TikTok-sovelluksen tietojen kerääminen ja yksityisyysongelmat

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tietotekniikka
Toukokuu 2024
Niklas Aaltonen

TURUN YLIOPISTO
Tietotekniikan laitos

NIKLAS AALTONEN: TikTok-sovelluksen tietojen kerääminen ja yksityisyysongelmat

TkK-tutkielma, 21 s.
Tietotekniikka
Toukokuu 2024

TikTok-sovelluksen tietojen kerääminen sekä niiden mahdollinen luovuttaminen Kiinan hallinnolle on herättänyt huolta viime vuosina. TikTok kerää käyttäjästään monenlaista tietoa, joista osa on jopa arkaluonteisia. Tässä kirjallisuuskatsauksessa tarkastellaan, kuinka TikTok kerää tietoja käyttäjästä ja mihin näitä tietoja käytetään. Tutkielmassa pohditaan myös, miten Kiinan hallinto hyötyisi TikTok-sovelluksen keräämästä tiedosta.
TikTokin keräämiä tietoja ovat esimerkiksi sijainti- ja laitetiedot, käyttäjän yhteystiedot, käyttäjän näppäilytyyli, leikepöydän sisältö sekä käyttäjän luoma sisältö. TikTok käyttää keräämäänsä tietoa pääasiassa suosittelualgoritmiinsa. Tämä mahdollistaa mm. mielipidevaikuttamisen Kiinalle myönteisellä tavalla. Kuitenkin TikTok-sovelluksen yksityisyysongelmat koskevat sen omistajan ByteDancen kiinalaista alkuperää ja Kiinan lainsäädäntö, joka pakottaa kiinalaiset yritykset luovuttamaan tietoja Kiinan tiedustelupalvelulle. Tutkielmassa huomattiin, että TikTok-sovelluksesta on tehty melko vähän akateemisia tutkimuksia ja tämän takia tutkielmassa ehdotetaan jatkotutkimusta TikTokista.

Asiasanat: TikTok, sosiaalinen media, yksityisyys, tiedonkeruu

Sisällys

1 Johdanto

Monille on tuttua rekisteröityessään sosiaalisen median palvelun klikata “olen lukenut tietosuojaselosteen ja hyväksyn tietojeni käsittelyn” ajattelematta kuitenkaan, mihin tulee suostuneeksi näin tehdessään. Hyväksyessään tietosuojaselosteen käyttäjä voi antaa palvelulle luvan kerätä monenlaista tietoa sekä luovuttaa kerättyä tietoa eteenpäin kolmansille osapuolille. Käyttäjä ei kuitenkaan yleensä voi vaikuttaa siihen, mitä tietoja hänestä kerätään, muuten kuin lopettamalla palvelun käyttämisen.

2020-luvulla TikTok-sovelluksesta on tullut tietoturvauhka, koska sen keräämien tietojen luovuttaminen sen kiinalaiselle emoyhtiölle huolettaa. Esimerkiksi helmikuussa 2024 Suomen eduskunta päätti kieltää TikTokin käyttämisen laitteillaan [1] ja maaliskuussa 2024 Yhdysvaltain edustajanhuone hyväksyi lakiehdotuksen, joka pakottaisi TikTokin emoyhtiön ByteDancen myymään TikTok-sovelluksen 180 päivän kuluessa lain voimaan tulosta [2].

Tämän kandidaatintutkielman on tarkoitus perehtyä siihen, kuinka sosiaalinen media kerää tietoja käyttäjästä ja mihin näitä tietoja käytetään.

Tämän tutkielman tutkimuskysymykset ovat:

- TK 1: Mitä tietoja TikTok kerää käyttäjistään?
- TK 2: Mitkä ovat näiden tietojen keräämisen vaikutukset ja mihin tietoja käytetään?

Tutkielma suoritettiin kirjallisuuskatsauksena. Artikkeleita tutkielmaan haettiin seuraavista tietokannoista: IEEE Xplorer, Google Scholar ja Web of Science käyttämällä hakulauseketta tiktok AND (”data collec*” OR privacy OR gdpr). Hakutuloksia rajattiin ensin artikkelien otsikon ja tiivistelmän perusteella. Sen jälkeen hakutuloksia rajattiin vielä artikkelin lukemisen jälkeen. Tutkielman haasteena oli akateemisen kirjallisuuden vähäinen määrä aiheesta.

Tutkielman toisessa luvussa esitellään sosiaalisen median suorittamaan tietojen keräämisen liittyvät käsitteet sekä syitä ja ongelmia tietojen keräämiseen liittyen. Kolmannessa luvussa esitellään miten TikTok-sovellus kerää käyttäjistään tietoja sekä mihin tarkoitukseen tietoja kerätään. Neljännessä luvussa pohditaan Kiinan valtion motiivia käyttää TikTok-sovellusta kerättyä tietoa sekä miten Yhdysvaltojen ja Suomen päätöksentekijöiden mielipiteet eroavat TikTok-sovelluksen kiellon suhteen. Viidennessä luvusssa on yhteenveto, jossa vastataan tutkielman tutkimuskysymyksiin sekä esitetään jatkotutkimusehdotuksia.

2 Tietojen kerääminen sosiaalisessa mediassa

Yksityisyydelle on vaikeaa löytää yleispätevää määritelmää. Yksi tapa havainnollistaa yksityisyyttä on ajatella sitä rajana yksityisen ja julkisen tiedon välillä [3]. Yksityisyys voitaisiin kuitenkin määritellä yksilön oikeutena päättää, mitä muut tietävät hänestä [3]. Yksi syy, jonka vuoksi yksityisyys vaikea määritellä on se, että ajan saatossa on ollut vaihtelevia näkemyksiä siitä, mikä koetaan yksityiseksi. Digitalisaation ja sosiaalisten medioiden tulon myötä yksityisyys on noussut tärkeäksi käsitteeksi, koska yksityisen ja julkisen tiedon välistä rajaa voi olla vaikea erottaa. Tässä luvussa perehdytään tutkielman kannalta olennaisiin käsitteisiin, sekä siihen miten yksityisyys näkyy nykypäivänä sosiaalisessa mediassa.

2.1 Henkilötieto

Melkein jokainen palveluntarjoaja kerää käyttäjistään jonkinlaista tietoa. Mbannaso ja Sogbesan käyttävät käyttäjistä kerätystä tiedosta nimitystä PII (Personally, identifiable information) eli tietoa, jota voidaan käyttää tunnistamaan käyttäjä [4]. Kirjoittajat myöskin toteavat, että PII on palveluntarjoajille erittäin arvokasta, koska sitä voidaan käyttää esimerkiksi kohdentamaan mainoksia tai tarjoamaan käyttäjälle parempaa sisältöä. Mban-

naso ja Sogbesan myöskin toteavat, että PII:hin liittyvä yksityisyys on hankalaa määritellä, koska se on kontekstuaalista ja kulttuurista riippuvaa, minkälaisen tieto on yksityistä ja mikä taas julkista.

Tietosuojavaltuutetun toimiston määritelmä henkilötiedolle on "kaikki tieto, joka liittyy tunnistettuun tai tunnistettavissa olevaan henkilöön" [5]. Kyseinen määritelmä on nykyään käytössä kaikissa Euroopan unionin jäsenvaltioissa keväällä 2018 voimaan tulleen uuden tietosuoja-asetus GDPR (General Data Protection Regulation) myötä. GDPR-asetuksen tarkoituksena on parantaa henkilötietojen suojausta sekä yhtenäistää tietosuojan sääntelyä Euroopan unionin alueella [6].

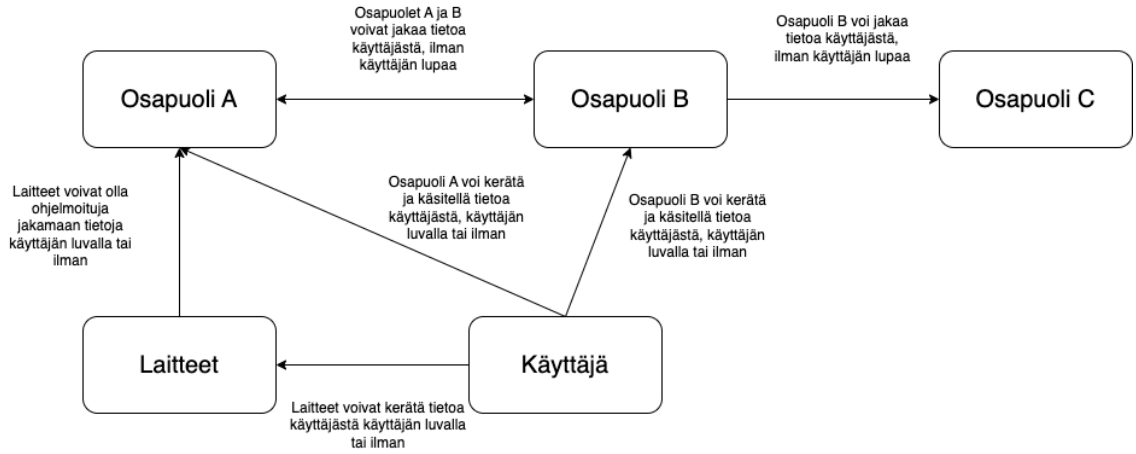
Sekä PII:iin että GDPR:n henkilötiedon määritelmät ovat hyvin samanlaisia. Kummassakin henkilötiedoksi luokitellaan kaikki tieto, josta käyttäjä on tunnistettavissa. GDPR:n tarkempi määritelmä näkyy muuan muassa siinä, että terveystiedot ja poliittiset näkemykset ovat GDPR:n määritelmän mukaan erityisten henkilötietoryhmien käsittelyä ja niiden käsittely on lähtökohtaisesti kiellettyä [6]. Erityisiä henkilötietoryhmiä voidaan kuitenkin käsitellä, jos niiden käsittelyyn on olemassa jokin peruste.

2.2 Tietojen keräämisen syyt ja ongelmat

Tietojen kerääminen on sosiaalisen median palveluntarjoajalle erittäin kannattavaa toimintaa. Palveluntarjoaja voi käyttää keräämänsä tietoa itse, esimerkiksi kohdentamaan paremmin sisältöä käyttäjälle ja siten aktivoida käyttäjää käyttämään palvelua tulevaisuudessakin tai palveluntarjoaja voi käyttää kerättyä tietoa kohdentamaan mainontaa paremmin. Palveluntarjoaja voi myöskin myydä kerättyä tietoa kolmansille osapuolille. Kolmas osapuoli voi käyttää ostamaansa tietoa omaksi hyödykseen tai myydä sen vielä eteenpäin. Palveluntarjoajalle tietojen kerääminen on tärkeää liiketaloudellisesta näkökulmasta, jolla se lisää mahdollista tuottoaan. Myös valtio voi myydä tai luovuttaa keräämiään tietoja

esimerkiksi eri maiden viranomaisten kesken.

Kuva 2.1 kuvaa, miten käyttäjästä kerätty tieto saattaa levitä monelle osapuolelle, vaikka käyttäjä ei olisi antanut lupaa tietojensa käsittelyyn kaikille osapuolille. Käyttäjän on myös mahdotonta vaikuttaa siihen, mitä tietoja mikäkin osapuoli luovuttaa eteenpäin ja mihin tarkoitukseen.



Kuva 2.1: Kuva tiedon jakamisesta osapuolten välillä. Viitattu mukaillen [4]

Aïmeur ja Lafond toteavat, että palveluntarjoajat eivät koskaan pakota käyttäjää luovuttamaan henkilötietojaan, mutta on kuitenkin epävarmaa ymmärtävätkö käyttäjät mitä tietoja heistä kerätään ja mihin tarkoitukseen [7]. Jos käyttäjä kuitenkin haluisi ymmärtää paremmin, mitä tietoja hänestä kerätään, niin tietosuojaselosteet ovat usein vaikeaselkoisia, eikä käyttäjä voi vaikuttaa niihin omilla valinnoillaan. Vaikka jokaisella palveluntarjoajalla olisi yksinkertainen ja helposti ymmärrettävä tietosuojaseloste, niin keskivertokäyttäjän on mahdotonta muistaa kaikkien käyttämiensä verkkosivustojen tietosuojaselosteita. Aïmeur ja Lafond myöskin ehdottavat, että ainoa tapa jolla käyttäjä voi säilyttää yksityisyyden sosiaalisessa mediassa on välillä valehdella käyttämilleen verkkosivustoille. Näin toimimalla kukaan ei pysty määrittämään mikä on totta ja mikä valetta.

Haggad ja muut vertailivat sosiaalisen median sovelluksien ja Covid-19-taudin jäljittämiseen tarkoitettujen sovellusten tietosuojaselosteita [8]. Monen jäljittämiseen tarkoitettujen

sovellusten keräämä tieto oli huomattavasti paremmin suojattua tiedon anonymisoinnin takia ja koska se poistettiin kokonaan, kun sitä ei enää tarvittu. Sosiaalisen median sovelluksissa tietojen suojaaminen ei ollut yhtä korkealla tasolla. Esimerkiksi Facebook väitti poistavansa keräämänsä tiedon 90 päivän kuluttua, mutta totesi myöskin tietosuojaselosteessaan, ettei voi valvoa kolmansille osapuolilleen luovuttamansa tiedon poistoa. Haggad ja muut vertailivat myös sosiaalisen median sovellusten ja jäljityssovellusten käyttäjäarvioita. Niistä selviää, että yhä useampi käyttäjä on huolestunut jäljityssovellusten yksityisyydensuojasta, kuin sosiaalisen median sovellusten yksityisyydestä. Osittain käyttäjien huolta yksityisyydestään saattaa selittää se, että tutkimuksessa huomattiin käyttäjien raportoineen enemmän virheitä ja kaatumisia jäljityssovelluksissa, kuin sosiaalisen median sovelluksissa.

Virheiden ja kaatumisten syy saattaa olla se, että monet jäljityssovellukset tuotiin markkinoille hyvin nopealla aikataululla Covid-19-pandemian aikana ja ne olivat pääasiassa valtion rahoittamia projekteja. Sosiaalisen median sovellukset taas ovat suurien yhtiöiden ylläpitämiä ja niiden taloudellinen motiivi parantaa käyttäjäkokemusta. On myöskin tärkeää huomioida, että jäljityssovellusten keräämään tietoon sisältyi henkilön mahdollinen Covid-19 tartunta, joka GDPR-lainsäädännön artiklan 9 mukaan on erityisten henkilötietoryhmien käsittelyä ja siten on myöskin ymmärrettävää, että käyttäjät olivat huolissaan yksityisyydestään [6].

2.3 Cambridge Analytica -vuoto

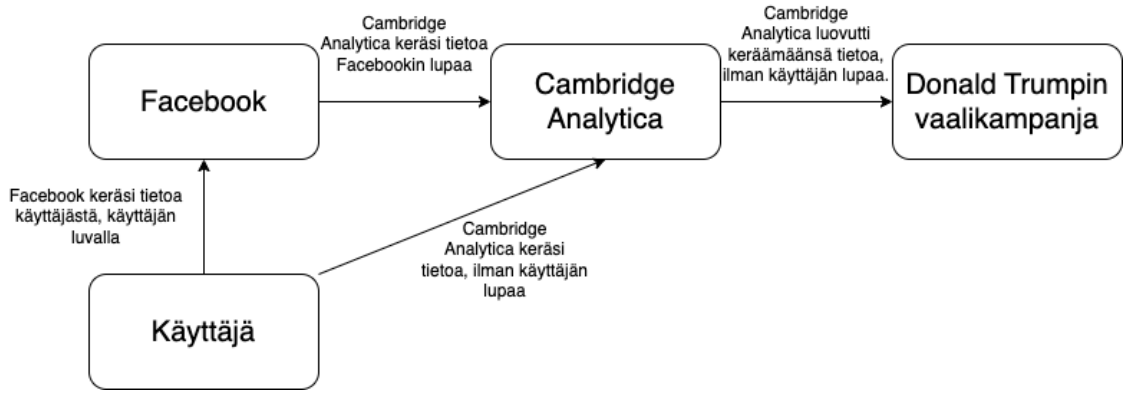
Vuonna 2018 paljastui Cambridge Analytica -nimisen yrityksen keränneen Facebookin ohjelmistorajapinnan kautta käyttäjätietoja ja yhdistäneen käyttäjätietoja käyttäjän tekemään luonnetestiin [4][9]. Cambridgen yliopistossa kehitetyllä testillä voitiin luoda henkilöstä persoonallisuusprofiili viiden suuren persoonallisuuspiirteen teorian avulla, joka

mittaa ihmisen avoimuutta, tunnollisuutta, ulospäinsuuntautuneisuutta, sovinnollisuutta ja neuroottisuutta [10]. Kun käyttäjän persoonallisuusprofiili yhdistettiin Facebookin ohjelmistorajapinnan kautta saatuihin tietoihin, voitiin käyttäjän äänestyskäyttäytymistä ennakoida.

Cambridge Analytican keräämää tietoa hyödynnettiin vuoden 2016 Yhdysvaltain presidentinvaaleissa Donald Trumpin kampanjassa, jolloin Cambridge Analytican keräämän tiedon avulla tietyille käyttäjäryhmille mikrokohdennettiin mainontaa. Cambridge Analytica myös seurasi koko ajan mainonnan vaikuttavuutta, jolloin se pystyi määrittelemään, millainen mainos tehoaa erilaisiin ihmisryhmiin ja näin kohdentamaan mainontaansa vieläkin tarkemmin. On kuitenkin vieläkin epävarmaa, kuinka luotettavasti persoonallisuusprofiilin avulla voidaan ennustaa käyttäjän äänestyskäyttäytymistä. Vuonna 2012 Konsinski ja hänen tiiminsä todistivat, että pelkästään 68 Facebookissa tehdyn tykkäyksen perusteella oli mahdollista ennustaa käyttäjän ihonväri, seksuaalinen suuntautuminen ja oliko käyttäjä demokraattisen vai republikaanisen puolueen kannattaja. Näin voidaan olettaa, että Cambridge Analytican keräämällä tiedolla on ainakin jollain tasolla voitu vaikuttaa vaalien lopputulokseen.

Kuva 2.2 kuvastaa, sitä miten Cambridge Analytica keräsi käyttäjästä tietoa käyttäjän tietämättä. Sekä suoraan käyttäjältä, että myöskin luvatta Facebookin ohjelmistorajapinnan kautta. Kerätyistä tiedoista Cambridge Analytica loi persoonallisuusprofiilin, jonka se luovutti Donald Trumpin vaalikampanjalle.

Moni käyttäjä, joka oli hyväksynyt sen, että Facebook kerää hänestä tietoa, ei todennäköisesti kuitenkaan halunnut, että hänestä kerättyä tietoa käytetään analysoimaan äänestyskäyttäytymistä. Monesti käyttäjä ei yleensä myöskään pysty vaikuttamaan kerätäänkö hänestä ollenkaan tietoa, muuten kuin lopettamalla palvelun käytön, johon todennäköisesti moni käyttäjä ei ole valmis. Hindsin tutkimuksessa selvitettiin ihmisten mielipiteitä yksityisyyteen liittyen Cambridge Analytica -skandaalin jälkeen [11]. Vastaajien mielipi-



Kuva 2.2: Kuva Cambridge Analytican saamien tietojen alkuperästä. Viitattu mukaillen [4]

teet vaihtelivat paljon, osa oli erittäin huolestuneita yksityisyydestään ja osa koki olevansa immuuneja Cambridge Analytican kaltaisten yritysten vaikuttamiselle. Tutkimuksesta käy hyvin ilmi luvun 2.1 maininta siitä, miten yksityisyys on hyvin kontekstuaalista ja kulttuurista riippuvaa, koska osa vastaajista kertoi, ettei jaa sosiaalisessa mediassa osoitetietojaan tai luottokortin tietoja, joten yksityisyys ei ole heille tärkeää.

Tässä luvussa käsiteltiin tutkielman kannalta olennaisia käsitteitä, sekä sitä miksi tietoja kerätään ja mitä ongelmia tietojen keräämiseen liittyy. Cambridge Analytica -vuoto ei välttämättä vaikuttanut kaikkien ihmisten mielipiteisiin sosiaalisen median suorittamasta tietojen keräämisestä ja seuraavassa luvussa tulemme tutkimaan, miksi TikTok-sovellus kuitenkin koetaan suureksi uhaksi.

3 Tietojen kerääminen TikTok-sovelluksessa

Vuonna 2018 julkaistu TikTok on yksi maailman suosituimmista sosiaalisen median sovelluksista. Sen toiminta perustuu käyttäjien jakamiin lyhyisiin videoihin. Helmikuussa 2024 sen sovellusta oli ladattu noin 4,7 miljardia kertaa. TikTokin suosiota selittää sen kehittynyt algoritmi, joka tarjoaa käyttäjälle sisältöä, josta käyttäjä voisi olla kiinnostunut. Suurin osa TikTokin käyttäjistä on nuoria, joidenkin arvioiden mukaan noin 60 % yhdysvaltalaisista TikTok-käyttäjistä on 16–24-vuotiaita. TikTokin suosiosta kertoo myös se, että keskimäärin käyttäjä viettää aikaa TikTokissa 95 minuuttia päivässä. Tässä luvussa perehdytään siihen, miksi nuorten suosiossa oleva sovellus on noussut 2020-luvulla tietoturvauhaksi. [12]

3.1 TikTokin käyttäjästään keräämät henkilötiedot

TikTok kertoo tietosuojaselosteessaan keräävänsä tietoja käyttäjästä kolmella eri tavalla. Käyttäjän itse luovuttamana, automaattisesti kerättynä, sekä kolmansilta osapuolilta saatuna tietona. Käyttäjän itse luomaa tietoa on esimerkiksi käyttäjän perustiedot kuten sähköpostiosoite ja salasana. Tietosuojakäytännön mukaan TikTok kerää myös tietoa kaikesta käyttäjän luomasta sisällöstä, kuten videoista, kuvista, tykkäyksistä ja kommenteista. Tik-

Tok myös kertoo keräävänsä tietoa laitteen leikepöydältä, jos käyttäjä haluaa kopioida tai liittää sisältöä. [13]

Automaattisesti kerättyä tietoa on esimerkiksi laitteen tekniset tiedot kuten IP-osoite, laitteen malli, sekä laitteen kieli. TikTok listaa laitteen teknisiksi tiedoiksi myös käyttäjän näppäilytavan ja -rytmin. Tietosuojakäytännössä kuvataan myös se, miten TikTok kerää käyttäjän tuottamasta sisällöstä ominaisuuksia ja piirteitä. TikTokin mukaan ominaisuuksia ja piirteitä ovat esimerkiksi videoissa esiintyvä esineet, maisemat ja kasvot, jotka tunnistetaan videoista automaattisesti tekoälyn avulla. [13] Käyttäjän näppäilytavan ja –rytmin seuraaminen on TikTokille ainutlaatuista tietoa, eivätkä muut sosiaalisen median palvelut yleensä kerää kyseistä tietoa. Näppäilytapa ja –rytmi on myöskin melko uniikki jokaiselle käyttäjälle, joten sitä voitaisiin todennäköisesti käyttää tunnistamaan käyttäjä.

Taulukossa 3.1 on listattuna jotain TikTokin keräämiä tietoja. Käyttäjä ei pysty vaikuttamaan TikTokin automaattisesti keräämiin tietoihin muun kuin sijaintitiedon osalta. Käyttäjä ei voi kuitenkaan kokonaan estää TikTokia käyttämästä sijaintitietoa, koska vaikka käyttäjä estäisi TikTokia saamasta käyttäjän tarkkaa osoitetta TikTok kuitenkin tallentaa käyttäjän sijainnin IP-osoitteen perusteella. Käyttäjän itsensä luovuttamiin tietoihin käyttäjä pystyy suurilta osin vaikuttamaan. Käyttäjä voi olla rekisteröitymättä, jolloin TikTok ei pysty keräämään käyttäjän sähköpostiosoitetta, syntymäpäivää tai käyttäjän luomaa sisältöä. Käyttäjän katsoma sisältö kerätään automaattisesti, mutta se on myöskin käyttäjän itse luovuttamaa. Käyttäjä voi olla luovuttamatta katsomaansa sisältö olemalla käyttämättä sovellusta. Myöskään TikTokin kolmansilta osapuolilta keräämään tietoon käyttäjä ei pysty vaikuttamaan.

TikTokin tietosuojaseloste on kuitenkin melko samanlainen, kuin muidenkin suurten sosiaalisten medioiden palvelujen selosteet. TikTokin tietosuojaseloste eroaa kuitenkin muista sosiaalisen median palveluista siinä, että se jakaa keräämänsä tietoa kolmansille osapuolille ja tytäryhtiöilleen. ByteDancen omistamia yrityksiä muun muassa BytePlus, joka myy

Taulukko 3.1: TikTokin keräämiä henkilötietoja.

Henkilötieto	Automaattisesti kerätty	Käyttäjän luovuttama	Kolmannelta osapuolelta	Käyttäjä voi estää keräämisen
IP-osoite	x			
Laitteen malli	x			
Laitteen kieli	x			
Sijaintieto	x			x
Näppäilytapa	x			
Sähköpostiosoite		x		x
Syntymäpäivä		x		x
Luotu sisältö		x		x
Katsottu sisältö	x	x		
Yhteystiedot		x		x
Toimet TikTokin ulkopuolella			x	x
Muista lähteistä			x	

tekoäly ja data-analyysi työkaluja. Näin TikTokin keräämää tietoa voidaan käyttää esimerkiksi kouluttamaan erilaisia tekoälytyökaluja. [14] Entisen TikTokin työntekijän mukaan raja TikTokin ja ByteDancen välillä oli erittäin häilyvä ja melkein olematon [15].

TikTok-sovellus ei ole käytettävissä Kiinassa, vaan ByteDance on julkaissut sinne oman sovelluksen Douyin. TikTok ja Douyin perustuvat pääosin samaan lähdekoodiin. Linin tutkimuksessa verrattiin TikTokin ja Douyin verkkoliikennettä sovellusta käytettäessä. Sovellusten verkkoliikenteessä ei huomattu suuria eroja. Douyin kuitenkin keräsi käyttäjän laitteen MAC-osoitteen, jolla laite voidaan tunnistaa tarkasti TikTok ei kuitenkaan laitteen MAC-osoitetta kerännyt. Tutkimuksessa ei myöskään huomattu kummankaan sovelluksen lähettävän laitteen yhteystietoja, kuvia tai tiedostoja laitteelta. [16] Tutkimus kuitenkin suoritettiin niin, että sovelluksen asentamisen jälkeen sovelluksesta katsottiin muutama ensimmäinen video, eli ei voida sanoa varmaksi, ettei TikTok tai Douyin lähettäisi lisää tietoa käyttäjästä tai laitteesta, kun sovellusta käytetään pidempään.

Linin tutkimuksessa kävi myöskin ilmi, että Douyin käyttää dynaamista koodin latausta joka tarkoittaa että, kun sovellus käynnistettiin, se latasi palvelimelta erillisen sovelluk-

sen. Tällä tavalla käyttäjä tai sovelluksen julkaissut sovelluskauppa ei pysty valvomaan sovelluksen toimintaa. TikTokin lähdekoodista ei kuitenkaan dynaamista koodin latausta löytynyt. [16]

TikTok tallentaa paljon kerättyä tietoa käyttäjästä laitteelle. Khoan ja muiden tutkimuksessa TikTok-sovellus oli tallentanut laitteelle 103 tiedostoa, käyttäjän toimista sovelluksessa. Tiedostot sisälsivät tietoa esimerkiksi, milloin sovellus oli asennettu, viimeksi avattu tai päivitetty. Tiedostot sisälsivät myöskin laitteen MAC-osoitteen sekä muita laitteen tunnistavia tietoja, vaikkakin edellä käsitellyssä Linin tutkimuksen mukaan TikTokin ei huomattu lähettävän niitä eteenpäin. Vaikkakaan Linin tutkimuksessa ei myöskään huomattu TikTokin lähettävän laitteen yhteystietoja, niin Khoan ja muiden tutkimuksessa TikTok oli kuitenkin luonut tiedoston, joka sisälsi laitteen yhteystietoja. [17]

3.2 Kerättyjen henkilötietojen käyttötarkoitukset

TikTok käyttää keräämäänsä tietoa suosittelualgoritmiinsa. TikTokin suosittelualgoritmia pidetään yhtenä parhaista. Sen suosittelualgoritmi pystyy tunnistamaan muun muassa sukupuolen sekä tietoa käyttäjän mielenterveydestä. Marwickin mukaan TikTokin suosittelualgoritmi toimii pääasiassa seuraamalla videon katsomisaikaa. On kuitenkin todennäköistä, että TikTok käyttää suosittelualgoritmissaan myös videoissa olevia ominaisuuksia ja piirteitä ja tarjoaa näin käyttäjälle samanlaisia videoita. Kun suosittelualgoritmin tieto yhdistetään kaikkeen tietoon, jota TikTok kerää kolmansilta osapuolilta voidaan käyttäjästä saada hyvinkin tarkkaa ja jopa salaista tietoa. [12]

ByteDancen mukaan algoritmi käyttää käyttäjän kiinnostuksen kohteita ja käyttämispiirteitä kuvaamaan käyttäjää. Käyttäjän avatessa sovelluksen ensimmäistä kertaa voi käyttäjä valita kirjautua sisään sosiaalisen median palvelun kuten Facebook tai Instagram kautta, jolloin TikTok voi hyödyntää sosiaalisen median käyttäjätietoja ja käyttää niitä hyväksi

kiinnostuksen kohteiden ja käyttämispiirteiden selvittämiseksi. [18]

TikTok kuitenkin eroaa muista suurista sosiaalisen median palveluista siinä, että se on kiinalaisessa omistuksessa. Kiinan vuoden 2017 kansallinen tiedustelulaki voi pakottaa kaikki kiinalaiset yritykset luovuttamaan tietojaan Kiinan tiedustelupalvelulle. Tiedustelulain tultua voimaan muun muassa Australia ja Yhdysvallat kielsivät Huaweita rakentamasta 5G-verkkoja, koska sitä epäiltiin tietojen vuotamisesta Kiinan tiedustelupalveluille. [15]

TikTok kieltää luovuttaneensa Kiinalle tietoja. TikTok on kuitenkin vuosien 2019–2021 välillä luovuttanut Yhdysvaltojen viranomaisten pyynnöstä tietoja yli 7000 kertaa Yhdysvaltojen lain perusteella. Marwick nostaa myös esille sen, että esimerkiksi vakuutusyhtiöt ja sosiaalipalvelut voivat kerätä tietoa TikTok-sovelluksesta ja näin esimerkiksi kieltäytyä palvelemasta asiakkaita. [12]

Kiina ei ole kuitenkaan ainut maa, jonka lainsäädäntö pakottaa maassa toimivia yrityksiä luovuttamaan tietoa tiedustelupalvelulle, vaan samankaltaisia lakeja on muun muassa Yhdysvalloissa ja Venäjällä [19]. Yhdysvaltojen Foreign Intelligence Surveillance Act 1978 pakottaa kaikkia yhdysvaltalaisyrityksiä luovuttamaan tietoja viranomaisille viranomaisen oikeudellisesti sitovasta pyynnöstä. Kyseisen lainsäädännön vuoksi Euroopan Unionin tuomioistuin kielsi vuonna 2020 henkilötietojen siirron Yhdysvaltoihin tietoturvaan liittyvien ongelmien vuoksi. Yhdysvalloilla on myöskin ollut valvontaohjelma PRISM, joka on voinut seurata esimerkiksi Facebookin, Googlen ja Microsoftin verkkoliikennettä reaaliaikaisesti. [20]

PRISM-ohjelmalla NSA sai hankittua tietoa käyttäjistä suoraan palveluntarjoajan palvelimelta, ilman oikeudellista pyyntöä. PRISM-ohjelma aloitettiin alun perin terrorismintorjuntaan ja mahdollisten terroristien viestinnän seuraamiseen ulkomailla, mutta ei kuitenkaan ole täysin varmaa onko PRISM-ohjelmaa käytetty myöskin yhdysvaltalaisten käyttäjien seuraamiseen. PRISM-ohjelmalla NSA sai hankittua palveluntarjoajilta muun muassa sähköposteja, viestejä, kuvia ja tallennettua tietoa. [21] PRISM-ohjelmalla saadut tiedot ovat siis melko samanlaisia, mitä Kiinan tiedustelupalvelu voisi pyytä TikTokia luovuttamaan.

Tässä luvussa tarkasteltiin, mitä tietoa TikTok kerää käyttäjistään ja mihin näitä tietoja käytetään. Seuraavassa luvussa pohditaan, miksi TikTok-sovellusta ollaan kieltämässä Yhdysvalloissa.

4 Pohdintaa

Kuten luvussa 3.1 todettiin, TikTokin keräämän tiedon määrä ei eroa suuresti muista suurista sosiaalisen median palveluista. TikTok on kuitenkin noussut länsimaissa suureksi uhaksi omistajansa ByteDancen Kiina-suhteiden takia. Tässä luvussa pohditaan, mikä olisi Kiinan motiivi käyttää TikTokista kerättyä tietoa ja tutkitaan miten Suomen ja Yhdysvaltojen päätöksentekijöiden mielipiteet eroavat TikTok-sovelluksen osalta.

Kiina on autoritäärinen maa, eli sen hallinto on keskittynyt yhdelle puolueelle Kiinan kommunistiselle puolueelle. Autoritäärisen hallinnon takia FBI pitää Kiinan suorittamaa vastavakoilua ja taloudellista vakoilua yhtenä suurimmista Yhdysvaltoja uhkaavista uhkista. FBI:n mukaan Kiinan tavoitteena on vaikuttaa päätöksentekijöihin ja yleisiin mielipiteisiin saavuttaakseen Kiinaa suosivampia päätöksiä. Toinen Kiinan tavoite on nousta maailman suurimmaksi supervallaksi, esimerkiksi immateriaalioikeuksien varkauksilla ja kybermurroilla sekä -hyökkäyksillä. [22]

TikTokin keräämästä paikkatiedosta voitaisiin etsiä käyttäjiä, jotka käyvät joka päivä samassa paikassa ja päätellä näin, että nämä käyttäjät ovat töissä kyseisessä paikassa. Jos kyseinen yritys olisi Kiinan hallinnolle hyödyllinen, voitaisiin TikTokin keräämän tiedon perusteella kohdentaa kyseisiin käyttäjiin esimerkiksi tiedustelua tai kalasteluyrityksiä teollisuusvakoilua varten. Paikkatiedon avulla voitaisiin myöskin selvittää arkaluonteisia paikkoja, kuten kävi vuonna 2017, kun terveyssovellus Strava julkaisi kartan käyttä-

jien käyttämistä reiteistä [23]. Kartasta näkyi selkeästi Yhdysvaltain armeijan tukikohtia Afganistanissa ja Syyriassa.

Suurin hyöty TikTokista Kiinan hallinnolle olisi sen käyttäminen päättäjiin ja yleiseen mielipiteeseen vaikuttaminen. TikTokin keräämän tiedon avulla voitaisiin esimerkiksi Kiinan hallintoon negatiivisesti suhtautuviin käyttäjiin kohdentaa mainontaa tai muita keinoja, joilla heidän mielipidettään saataisiin muokattua, kuten Cambridge Analytican tapauksessa, jossa mainontaa kohdistettiin tiettyihin ihmisryhmiin.

Mielipiteisiin vaikuttamista voitaisiin suorittaa TikTokissa myöskin sensuroimalla arkaluonteisia aiheita. Lin:in tutkimuksessa havaittiin Douyin sensuroivan Kiinan hallinnolle arkaluonteisia aiheita, kuten Taiwan ja Covid-19. TikTokissa ei kuitenkaan havaittu samanlaista sensurointia, mutta TikTokin lähdekoodissa oli kuitenkin viitteitä koodista, jolla voitaisiin sensuroida sisältöä [16].

Tietojen keräämistä ja niiden käyttämistäkin suurempi uhka TikTokissa on kuitenkin disinformaatio. Tietokirjailija Petteri Järvinen esittää Yle uutisten analyysissa kysymyksen, jos TikTok olisi venäläinen, miten siihen suhtauduttaisiin ja minkälaista sisältöä se näyttäisi esimerkiksi Ukrainan sotaan liittyen [24].

Jos TikTok olisi venäläinen sovellus ja olisi vaara, että se luovuttaisi tietoja Venäjän hallinnolle, olisivatko länsimaat silloin tiukemmin TikTokin kieltämisen kannalla ja miksi? Melko todennäköistä olisi, että tässä tapauksessa TikTokin toimintaa tarkkailtaisiin huomattavasti tarkemmin tai se olisi kielletty monissa maissa kokonaisuudessaan. Osittain kriittisempää suhtautumista TikTokiin selittäisi Venäjän käymä sota Ukrainassa ja sen aiheuttamat pakotteet. Mutta suhtautumista selittäisi myös se, että Venäjällä ihmisoikeustilanne ei ole niin hyvä mitä monissa muissa maissa. Venäjällä esimerkiksi sanavapautta ja lehdistönvapautta on rajoitettu huomattavasti, joten jos TikTok olisi venäläinen niin olisi suuri huoli siitä, että sen keräämää tietoa käytettäisiin löytämään ihmisiä, jotka olisivat

Venäjän hallinnon kanssa eri mieltä.

Näin voidaan nähdä miten Kiina hyötyisi TikTok-sovelluksen käyttämisestä. Kiinan hallinto voisi käyttää TikTok-sovelluksen keräämää tietoa seuraamaan ihmisiä, joiden mielipiteet eivät ole myönteisiä Kiinan hallintoa kohtaan. TikTok-sovellusta voitaisiin myöskin käyttää sensuroimaan sisältöä, joka ei ole Kiinan hallinnolle mieluista. Myös TikTok-sovelluksen algoritmiin vaikuttamalla Kiinan hallinto voisi vaikuttaa sovelluksen sisältöön, niin että sovelluksella voitaisiin vaikuttaa yleiseen mielipiteeseen.

Yhdysvaltalaiset päätöksentekijät ovat saaneet turvallisuusasiantuntijoiden salaisia raportteja TikTok-sovelluksesta. Päätöksentekijöiden kommenttien perusteella voitaisiin kuitenkin arvioida, että raporteissa ei ole ollut todisteita siitä, että Kiina olisi päässyt käsiksi TikTokin keräämään tietoon ja raportit ovat sisältäneet vain uhkakuvia siitä, miten Kiinan voisi hyötyä TikTokin käyttämisestä esimerkiksi poliittiseen vaikuttamiseen.

Syy Yhdysvaltojen haluun kieltää TikTok-sovellus on todennäköisesti pelko sovelluksen suorittamasta käyttäjien vakoilusta. Yhdysvallat haluaa torjua Kiinan vakoilua, koska se ei halua Kiinan nousevan supervallaksi, jolloin Kiina voisi uhata Yhdysvaltojen asemaa maailmanpolitiikassa. Toinen syy on myöskin pelko Kiinan kyvystä vaikuttaa TikTok-sovelluksen algoritmiin. Kiina on yrittänyt vaikuttaa Yhdysvaltojen vuoden 2016 ja 2018 vaaleihin hakkeroinneilla [25]. Vaikuttamalla TikTok-sovelluksen algoritmiin, Kiina voisi vaikuttaa suurestikin Yhdysvaltojen tuleviin presidentinvaaleihin.

Ylen kyselyn mukaan 126 suomalaisesta kansanedustajasta 84 kieltäisi TikTok-sovelluksen Euroopan unionissa. Kyselyyn vastanneista kansanedustajista 19 ei kannattaisi TikTok-sovelluksen kieltämistä. TikTok-sovelluksen kieltämistä kansanedustajat perustelevat esimerkiksi sovelluksen kiinalaisella alkuperällä, sen vaikutuksilla käyttäjiinsä sekä sen keräämän tiedon takia. Muutama kansanedustaja mainitsee TikTok-sovelluksen vakoilevan Kiinan valtiolle. TikTok-sovelluksen kieltämistä vastustavista kansanedustajista osa myön-

tää sovelluksessa olevan ongelmia, mutta ei kannata kieltoa sen takia, että sitä voitaisiin kiertää. Moni kansanedustaja myöskin kannattaa muidenkin sosiaalisen median palveluiden, kuin pelkän TikTok-sovelluksen rajoittamista. [26]

Suomessa päätöksentekijät ovat huomattavasti enemmän huolissaan TikTok-sovelluksen vaikutuksista sen käyttäjiin. Yhdysvaltaiset päätöksentekijät ovat keskittyneet enemmän sovelluksen mahdolliseen vakoiluun. Mielipiteissä näkyy hyvin jo aiemmin mainittu Yhdysvaltojen suurvalta-asema, joten se on enemmän huolissaan Kiinan nousemisesta suurvallaksi ja Suomessa ollaan enemmän huolissaan sovelluksen koukuttavuudesta ja haitallisesta sisällöstä, eikä niinkään mahdollisesta vakoilusta.

TikTok-sovelluksen kielto ei kuitenkaan saa kovin suurta kannatusta yhdysvaltalaisilta käyttäjiltä. 38 % yhdysvaltalaista aikuisista kannatti TikTok-sovelluksen kieltämistä Yhdysvalloissa ja 27 % ei kannattanut kieltoa. 13–17-vuotiaista kieltoa kannatti 18 % ja kieltoa vastusti 50 % vastaajista [27]. Nuorten vastustus kieltoa vastaan, johtuu todennäköisesti siitä, että suurin osa nuorista käyttää usein TikTok-sovellusta eikä halua luopua siitä. Kyselyssä myös korostuu se, että suurempi osa republikaanipuolueen kannattajista kuin demokraattien kannattajista on sovelluksen kieltämisen kannalla. Ilmiötä ovat todennäköisesti voimistaneet presidentti Donald Trumpin kielteiset näkemykset Kiinasta.

5 Johtopäätökset

Tässä luvussa vastataan tutkielman tutkimuskysymyksiin, sekä esitetään ehdotuksia jatkotutkimukselle.

TK1: Mitä tietoja TikTok kerää käyttäjästään?

TikTok kerää käyttäjistään monenlaista tietoa kolmella eri tavalla: automaattisesti kerättynä, käyttäjän itse luovuttamana sekä kolmansilta osapuolilta saatuna.

Automaattisesti kerättyä tietoa ovat esimerkiksi laitteen malli sekä IP-osoite. Automaattisesti kerättyyn tietoon käyttäjä ei voi vaikuttaa, koska näiden tietojen kerääminen on automaattista ja oletusarvoista. Käyttäjä ei myöskään pysty kieltämään näiden tietojen keräämistä, muuten kuin poistamalla sovelluksen.

Käyttäjän itse luovuttamaa tietoa ovat esimerkiksi rekisteröityessä syötetty sähköpostiosoite, sekä kaikki sisältö, jonka käyttäjä on luonut sovelluksessa. Käyttäjä pystyy vaikuttamaan joiltain osin luovuttamaansa tietoon esimerkiksi olemalla luomatta sisältöä. Käyttäjä voi myös olla rekisteröitymättä palveluun, jolloin käyttäjä ei luovuta TikTokille muuta tietoja, kuin katsomansa videot.

Kolmansilta osapuolilta saatua tietoa on esimerkiksi mainostajilta saatu tieto. Kolmansien osapuolien luovuttamaan tietoon käyttäjä ei voi vaikuttaa. Käyttäjä ei myöskään voi tietää

millaista tietoa kolmas osapuoli luovuttaa TikTokille.

TikTokin tietosuojaseloste ei eroa suuresti muiden suurten sosiaalisen median palveluiden tietosuojaselosteista. TikTok kuitenkin kerää ja jakaa tietoa kolmansien osapuolien kanssa ja tytäryhtiöidensä kanssa enemmän kuin muut sosiaalisen median palvelut. Tutkimuksissa TikTokin on todettu keräävän paljon tietoa laitteesta ja osa tiedosta on myös laitteen tunnistavia tietoja. Tutkimuksissa ei kuitenkaan ole voitu todistaa, että TikTok lähettäisi näitä tietoja palvelimilleen.

TikTok kerää käyttäjästä hyvin monenlaista tietoa, joista osa on jo itsessään arkaluonteista tietoa. Kun eri tietoja yhdistetään niin käyttäjästä voidaan luoda erittäin tarkka profiili, joka voi sisältää hyvinkin paljon arkaluonteista tietoa käyttäjästä. Käyttäjä ei pysty suurilta osin vaikuttamaan TikTokin keräämän tiedon määrään ja miten arkaluonteista tietoa TikTok kerää käyttäjästä.

TK2: Mitkä ovat näiden tietojen keräämisen vaikutukset ja mihin niitä käytetään?

TikTokin keräämää tietoa käytetään pääasiassa sen suosittelualgoritmille. Syöttämälle suosittelualgoritmille käyttäjästä kerättyä tietoa algoritmi voi suositella käyttäjää kiinnostavaa sisältöä, ja näin pidentää käyttäjän sovelluksessa käyttämää aikaa. TikTokin suosittelualgoritmia pidetään yhtenä sosiaalisen median parhaimmista suosittelualgoritmeista ja sen menestyksen takana on todennäköisesti se miten paljon erilaista tietoa sille syötetään.

TikTok kerää käyttäjästä myöskin sellaista tietoa, joka sellaisenaan sekä yhdistettynä muihin tietoihin on hyvin arkaluontoista. Koska Kiinan tiedustelulainsäädäntö takaa Kiinan tiedusteluviranomaisille pääsyn kiinalaisten yritysten tietoihin, on herännyt huoli Kiinan tiedusteluviranomaisten pääsystä TikTok-sovelluksen käyttäjistä keräämään arkaluontei-

siin tietoihin. Tämän takia TikTok on noussut tietoturvauhkaksi ja esimerkiksi Yhdysvallat on hyväksynyt lain, joka pakottaisi TikTokin myymään Yhdysvaltojen toimintonsa yhdysvaltalaiselle yritykselle. Yhdysvallat on myöskin huolissaan Kiinan hallinnon käyttävän TikTokia esimerkiksi päätöksentekijöihin ja yleiseen mielipiteeseen vaikuttamiseen.

Jatkotutkimus

Vaikka TikTok-sovellus on julkaistu vuonna 2018, sitä koskevia tutkimuksia on tehty melko vähän ja ne ovat olleet melko pintapuolisia. TikTok-sovellusta ollaan kieltämässä Yhdysvalloissa vaikka ei ole julkisia todisteita, siitä että Kiinan tiedusteluviranomaiset käyttäisivät TikTok-sovellusta vakoillakseen käyttäjiä tai että viranomaiset olisivat pyytäneet tietoja TikTokilta. Siksi olisi tärkeää tehdä jatkotutkimusta TikTok-sovelluksesta, vaikkakin jatkotutkimuksella ei olisi vaikutusta jo laadittuun TikTok-sovelluksen kieltoon. Jatkotutkimusta voitaisiin myös tehdä siitä, millainen ja miten tarkka profiili käyttäjästä voidaan luoda TikTok-sovelluksen keräämän tiedon perusteella, ja onko tällainen profiili hyödyllinen esimerkiksi vakoilu- tai vaikuttamistarkoituksessa.

Lähdeluettelo

[1] Eduskunta, *Eduskunta estää TikTokin käytön laitteillaan*, https://www.eduskunta.fi/FI/tiedotteet/Sivut/Eduskunta-estaa-TikTokin-kayton-laitteillaan.aspx, 2024. (viitattu 29. 02. 2024).

[2] CBS News, *A bill that could lead to a TikTok ban is gaining momentum in Congress Here's what to know.* https://www.cbsnews.com/news/tiktok-ban-congress-bill-bytedance-divest/, 2024. (viitattu 29. 02. 2024).

[3] A. Lukács, ”What is privacy? The history and definition of privacy”, 2016.

[4] U. Mbannaso ja A. Sogbesan, ”The conceptualisation of a Configurable Consent Architecture for Personal Data Release”, teoksessa *2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON)*, 2022, s. 1–5. DOI: 10.1109/NIGERCON54645.2022.9803088.

[5] Tietosuojavaltuutetun toimisto, *Usein kysyttyä EU:n tietosuoja-asetuksesta*, https://tietosuoja.fi/gdpr. (viitattu 15. 02. 2024).

[6] Euroopan parlamentti, *EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679*, 2016. url: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679 (viitattu 29. 02. 2024).

[7] E. Aïmeur ja M. Lafond, ”The Scourge of Internet Personal Data Collection”, teoksessa *2013 International Conference on Availability, Reliability and Security*, 2013, s. 821–828. DOI: 10.1109/ARES.2013.110.

[8] O. Haggag, S. Haggag, J. Grundy ja M. Abdelrazek, ”COVID-19 vs Social Media Apps: Does Privacy Really Matter?”, teoksessa *2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS)*, 2021, s. 48–57. DOI: 10.1109/ICSE-SEIS52602.2021.00014.

[9] J. Isaak ja M. J. Hanna, ”User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection”, *Computer*, vol. 51, nro 8, s. 56–59, 2018. DOI: 10.1109/MC.2018.3191268.

[10] I. ur Rehman, ”Facebook-Cambridge Analytica data harvesting: What you need to know”, *Library Philosophy and Practice*, s. 1–11, 2019.

[11] J. Hinds, E. J. Williams ja A. N. Joinson, ”“It wouldn’t happen to me”: Privacy concerns and perspectives following the Cambridge Analytica scandal”, *International Journal of Human-Computer Studies*, vol. 143, s. 102 498, 2020.

[12] A. Marwick, ”Privacy without power: What privacy research can learn from surveillance studies”, *Surveillance & Society*, vol. 20, nro 4, s. 397–405, 2022.

[13] TikTok, *Privacy Policy*, https://www.tiktok.com/legal/page/eea/privacy-policy/en. (viitattu 17. 04. 2024).

[14] A. Zulkifli, ”TikTok in 2022: Revisiting Data and Privacy”, *Computer*, vol. 55, nro 6, s. 77–80, 2022. DOI: 10.1109/MC.2022.3164226.

[15] H. Lamb, ”That TikTok privacy debate in 10 questions”, *Engineering & Technology*, vol. 18, nro 4, s. 47–51, 2023. DOI: 10.1049/et.2023.0407.

[16] P. Lin, ”TikTok vs Douyin A Security and Privacy Analysis”, University of Toronto, tekninen raportti, 2021.

[17] N. Hoang Khoa, P. The Duy, H. Do Hoang, D. Thi Thu Hien ja V.-H. Pham, ”Forensic analysis of TikTok application to seek digital artifacts on Android smartphone”, teoksessa *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)*, 2020, s. 1–5. DOI: 10.1109/RIVF48685.2020.9140739.

[18] Z. Zhao, ”Analysis on the “Douyin (Tiktok) Mania” phenomenon based on recommendation algorithms”, teoksessa *E3S Web of Conferences*, EDP Sciences, vol. 235, 2021, s. 03 029.

[19] Tietosuojavaltuutetun toimisto, *Tietosuojavaltuutetun päätös tiedonsiirtojen kieltämisestä ja keskeyttämisestä*, https://finlex.fi/fi/viranomaiset/tsv/2023/20231923. (viitattu 08. 05. 2024).

[20] Tietosuojavaltuutetun toimisto, *Kirjastojen verkkosivustolla käytettäviin seurantateknologioihin liittyvä henkilötietojen käsittely*, https://finlex.fi/fi/viranomaiset/tsv/2022/20221663. (viitattu 08. 05. 2024).

[21] G. Greenwald ja E. MacAskill, ”NSA Prism program taps into user data of Apple, Google and others”, *The Guardian*, vol. 7, nro 6, s. 1–43, 2013.

[22] FBI, *The China Threat*, https://www.fbi.gov/investigate/counterintelligence/the-china-threat. (viitattu 08. 05. 2024).

[23] A. Hern, *Fitness tracking app Strava gives away location of secret US army bases*, https://www.theguardian.com/world/2018/jan/28/fitness-

tracking-app-gives-away-location-of-secret-us-army-bases. (viitattu 08. 05. 2024).

[24] H. Valkama, *Analyysi: Pitäisikö Tiktok kieltää?*, https://yle.fi/a/74-20068168. (viitattu 08. 05. 2024).

[25] VOA News, *China, Caught Meddling in Past Two US Elections, Claims 'Not Interested' in 2020 Vote*, https://www.voanews.com/a/east-asia-pacific_china-caught-meddling-past-two-us-elections-claims-not-interested-2020-vote/6188474.html. (viitattu 08. 05. 2024).

[26] J. Hara, *Iso osa kansanedustajista kieltäisi Tiktokin – katso, miten oma edustajasi vastasi*, https://yle.fi/a/74-20086759. (viitattu 08. 05. 2024).

[27] C. Mcclain, *A declining share of adults, and few teens, support a U.S. TikTok ban*, https://www.pewresearch.org/short-reads/2023/12/11/a-declining-share-of-adults-and-few-teens-support-a-us-tiktok-ban/. (viitattu 08. 05. 2024).