,14,137,26, 31,5,132,45, 6,13,36,9, 6,9,32,10, 28,8,25,20, 17,29,34,24, 14,7,63,10, 20,4,71,10

You might notice that my PhotoDNA hash is a little different from Microsoft's published hash. This is because I'm working off of the scaled and recolored image that I extracted from their PDF; this is not the original source that they used. For clarity: I am generating the correct PhotoDNA hash for this specific version of this file.



Slight cropping:

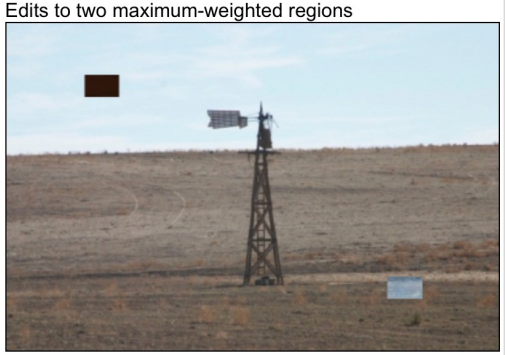


A slight crop changes the hash values a little. The numbers in bold are different from the uncropped source and red denotes values that changed by more than 5. The differences appear as mostly small numerical changes.

2,9,2,**12**, 4,10,6,**11**, 13,14,**63**,**9**, 16,**7**,**32**,**10**, 6,0,3,11, 5,0,0,12, 7,5,**131**,16, **41**,3,**169**,14, **183**,**60**,255,**106**, **39**,**186**,255,**30**, **13**,**4**,**206**,20, 20,0,**204**,**12**, 14,20,255,1, **25**,**8**,255,**5**, **128**,**27**,255,36, **73**,**157**,255,**12**, **30**,**6**,255,4, **39**,**1**,255,5, 0,43,**42**,**46**, **6**,**31**,**48**,**56**, **111**,**21**,**44**,**37**, **63**,**126**,**54**,**29**, **17**,**5**,**52**,34, **22**,1,**41**,**29**, 3,**17**,**134**,**16**, 9,14,**165**,**10**, **99**,**15**,**150**,**9**, **54**,**112**,**125**,**16**, 20,**13**,**133**,**23**, **29**,**6**,**128**,**40**, **7**,**12**,**32**,9, 6,**10**,32,10, **29**,**7**,**26**,**23**, 17,**33**,34,**27**, 14,**9**,**66**,**12**, 20,4,**74**,**13**

One of the hints that I received applied an equalization across the sum-of-gradients in order to scale the values to the range 0 to 255. This has the unfortunate impact of changing lots of values when only a few sum-of-gradients changed. This equalization dramatically increases the number of false-negative matches. (This is the only additional limitation that I've found since writing the original 2014 paper.)

Edits to two maximum-weighted regions



197,84,201,95, 20,155,112,55, **10**,**11**,48,**8**, **13**,**5**,23,**8**, **5**,0,**2**,**9**, **4**,0,0,**9**, 104,42,123,156, 42,76,146,88, 145,50,255,79, 28,143,220,21, **11**,3,166,**16**, **16**,0,165,**10**, **11**,**16**,255,1, 20,**7**,255,**4**, 104,23,255,29, 54,123,255,**8**, 25,**4**,255,**3**, 30,**1**,255,**4**, 0,34,36,37, **5**,26,43,45, 91,**18**,39,29, 46,97,47,24, **14**,**3**,46,27, **19**,1,38,24, **2**,**12**,105,**11**, **7**,**11**,130,**6**, 79,**13**,118,**8**, 37,84,101,**15**, **18**,27,108,36, 46,12,103,65, **5**,**11**,28,**7**, **5**,**7**,26,**8**, 22,**7**,19,**16**, **13**,23,27,**19**, 14,43,73,16, 67,23,101,24

Inverting two of the maximum overlap regions directly impacts four gradient sets (in gray) and changes nearly all hash values.

Why didn't it only change 8 of the 36 grids or 32 of the 144 values? The algorithm applies an equalization after calculating the gradient sums. This causes big changes to propagate across all of the hash values. Most of the red values are clustered around the 8 grids that are directly impacted by the edits.

PERUSTEET

- Ehdotus ei suojaa lapsia seksuaaliselta hyväksikäytöltä
  - Ei sisällä verkkohoukuttelun valvontaa, eikä uuden seksuaaliväkivaltaa todistavan materiaalin tunnistaminen
  - Ei estäisi uuden materiaalin tuottamista eikä houkuttelua, joilla myönteisin vaikutus uhrien perusoikeuksiin, koska nämä edistäisivät parhaiten hyväksikäytön ehkäisemistä
  - Menetelmän tehokkuus erittäin kyseenalainen (käyttäjävalinnat (WhatsApp –> WhatsApp Business tai pimeän verkon palvelut), tunnistamisalgoritmin häirintä, tiivistetietokannan kiertäminen sekä väärien ilmoitusten tuottaminen (esim. Apple), materiaalin poistamisen tehottomuus, pääsynhallinnan rajoitukset
  - Jää parhaimmillaankin hyvin rajalliseksi lapsen edun näkökulmasta
- Ehdotus perusoikeuksien rajoittamisesta ei tarpeellisuus- ja suhteellisuusperiaatteen mukainen
  - Yksityiselämän ja viestinnän suojaa (ml. kirjesalaisuus) heikennettäisiin perustavanlaatuisesti (PL 10:4 §)
  - LiV edellyttänyt, että salauksen käyttöä ei heikennetä (kukaan muu kuin viestin lähettäjä ja tarkoitetut vastaanottajat eivät voi lukea viestejä tai muuten analysoida niitä päätelläkseen viestin sisältöä)
  - Punnintatilanteessakin yksityiselämälle ja –viestinnälle annettava etusija (Euroopan ihmisoikeustuomioistuin, EUTI, EDPB/EDPS, YK)
  - Luottamuksellisen viestin salaisuuden suojaan puuttumisen tulee olla mahdollisimman kohdennettua ja rajattua, jolloin yleistä ja kohdentamaton tietoliikenteen seuranta ei ole mahdollista (PeVL)
  - Vaikka tarkkuutta on näennäisesti parannettu (rajaus ns. ”korkeariskisiin” palveluntarjoajiin sekä visuaaliseen sisältöön ja linkkeihin, tunnistamismääräyksen viimesijaisuus sekä ajallisen keston rajaaminen) valvonta silti poikkeuksellisen laajaa ja yksilöimätöntä eikä perustuisi konkreettiseen ja yksilöityyn rikosepäilyyn (vaan palveluiden ”riskitasoon”) HUOM! rikoksentekijät käyttävät suosituimpia palveluita

PERUSTEET

- Ehdotus ei mahdollista poliittisten tavoitteiden saavuttamista
  - Ei ole hallitusohjelman suuntaviivojen mukainen, vaikka toki hyväksyttävä ja tärkeä pyrkimys suojata lapsia verkkovälitteiseltä seksuaaliväkivallalta
  - Viestinnän yksityisyyden perustavanlaatuinen heikentäminen ei täytä rikosten ehkäisemisen, rikoksentekijöiden saattaminen vastuuseen teoistaan tai uhrien auttamisen tavoitteista
  - Jo annettuja esitutkintatoimivaltuuksien ja –resurssien kohdentaminen, syyttäjien ja tuomioistuimien resursoiminen vaikeiden juttujen huolelliseen käsittelyyn sekä rikosprosessin hallinnollinen tehostaminen
- Ehdotus on ensimmäinen vaihe sähköisen viestinnän luottamuksellisuuden ja yksityisyyden ydinalueen murentamiselle
  - Europol ja jäsenmaiden lainvalvontaviranomaisten johtajat julkaisivat keväällä 2024 yhteisen julistuksen, jonka tavoitteena on murtaa salaus eli yksityisyyden suoja kaikelta viestinnältä
  - Poliittisille päättäjille on turvallisuuden nimissä harhaanjohtavasti perusteltu yksittäisten toimien tarpeellisuutta viestinnän valvonnan laajentamiseksi
  - Unkarin ehdotus vaarantaa Suomen aseman korkean digitaalisen luottamuksen ja perusoikeudet takaavana maana, mikä heikentää liiketoimintaa ja investointihalukuutta, sillä myös elinkeinotoiminta nojaa oikeussubjektien oikeuteen viestiä ja siirtää tietoa luottamuksellisesti osapuolten välillä
  - Saksa, Alankomaat ja moni muu EU-jäsenvaltio on todennut selvästi, että lakiehdotuksella ei ole paikkaa demokraattisessa oikeusvaltiossa

PERUSTEET

- Ehdotus uhkaa yhteiskunnan kokonaisturvallisuutta
  - Järjestelmä mahdollistaisi valtioiden välisen tiedustelun laajentamisen toisten valtioiden oikeudenkäyttöpiiriin sekä laajamittaisen laittoman vakoilun pahantahtoisille valtioille, kuten Venäjä ja Kiina
  - Data ulkomailla ja komponentti haavoittuva: tietoturvan heikentämistä ei voi toteuttaa vain kotimaan turvallisuusviranomaisten tarpeita varten (LiV)
  - Kansalaisten ja kansanvallan valvonta olisi mahdotonta
  - Sensitiivisten järjestelmien rajaaminen valvonnan ulkopuolelle on vahva osoitus menetelmän riskeistä
  - Esim. Alankomaiden turvallisuuspalvelu on todennut, että tällaisen järjestelmän käyttöönotto viestintäpalveluissa muodostaa riskin, jota ei voi hyväksyä
- Ehdotus on voimassa olevan EU-oikeuden vastainen
  - Viestin valvontaan suostumisen edellyttäminen on vapaaehtoisuuteen perustumaton sekä seurauksiltaan käyttäjälle haitallinen ja siten ehdotus ei täytä yleisen tietosuoja-asetuksen edellytyksiä
- Suomen tulisi edistää vähemmän haitallisia ja tehokkaita ratkaisuja lasten suojelemiseen
  - 47 ihmisoikeusjärjestöä vastustaa ehdotusta ja 379 tieteilijää kyberturvallisuuden ja tietosuojan alalta 36 maasta on allekirjoittanut Unkarin uusinta ehdotusta perustellusti vastustavan kannanoton
  - Keinoja mm. käyttäjäpohjainen turvallisuusraportointi ylläpitäjille, käyttäjien perehdyttäminen verkkohoukuttelun riskeihin, suunnitteluperiaatteiden ja oletusasetusten asettaminen (Bik+), verkkoikävarmennus (eIDAS 2.0), käyttäytymiseen perustuvat kontrollit
  - Käyttäjäkoulutus, digitaalinen lukutaito, huoltajien valvonta, Eurooppalainen rikostorjuntapriorisointi, lapsen lähestymistä seksuaalisessa tarkoituksessa koskevan rikos- ja poliisilain muuttaminen (peitetoiminta)


Finnish Information
Security Cluster