

# **Kätevyyden hinta: Vertaileva analyysi Googlen, Microsoftin ja Applen tietojenkeräysmenetelmistä**

Tieto- ja viestintätekniiikan tutkinto-ohjelma  
Tietotekniikan laitos, Teknillinen tiedekunta  
Kandidaatin tutkielma

Laatija:  
Valtteri Ingman

Helmikuu 2023

Turun yliopiston laatu järjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu  
Turnitin OriginalityCheck -järjestelmällä.

**Kandidaatin tutkielma**  
**Tietotekniikan laitos, Teknillinen tiedekunta**  
**Turun yliopisto**

**Tutkinto-ohjelma:** Tieto- ja viestintäteknikka

**Tekijä:** Valtteri Ingman

**Otsikko:** Vertaileva analyysi Googlen, Microsoftin ja Applen tietojenkeräysmenetelmistä

**Sivumäärä:** 23 sivua, 4 liitesivua

**Päivämäärä:** Helmikuu 2023

Lukemattomat internetin sivut pidetään käyttäjilleen ilmaisina mainosten ja näiden kohdistamista varten kerätyn datan avulla. Tämä mainosseurannaksi kutsuttu toiminta on kasvavissa määrin tunkeilevampaa ja yksityisyyttä rikkovaa, mikä on saanut ihmiset etsimään anonymiteettiä tukevia vaihtoehtoja internetin eri palveluille.

Jokainen nettiä käyttävä ihminen on tavalla tai toisella tekemisissä joko Applen, Microsoftin tai Googlen kanssa heidän palveluidensa tai käyttöjärjestelmien kautta. Tutkielmassa tehtiin vertaileva analyysi näiden kolmen yrityksen tietojenkeruun kattavuudesta, sekä selvitettiin mahdollisuuksia sen välttämiseen.

Tutkimusmenetelmät koostuivat tietosuojalausekkeiden analysoinneista, lakiasiakirjojen lukemisesta sekä artikkeleista, jotka käsitelivät väliintulohyökkäyksellä seuloottua verkkoliikennettä mainosverkostoille.

Lopputuloksena selvisi, että Google on näistä kolmesta kaikista suurin datan kerääjä. Heidän seurantansa ylittää aina laiterajojen yli, myös silloin kun et omista heidän tiliään. Seuraavaksi eniten kerää Microsoft, mutta heidän seurantansa ja sillä kohdistetut mainokset rajoittuvat vain Windowsin sisälle ja muutamalle heidän omistamalle palvelulleen. Apple kerää pääasiassa vain teknistä dataa, mutta tämä on vähitellen muuttumassa heidän aloitettuaan kohdennettua mainontaa laitteissaan loppuvuodesta 2022.

Mainosseurantaa ei oikeastaan voi mitenkään välttää, nimenomaan juuri Googlen takia. Ainoa asia mitä yksittäinen ihminen voi tehdä, on kiristää yksityisyysasetuksensa ja tehdä vain pakolliset tilit palveluihin.

**Asiasanat:** yksityisyys, mainosseuranta, Google, Microsoft, Apple, profilointi

## Sisällysluettelo

<b>1</b>	<b>Johdanto</b>	<b>1</b>
1.1	Tutkielman tarkoitus	1
1.2	Aiheen rajaus	1
1.3	Mallikäyttäjä	2
1.4	Tutkimuskysymykset	3
1.5	Tutkimusmenetelmät ja tiedonhaku	3
1.6	Tutkielman rakenne	5
<b>2</b>	<b>Mainos seurannan toteutuminen</b>	<b>6</b>
2.1	Applen, Microsoftin ja Google seuranta tietosuojalausekkeiden perusteella	6
2.2	Microsoftin ja Googlen yksityisyyden hallintapaneelit	11
2.3	Windows	14
2.4	Android	14
<b>3</b>	<b>Tulokset ja analyysi</b>	<b>18</b>
3.1	Mobiiliseurannalta suojautuminen DuckDuckGo:lla	18
3.2	Yksityisyyden säilyttäminen internetissä	19
3.3	Sähköpostin yksityisyyden lisääminen	20
<b>4</b>	<b>Yhteenveto</b>	<b>21</b>
4.1	Mallikäyttäjistä tiedetyt tiedot	21
4.2	Voiko mainos seurantaa välttää?	22
4.3	Ongelmat ja jatkotutkimus	22
<b>5</b>	<b>Lainatut lähteet</b>	<b>24</b>
	<b>Liitteet</b>	<b>28</b>
	Liite 1. Esimerkki tyypillisestä Googlen profiloinnista	28
	Liite 2. Windowsin seurannan poisto asennuksen yhteydessä	29
	Liite 3. Chrome selaimen lähettämät tiedot Facebookille	30
	Liite 4. Sopimus Incognin kanssa	31

# 1 Johdanto

## 1.1 Tutkielman tarkoitus

Monet internetin mahdollistamat sivut ja palvelut ovat käyttäjilleen ilmaisia kohdennetun mainonnan ansiosta. Kyseessä on toiminta, jossa digitaalista tuotetta käyttävän henkilön ostoskäyttäytymistä yritetään ennustaa hänestä kerättyjen tietojen avulla. Tätä tietojenkeruuta kutsutaan yleisesti mainos seurannaksi.

Mainos seurannan tungettelevuus ja tätä myötä yksityisyys internetissä ovat huolestuttaneet ihmisiä yhä enemmässä määrin. Varsinkin kun seuranta ei enää rajoitu vain sivustoille, vaan jatkuu tietokoneilta aina kotiemme ulkopuolelle. Älypuhelimemme tietävät, missä olemme ja mihin aikaan päivästä samalla älykellon pitäessä kirjaa terveydentilastamme. Käytännössä jokainen esineiden internetiin yhdistetty laite kertoo jotain tietoa eteenpäin mainostajille.

”Minulla ei ole mitään salattavaa” on yleinen näkökulma, jota kuulee yksityisyydestä keskustellessa. Kaikilla on jotain salattavaa. Googlen entinen toimitusjohtaja Eric Schmidt vihjasi 2009, ettei viattomilla ole mitään piilotettavaa [1]. Viaton Schmidt ei ollut kuitenkaan samaa mieltä asiasta 2005, kun CNET (Computer Network) julkaisi selvityksen hänen tuloistaan, naapurustostaan ja poliittisista lahjoituksistaan [2]. Toinen syy yksityisyyden puolustamiselle on sen kuuluminen samoihin ihmisoikeuksiin sananvapauden kanssa [3]. Ihmisistä kerätyllä tiedolla voidaan asettaa eri ryhmiä eriarvoiseen asemaan sulkemalla heitä yhteiskunnan ja internetin palveluiden ulkopuolelle. Maissa, joissa poliittinen valta on keskittynyt yhdelle taholle, voidaan kerätyllä tiedolla hiljentää oppositio sekä tukahduttaa eriäviä mielipiteitä esittäviä henkilöitä ennen kuin he edes pääsevät ääneen.

## 1.2 Aiheen rajaus

Koska mahdollisia laitteita mainos seurantaan on niin paljon, keskityn vain internetin selaamisessa ja älypuhelimessa tapahtuvaan seurantaan. Internetin selaamisella tarkoitetaan tässä tutkielmassa sekä puhelimella että tietokoneella tapahtuva verkon käyttöä. Verkkosivujen teknillinen toteutus ei juurikaan eroa tietokoneen ja mobiililaitteen välillä, muuten kuin elementtien asettelulta.

Rajaukseen on otettava mukaan myös käyttöjärjestelmä, sillä se on edellytys internetin käytölle tietokoneella, ja tähän olen valinnut Microsoft Windowsin. Valinta perustuu omaan mieltymykseeni, sekä siihen, että Microsoft ei ainakaan toistaiseksi pakota käyttäjiään riippuvaiseksi tuoteperheestään.

Tämä saattaa toki muuttua tulevaisuudessa. Pian julkaistava Windows 11 on vaikeuttanut entisestään Microsoft-tilin välttämistä käyttöjärjestelmän asentamisen yhteydessä. Tili on edellytys muun muassa sovelluskaupan ja Office-tuotteiden käytölle.

Rajaan älypuhelimella tapahtuvan seurannan Android-käyttöjärjestelmään, koska siitä on saatavilla paljon helpommin materiaalia. Nämä kaksi seurannan tapaa ovat myös kaikista yleisimpiä, harvempi käyttää puhelinta ja tietokonetta enempää teknologiaa arjessaan. Aion havainnollistaa Androidin seurantaa vertaamalla sitä iPhoneen kanssa, mutta iPhonea ei sen enempää käsitellä tutkielman rajallisen pituuden vuoksi.

Mainosseurantaa ei voi juurikaan välttää, mutta sitä voidaan kyllä rajoittaa. Vertailemalla Microsoftin ja Googlen tarjoamia keinoja mainosseurannan välttämiseen pyrin osoittamaan, kumpi tekee asian paremmin. Apple on pitkään kunnioittanut käyttäjiensä tietosuojaa, mutta vuoden 2022 lopussa hekin alkoivat kohdistamaan mainoksia. Koska heidän toimistaan ei ole vielä kunnolla tietoa, heille ei ole omaa osuutta omistettu tutkielmassa. Miltä osin tietoa on, se tuodaan esille vertailun vuoksi.

### **1.3 Mallikäyttäjä**

Internet vaatii myös jatkorajauksia sen palveluiden määrän takia. Tutkimuksen pituuden vuoksi oletan yksityisyyttä tavoittelevan mallikäyttäjän, joka käyttää vain välttämättömiä palveluita sujuvan käyttökokemuksen mahdollistamiseksi. Mallikäyttäjä omistaa Google-tilin, joka on edellytys Android-puhelimen käytölle ja Windows-tietokonettaan hän käyttää ilman Microsoft-tiliä. Oletukseen sisältyy, että hän ei käytä tietokoneella mitään sellaisia viihteen tai median palveluita, joihin ei voi kirjautua Microsoftin tai Googlen tunnuksilla.

Sähköpostitileistä huomioidaan vain Microsoftin ja Googlen vaatimat pakolliset sähköpostiosoitteet. Yksi Gmail-tili ja yksi suomalaisen palveluntarjoajan tili Microsoft-tilille. Suomalaisen palveluntarjoajan tili omistetaan viralliseen asiointiin työn ja perheen kanssa, kun taas Gmail-tilillä hän kirjautuu viihteen ja median palveluihin. Hän tekee näin tarkoituksenaan piilottaa Googlelta henkilökohtaiset tietonsa. Samaisesta syystä hän on antanut valheelliset henkilötiedot Microsoftille ja Googlelle. Hänen oikea nimensä ja sukunimensä näkyy vain Microsoft-tilin sähköpostissa.

## 1.4 Tutkimuskysymykset

### Kysymys 1: Mitä tietoja mallikäyttäjistä tiedetään?

On selvää, ettei kukaan käytä vain ja ainoastaan Microsoftin tai Googlen palveluja, mutta näitä kahta yritystä on käytännössä mahdotonta välttää. Vaikka myös Apple on kelvollinen tämän määritelmän mukaan, jätän sen vähemmälle huomiolle, koska heidän tietosuojan rikkeensä ovat olleet varsin vähäisiä. Osittain myös siksi, etten käytä heidän tuotteitaan. Applen tuoteperhettä vasten tehdään kuitenkin vertailuja siltä osin, kuin se on havainnollistamisen kannalta hyödyllistä.

Mallikäyttäjistä kerätyt tiedot tullaan erittelemään Microsoftin sekä Googlen kesken ja selvitän, miten nämä tiedot ylipäättään on saatu. Koska Android noudattaa samaa tietosuojalauseketta kuin Googlen palvelut, alistan sen keräämät tiedot Googlelle.

### Kysymys 2: Voiko mainosseurantaa realistisesti välttää?

Tarkoituksena on selvittää, voiko omat tiedot poistaa helposti internetin välttämättömistä palveluista ja kuinka helppoa tämä loppujen lopuksi on. Kun tähän tavoitteeseen on päästy, pitää selvittää kuinka työlästä anonymiteetin ylläpito on.

## 1.5 Tutkimusmenetelmät ja tiedonhaku

Artikkeleiden löytäminen oli erittäin vaikeaa, melkein mahdotonta. Tutkimusta ei juurikaan ole olemassa mainosprofiloinnin kattavuudesta ja määrästä, koska tätä varten pitäisi päästä käsiksi yritysten palvelimiin. Suurin osa lähteistä koostuukin erinäisistä teknisistä raporteista ja tutkivan journalismin artikkeleista. Vaikka lähteet olivat kaikissa kunnossa ja menetelmät olivat hyvin kuvattu, harvemmin niitä oli vertaisarvioitu. Käyttämäni sosiaalisen median palvelut myös ehdottivat aika ajoin yksityisyyteen liittyvää sisältöä, jossa oli mainittu jokin tutkielman kannalta oleellinen artikkeli tai selvitys.

Web of Science ei tuottanut mitään tuloksia suoraan. Käytin muun muassa termejä: ”privacy pol\*”, ”Microsoft”, ”Google”, ”personal data”, ”data collection”. Yhdistelin näitä eritavoilla and- ja or-operaattoreilla. Mikään vertaisarvioitu artikkeli ei suoraan tuottanut tuloksia liittyen kerätyn henkilökohtaisen datan määrään saati sen yksityiskohtaisuuteen. Myöskään tietoturvalausekkeiden luotettavuudesta ei ole juurikaan tehty tutkimusta. Olennainen tieto oli paljolti valittava aihetta läheisesti sivuavista julkaisuista ja niiden viittauksista. Parhaiten näitä artikkeleja löysi, kun kohdisti

edellä mainitut hakutermit artikkeleiden otsikoihin. Lopputulokseksi sain 24 sopivaa julkaisua, joista kolme osoittautui hyödylliseksi.

Yritysten tietosuojalausekkeiden läpikäynti oli paras keino tiedon hakemiseen yksityisyyttä koskien. Tämä luonnollisesti nostaa kysymyksen siitä, kuinka luotettavia nämä lausekkeet ovat. Niin laillisesti päteviä kuin ne ovatkin, mikään ei estä tarpeeksi isoa yritystä vain valehtelemasta ja toimimasta omaa lausekettaan vastaan. Käytännössä kaikki yritykset sanovat jossain muodossa, että ”me emme myy tietojasi eteenpäin”. Silti he useimmiten toimivat toisin kuin väittävät tulkitsemalla lakia vaihtoehtoisin tavoin ja tämän huomaaminen on usein varsin aikaa vievää. Esimerkiksi Googlea vastaan nostettiin ryhmäkanne 2021 yksityisyysloukkauksista, jotka heidän RTB-järjestelmänsä (Real Time Bidding) mahdollisti. [4] Tästä huolimatta tietosuojalausekkeisiin on pakko uskoa niiden laillisen pitävyyden vuoksi. Lausekkeiden rikkomisesta annetut sanktiot ovat niin isoja, etteivät yritykset uskalla ainakaan suoraan mennä niitä vastaan. Silloinkin kun he uskaltavat, käyttäjien joukosta löytyy aina ihmisiä, joilla on aikaa ja halua lukea lausekkeet huolella läpi. Toinen tekijä mikä sitoo yrityksiä heidän lausekkeisiinsa, ovat tietovuotajat. Riski negatiivisesta julkisuudesta ja tämän mukana tuomista oikeusseuraamuksista on tarpeeksi suuri saamaan yritykset pitämään lupauksensa muun muassa tietojen poistosta (kuva 1).

### Does Google really delete users' account history when they choose to?



**Lalit Kundu**

Software Engineer at Google (company) · Upvoted by Shравan Murali, works at Google (2018-present) Author has **219** answers and **4M** answer views · 5y

Yes. When a user deletes their Google account, there is a period of around a month after which Google completely wipes out all the data related with that certain account, across all Google products.

We have an entire team responsible for ensuring that data deletion requests are upheld by every user facing product, and that too in within a time bound. Getting an approval from this team is necessary for any user facing launch.

However, there might be some data which can't be wiped out completely, for example, financial transactions which Google is bound to maintain records of, for audit purposes. In these cases, we make sure that data is anonymised and bare minimum is held for audit purposes.

Kuva 1: Kuvakaappaus Quora-keskustelupalstalta. Netissä on löydettävissä keskusteluja, joissa mm. Googlen työntekijät myöntävät noudattavansa datan poistopyyntöjä

Viimeisen vuoden aikana suureen suosioon noussut ChatGPT-tekoäly oli myös yksi vaihtoehtoista, jota käytettiin tiedonhaun aikana. Se jouduttiin kuitenkin hylkäämään sen annettua täysin väärää tietoa. Se antoi muun muassa tulokseksi listauksen tunnetun tietoturva-alan tutkijan, Sarah Spiekermannin, ”tutkimuksia”, joita ei ollut olemassa alun alkaenkaan. Se jakoi näennäisesti päteviä linkkejä tieteellisten tietokantojen artikkeleihin, jotka eivät kuitenkaan johtaneet mihinkään kyseisillä sivuilla. Tekoälyn tapa esittää valheellista tietoa totena oli niin vakuuttavaa, että sen tarjoamien tutkimusten olemassaolo oli lopulta pakko varmistaa Spiekermannin sihteeriltä. Näitä papereita ei koskaan ollutkaan olemassa, vaikka henkilö meriitteineen oli todellinen.

Tieteellisten lähteiden puuttuessa erittäin arvokkaaksi osoittautuivat oikeushaasteet. Näihin luottaminen on perusteltua, koska syyttäjän on tehtävä erittäin hyvin taustatyönsä, jotta haasteella on edes mahdollista mennä läpi. Google haastetaan melkein joka vuosi jostakin asiasta tietosuojaan liittyen oikeuteen, tämänkin tutkimuksen aikana heidät haastettiin oikeuteen tammikuussa 2023.

Osallistuin myös TEK:n pitämään seminaariin Hyvä ja paha internet, jossa Mikko Hyppönen kertoi yksityisyydestä ja tietoturvasta internetissä. Luin myös samaista aihetta käsittelevän Hyppösen kirjan, Internet [5].

## 1.6 Tutkielman rakenne

Luvussa kaksi käyn läpi tietosuojalausekkeet Microsoftilta ja Googelta. Applea käsittelem lyhyemmin, koska heidän mainosseurantansa on niin uusi ilmiö. Microsoftilla ja Googella on tietojenkeruun koontinäyttö ja omistan näille luvussa oman kappaleensa, kappaleesta voidaan nähdä kuinka paljon enemmän Google tietää Microsoftiin verrattuna. Käsittelem myös Microsoftin mainosseurantaa, joka tapahtuu käytännössä yksinomaan Windowsin kautta. Lopuksi tiivistän luvussa kaksi Android Data Collection nimisen teknisen raportin sisällön.

Kolmannessa luvussa kerron mobiiliseurannalta suojautumisesta Android-laitteella, esittelen yksityisemmän tavan sähköpostin käyttöön ja kerron miten yksityisyyttä voi verkossa edistää.

Neljäs luku vetää yhteen saadut tulokset. Vastaan tutkimuskysymyksiin ja kerron kohtaamistani ongelmista työn aikana.



## 2 Mainos seurannan toteutuminen

Johdannossa mainitun käyttäytymismetriikan ja palveluihin annettujen henkilökohtaisten tietojen perusteella henkilöstä luodaan mainostunnus, jota myydään mainosverkostoille.

Yksittäinen henkilö ei ole kuitenkaan kovinkaan arvokas, vain 0,0005 \$ [6]. Tämän vuoksi moni sosiaalisen median palvelu on julkaissut erinäisiä tilauspalveluita ilmaisen käyttökokemuksen rinnalle. Kerätty tieto onkin arvokasta vain suurissa massoissa ja mahdollisimman monelle taholle myytyinä. Mainos seuranta toteutetaan pääosin evästeillä, pienillä tekstitiedostoilla, joita verkkosivut lähettävät selaimen välimuistiin. Näiden avulla voidaan muistaa vaikkapa kirjautumistietoja, verkkokaupan ostokoreja taikka sivustoasetuksia. Evästeitä käytetään kuitenkin enemmässä määrin käyttäjien profilointiin, koska evästeillä ei ole mitään rajoituksia siitä mitä tietoa ne voivat lähettää tai tallentaa. Vain hyvin pieni määrä sivustoja ei käytä mitään evästeitä, esimerkiksi duckduckdo.com ja privacytools.io ovat kokonaan evästeettömiä.

### 2.1 Applen, Microsoftin ja Google seuranta tietosuojalausekkeiden perusteella

Niin kutsutuilla FANMAG-yrityksillä on eniten vaikutusta siihen mitä tietoja sinusta kerätään ja miten tätä tietoa myydään eteenpäin. FANMAG on akronyymi siihen kuuluvien yritysten nimistä: ”Facebook, Apple, Netflix, Microsoft, Amazon, Google”. Näistä jokainen kerää evästeitä ja muodostaa sitä kautta mainostunnuksia käyttäjistään, mutta kohtelee käyttäjiensä tietoja hieman eri tavalla. Facebook ja Google rahoittavat toimintansa käytännössä yksinomaan mainoksilla, joten heidän seurantansa on kaikista kattavinta. Microsoft ja Apple ovat ensisijaisesti laitteisto (hardware) ja ohjelmisto (software) kauppiaita, joten heidän tarpeensa käyttäjien seurannalle ei ole läheskään yhtä suuri. Facebook, Netflix ja Amazon jätetään tarkastelun ulkopuolelle, koska ne eivät ole välttämättömiä sujuvan ja esteettömän internetin käytön kannalta. Mainittakoon kuitenkin, että nämäkin yritykset ovat olleet monissa tietoturvakohuissa mukana. Esimerkiksi heinäkuussa 2021 Amazonille langetettiin \$886 miljoonan dollarin sakot tietoturvan laiminlyönnistä [7].

**Applen käytännöt.** FANMAG-yrityksistä Apple on pitkään ottanut tiukan linjan mainonnasta kieltäytymisestä. Heidän brändinsä ylellisyys on antanut heille mahdollisuuden kieltäytyä rahan tekemisestä mainonnan keinoin. Tähän on kuitenkin tulossa muutos, loppuvuodesta 2022 Apple

ilmoitti aloittavansa mainosten näyttämisen osassa palveluistaan ja lisäsi tietoturvalausekkeeseensa mainontaa koskevan lisäosan 12.12.2022 [8].

Vaikka Apple tätä nykyä mainostaakin käyttäjilleen, he vaikuttavat kohtelevan käyttäjiensä yksityisyyttä merkittävästi paremmin kuin Google ja Facebook. Tutkielman kirjoitushetkellä Applella on kaikista yrityksistä lyhyin ja selkein tietosuojalauseke, jossa he tekevät yksiselitteisesti selväksi, etteivät he myy tai jaa käyttäjästä kerättyä tietoa [9]. He noudattavat sijainnista riippumatta Kalifornian CPRA-tietosuojalakia kaikille käyttäjille kaikkialla [10]. Tietosuojalauseke kertookin enemmän siitä mitä he eivät tee, kuin mitä he tekevät [8]:

- ”Mainosalusta ei yhdistä Applen aipeista kerättyjä käyttäjä- tai laitetietoja kolmansilta osapuolilta kerättyihin käyttäjä- tai laitetietoihin mainonnan kohdentamis- tai mittaustarkoituksissa.
- ”Mainosalusta ei myöskään jaa käyttäjä- tai laitetietoja tiedoilla kauppa käyville tahoille.”
- ”Mainosalusta ei rakenna profiileja sijainnista eikä käytä tai säilytä tarkkaa sijaintiasi edes silloin, kun annat jollekin apille luvan käyttää tarkkaa sijaintiasi.”
- ” Applen mainosalusta saa tietoja mainoksista, joita napautat ja tarkastelet, satunnaisen tunnisteen kautta, jota ei yhdistetä Apple ID:hesi.”
- ” Applen mainosalusta ei saa sijaintipohjaisia tietoja, kun laitat laitteesi Sijaintipalvelut pois päältä.”
- ”Voit laittaa Räätelöidyt mainokset pois päältä iOS- tai iPadOS-laitteessa.”

Tutkielman kirjoitushetkellä Applen mainos seuranta on vain noin kolme kuukautta vanha ilmiö, ja oikeustapauksia tässä ajassa on ehtinyt kertyä jo neljä [11], kaikki yksityisyysloukkauksiin liittyen. Ensimmäiset sakot he saivat alle kuukauden sisään tietosuojalausekkeensa muutoksista, kun vain noin kaksi viikkoa myöhemmin joulukuussa 2022 Ranskan tietosuojavaltuusto (CNIL) sakotti Applea kahdeksalla miljoonalla dollarilla. Apple oli laittanut iOS-puhelimissaan mainos seuranta-asetukset valmiiksi päälle ja hankaloittanut näiden asetusten sammuttamista [12]. Lyhyessä ajassa Apple on osoittanut rikkovansa monia yksityiskohtia tietosuojalausekkeessaan, ja oikeustapausten kertyessä luotto heidän muuten selkeään lausekkeeseen menettää arvonsa. On odotettava mihin nämä kanteet lopulta johtavat [12] [13] [14] [15]. Ennen tätä muutosta Applen keräämät tiedot ovat olleet teknisen toiminnallisuuden kannalta välttämätöntä (kuva 2).

App Store, iTunes Store, iBooks Store and Apple Music activity	<input type="checkbox"/>
Apple ID account and device information	<input type="checkbox"/>
Apple Online Store and Retail Store activity	Show more <input type="checkbox"/>
AppleCare support history, repair requests and more	Show more <input type="checkbox"/>
Game Center activity	<input type="checkbox"/>
iCloud Bookmarks and Reading List	<input type="checkbox"/>
iCloud Calendars and Reminders	<input type="checkbox"/>
iCloud Contacts	<input type="checkbox"/>
iCloud Notes	<input type="checkbox"/>
Maps Report an Issue	<input type="checkbox"/>
Marketing subscriptions, downloads and other activity	<input type="checkbox"/>
Other data	<input type="checkbox"/>

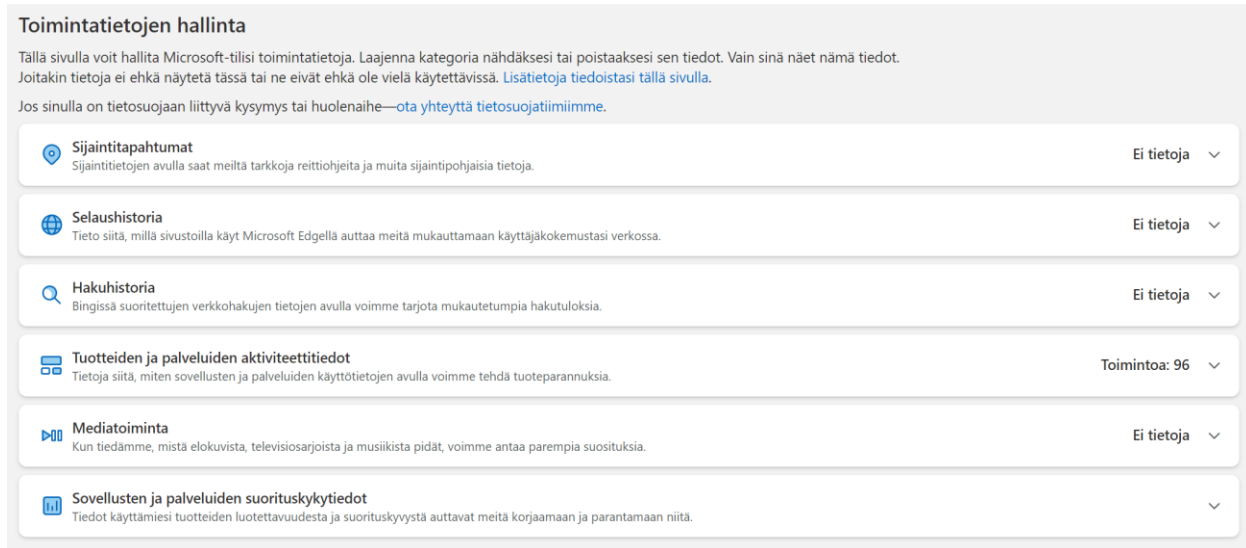
Kuva 2: Kuvakaappaus Applen tietoturvaportaalista. Apple ei ole mainosprofiileja aikaisemmin tehnyt, joten heidän hallussaan olevat tiedot liittyvät tavalla tai toisella heidän laitteidensa normaaliin toimintaan.

**Microsoftin käytännöt.** Microsoft kerää laajasti tietoa käyttäjistään evästeiden ja Windowsin mainostunnuksen avulla [16], lisäksi he ostavat tietoa ulkopuolisilta mainostoimistoilta. Tämä ei kuitenkaan ole välittömästi selvää, kun lukee heidän tietosuojalausekkeensa läpi. He sanovat, etteivät myy henkilökohtaista dataasi, mutta kuitenkin jakavat sen käytännössä jokaiselle, joka heidän kanssaan yhteistyötä tekee. Ainoa tapa tunnuksen vastustamiseen on siitä kieltäytyminen, profilointia kun suoritetaan vain sen ollessa käytössä [17]. Mikäli pidät tämän tunnuksen saatavilla Windowsin asetuksista, annat luvan tietojesi käyttöön 2014 erilaiselle mainostoimistolle ja niiden alaosastoille, joiden kanssa Microsoft on yhteistyössä [18]. Microsoftin ja edellä mainittujen kumppanien näyttämien mainosten joukossa voi olla evästeitä yli 360 erilaista. Moni näistä evästeistä kuuluukin Microsoftin suorille kilpailijoille kuten Amazon, Twitter, Facebook ja Google [19].

Yli kahdentuhannen mainostoimiston ja kolmensadan erilaisen evästeen tietosuojalausekkeiden läpikäynti ei ole uskottavaa keneltäkään. Varsinkaan jos kyseessä on henkilö, joka arvostaa yksityisyyttään. Tämä jättää ainoaksi kannattavaksi vaihtoehdoksi mainostunnuksen keräämisestä kieltäytymisen.

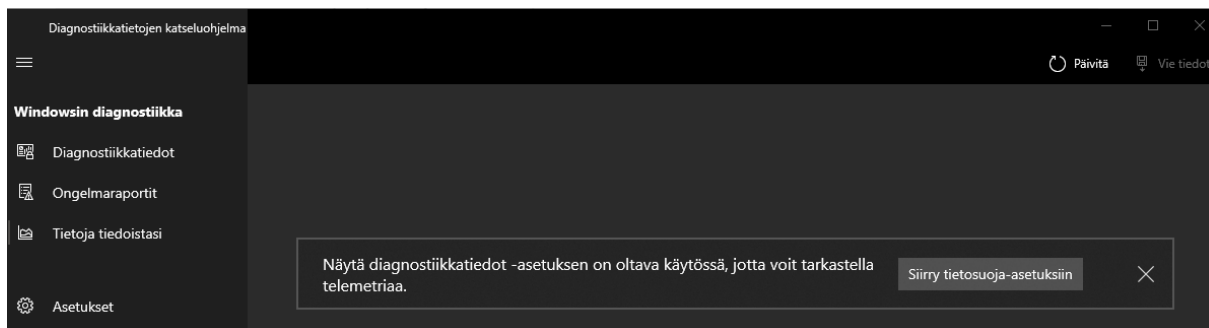
Kaikesta tästä huolimatta Microsoft antaa todella kattavat työkalut mainonnan välttämiseen, sekä kertoo ettei käytä mainonnassa arkaluontoista tietoa kuten henkilökohtaisia keskusteluja tai tiedostoja [20]. Lisäksi he ovat tehneet erittäin helpoksi kieltäytyä käytännössä kaikesta seurannasta Windowsin sisällä, eikä Microsoft-tili ole välttämättömyys arkipäiväisessä internetin tai tietokoneen käytössä. Helpoin tapa Microsoftin seurannan välttämiseen onkin jättää tekemättä tiliä heidän palveluihinsa.

Microsoft tarjoaa yksityisyyden hallintapaneelin (kuva 3), jossa on suurin osa, muttei kaikkea, henkilöstä kerätystä tietoa. Tarkemman tiedot saa ottamalla heihin yhteyttä siihen tarkoitettulla lomakkeella [21].



Kuva 3: Microsoftin toimintotietojen hallintasivu. Seurannasta kieltäytymisellä on havaittavat vaikutukset hallintapaneelissa

Microsoft lisää luotettavuutta Windowsin lähettämästä datasta tarjoamalla diagnostiikkatietojen katseluohjelman (kuva 4). [22]



Kuva 4: Diagnostiikkatietojen katseluohjelma Windowsissa. Mitään tietoja ei lähetetä ellei erikseen sitä salli. Tieto Microsoftin harjoittamasta seurannasta on kuitenkin varsin ristiriitaista. He antavat kattavat työkalut yksityisyyden varjelemiseen, mutta jättävät tämän täysin käyttäjän itse selvitettäväksi. He mahdollistavat Windowsin käytön ilman Microsoft-tiliä, mutta pakottavat sen luonnin asennuksen yhteydessä ellei itse ymmärrä pitää verkkojohtoa irti asennuksen ajan. He antavat yksityisyyden hallintapaneelin käyttöösi, mutta myöntävät ettei sieltä kaikkia tietoja saa. Lisäksi he tallentavat valintasi kohdenneetusta mainonnasta kieltäytymiseen evästeillä, jolloin sinun on kieltäydyttävä

uudelleen, mikäli poistat evästeet [23]. He sanovat, etteivät myy tietojasi kolmansille osapuolille, mutta kuitenkin tekevät yhteistyötä ”luotettavien kumppaneiden” kanssa. Luotettavia kumppaneita on tässä tapauksessa yli 2000, ja niiden läpikäyminen ei ole millään lailla uskottavaa keneltäkään. Varsinkaan kun näihin kumppaneihin sisältyy Facebookin ja Googlen kaltaisia yrityksiä, jotka ovat olleet useamman tietoturvakohun keskellä.

**Googlen käytännöt.** Google on näistä kolmesta yrityksestä hankalin tulkita. Helppolukuinen ja visuaalisesti miellyttävä tietosuojalauseke luo luottamuksen tunnetta, mutta ei kuitenkaan tarjoa riittävää tietoa siitä, mitä tietoja kerätään ja miten niitä käsitellään. Itse asiassa jokaisessa yhteydessä, jossa he sanovat keräävänsä jotakin tietoa, he käyttävät epämääräistä ja kiertelevää termistöä. Tästä osoituksena ovat sanat: ”kuten”, ”esimerkiksi”, ”muun muassa” ja ”saatamme”. On siis syytä olettaa heidän keräävän muutakin kuin sen minkä he suoraan myöntävät. Jättämällä tietoisesti listaamatta ja jaottelematta kaikkia kerättyjä tietoja, he antavat varaa tulkinnalle. Tällaista tulkinnanvaraisuutta ei tulisi olla lakiteksteissä, joiden tulee olla mahdollisimman kattavia ja yksiselitteisiä.

Google vaikeuttaa entisestään lausekkeensa ymmärrettävyyttä linkittämällä tarkemmat tiedot uusille välilehdille, ja täältä aina edelleen alavalikoihin. Tällaista tekstien ristiviittausten aikaansaama epäselkaisuuden määrää mitataan horisontaalisella intertekstuaalisuudella [24]. Tietosuojalausekkeessa ei ole myöskään millään lailla eroteltuna Googlen eri tuotteiden kuten Androidin, Google Driven tai Gmailin tietosuojakäytäntöjä. Erittely heidän palveluidensa käytännöistä poistettiin maaliskuussa 2012 [25]. Näin ollen jokaisen kolmen edellä mainitun palvelun tietosuojalauseke ohjautuu samalle pääsivulle, jossa kerrotaan vain päällisin puolin kerätystä tiedosta.

Mitä enemmän tietosuojalauseke sisältää alidokumentteja, sitä suurempi vertikaalinen intertekstuaalisuus sillä on [24]. Mitä isommaksi yritys kasvaa, sitä vertikaalisemmaksi tulisi heidän tietosuojalausekkeensakin muuttua. Google toimi kuitenkin täysin päinvastoin vuonna 2012. Samana vuonna, jona he alkoivat jakaa keräämäänsä henkilökohtaista dataa kaikkien omistamiensa palveluiden kesken. He pyrkivät tietoisesti epätarkkoihin kuvauksiin toimissaan minimoimalla alidokumenttien määrän (vertikaalisen intertekstuaalisuuden) tietosuojalausekkeessaan ja maksimoimalla siinä olevien linkkien ja ristiviittausten määrän (horisontaalisen intertekstuaalisuuden). Vastaesimerkkinä Microsoftin tietosuojalauseke on erittäin vertikaalinen, koska kaikki heidän palvelunsa ovat yhdellä sivulla ilman, että tarvitsee avata uusia välilehtiä.

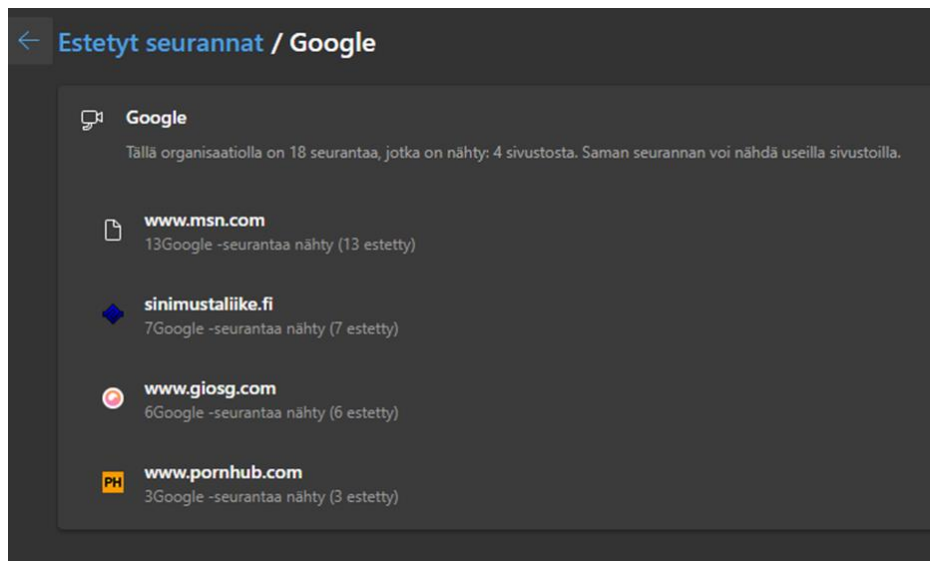
Kun käyttäjä luo Google-tilin, hän antaa automaattisesti hyväksynnän kaikkeen siihen seurantaan, jota Google harjoittaa. Osan näistä oikeuksista voidaan jälkikäteen poistaa, mutta sekin on tehty työlääksi. Tästä tietojen keruun epäselvyydestä ja siitä kieltäytymisen vaikeudesta CNIL antoi Googlelle 50 miljoonan euron sakot alkuvuodesta 2019 [26]. Tämä kieltäytymisen vaikeus toteutuu myös Android-laitetta käyttöön ottaessa, jossa ei anneta vaihtoehtoja omien mainosasetusten säätämiseen. Antamalla lupa kaikkeen Androidin tiedonkeruun kerralla, jättämällä kieltäytymisen vaihtoehdon pois sekä kerätyn tiedon esittämättä jättämisellä Google syylistyy suoraan GDPR-lainsäädännön rikkomiseen [27].

## 2.2 Microsoftin ja Googlen yksityisyyden hallintapaneelit

Samoin kuin Microsoft, Google tarjoaa yksityisyyden hallintapaneelin osoitteessa [myaccount.google.com](https://myaccount.google.com). Kuitenkaan, täällä ei ole kaikkia tietoja keskitettynä ja esimerkiksi Android-puhelimesta on erikseen asetuksista estettävä mainonnan personointiasetukset. Vaikka Google käyttää epäselvää retoriikkaa puhuessaan kerätystä henkilökohtaisesta tiedosta ja sen käsittelystä, on sen lopputulokset kuitenkin selkeästi nähtävillä sivulla [myadcenter.google.com](https://myadcenter.google.com). Täältä voidaan nähdä tavanomaisten tietojen kuten iän, sukupuolen ja kansalaisuuden lisäksi merkittävästi henkilökohtaisempia tietoja. Google tietää parisuhteesi, koulutuksesi, ammattisi, työpaikkasi, harrastuksesi ja varallisuutesi (Liite 1).

Arkaluontoisista tiedoista siellä on nähtävissä muun muassa laihdutatko tai uhkapelaatko. Näihin tietoihin ei heidän omien sanojensa mukaan lasketa seksuaalista tai poliittista suuntautumistasi. Tämä on kuitenkin valetta. Google käyttää arkaluontoista tietoa välillisesti hyväkseen. Esimerkiksi on todennäköistä, että vahvasti uskonnollinen ihminen kannattaa tiettyjä konservatiivisia arvoja. Nämä arvot taas jälleen ohjaavat tämän ihmisen ostoskäyttäytymistä.

Monissa selaimissa on sisäänrakennettuna mainos seurannan estämiseen tarkoitettuja toimintoja. Tutkimuksen aikana palautettiin Edge-selaimen tehdasasetukset ja tehtiin vierailuja sivustoille, joissa Googlen seuranta olisi mahdollisimman haitallista käyttäjän yksityisyydelle. Mikäli Googlen seuranta tällaisilla sivuilla olisi käytössä, tulisi Edgen mainos seurannan eston myös aktivoitua. Näin kokeessa myös tapahtui, kun tehtiin tarkoitushakuisesti vierailuja aikuisviihteen, äärioikeiston ja apteekkien sivuilla (kuva 5).



Kuva 5: Testitulos Edgen mainoseurannan estosta. Googlen evästeet ovat käytännössä jokaisella arkaluontoisella sivulla tavalla tai toisella. Giosg on Googlen kanssa yhteistyötä tekevä suomalainen mainostoimisto, jolla on evästeitä muun muassa Alkon ja Yliopiston apteekin sivuilla.

Microsoftin seurannan hallintapaneeli sisältää varsin pintapuolisesti henkilöstä kerätyt tiedot (Kuva 2). Se ei sisällä esimerkiksi ikää, ammattia, asumismuotoa tai parisuhdetilannetta. Kuitenkin profiilissa olevien tietojen vähäisyys ja tietosuojalausekkeessa esitetyt tiedot ovat ristiriidassa keskenään. Todella moni asia kertoo Microsoftin vastuullisesta tietosuojan kunnioittamisesta, mutta aivan samoissa määrin löytyy vastaesimerkkejä. He myöntävät keräävänsä samoja tietoja kuin Google, mutta korostavat melkein jokaisessa sen tapahtuvan vain heidän tuotteidensa sisällä. Hallintapaneeli antaa ymmärtää, että he eivät tee henkilöistä profiileja mainostarkoituksiin, mutta myöntävät jakavansa kyllä tietojasi mainosverkostojen kesken. Tämä on nähtävissä heidän CCPA-läpinäkyvyysraportistansa [28]. Lisäksi he täydentävät keräämäänsä dataa ostamalla sitä datameklareilta (data brokers).

Varmaksi ei voida sanoa mitä tarkalleen Microsoft tietää jostakin tietystä henkilöstä, muuta kuin sen mitä hallintapaneelissa esitetään. Lisäkysymyksissä ja kattavammissa tietojen selvityksessä, he pyytävät ottamaan yhteyttä heidän tietosuojavaltuutettuun. Näin tutkimuksen aikana toimittiinkin, mutta vastaus ei kertonut mitään uutta verrattuna tietosuojalausekkeeseen:

Hello,

To clarify, when you request an export using our privacy request form, your export data will include any personal data that falls within the following categories: software, setup, and inventory, device connectivity and configuration, feedback and ratings, fitness and activity, support content, support interaction, environmental sensor.

Please note that this will not include data accessible through in-product experiences. You can find more information about data you are able to control directly through apps and services on our [Privacy Frequently Asked Questions \(FAQs\)](#). This will also not include data related to LinkedIn. If you have a LinkedIn account and would like to make a request about that data, you should reach out to LinkedIn [here](#). If you would like to delete your LinkedIn data, please reach out to LinkedIn [here](#).

Once it is available, your data will be available to download as an archive at <https://account.microsoft.com/privacy/download-data>

Please let me know if you have any questions.

Kind Regards,

Carter

Microsoft Privacy

On kuitenkin huomionarvoista, että Microsoft omatoimisesti laajensi GDPR-asetuksen oikeudet koskemaan kaikkia asiakkaitaan maailmanlaajuisesti marraskuussa 2018 [29]. Samaisen lausunnon yhteydessä he julkaisivat yksityisyyden hallintapaneelin kaikkien ihmisten saataville kaikkialle maailmassa. Positiivisen julkisuuskuvan lisäksi he tukivat tällä aikaisempaa lausuntoaan vuodelta 2005, jossa he vaativat kattavaa tietosuojalainsäädäntöä liittovaltiotasolla [30]. Microsoftin sanat ja teot vahvemman tietosuojan puolesta voidaan nähdä yrityksenä horjuttaa Googlen ja Facebookin valta-asemaa. Toisin kuin nämä kaksi yritystä, Microsoft ei ole riippuvainen mainostuloista. Se tekee suurimman osan voitostaan käyttäjärjestelmänsä lisensointisopimuksilla, Xbox-pelikonsoleilla, palvelinratkaisuilla ja muilla laitteistotuotteilla. Vain noin 6 % Microsoftin tuloista tulee mainonnan kohdentamisesta [31]. Microsoft näyttää mainoksiaan vain kolmessa eri palvelussa: ”AOL, Yahoo ja Bing” [32], ja nämä eivät ole välttämättömiä eivätkä kovinkaan yleisiä keskivertokäyttäjän arjessa.



## 2.3 Windows

Windowsin henkilökohtaisen datan keruu on loppujen lopuksi varsin vähäistä. Lähetetystä tiedosta valtaosa on telemetriaa, eli teknistä dataa, joka ei käyttäjälle kerro juurikaan mitään. Tätä käytetään tietoturvaongelmien löytämiseen ja bugien havaitsemiseen. Telemetrian keräämä tieto on eriteltyä sille omistetuille sivulle [33].

Windows antaa mahdollisuuden kieltäytyä käytännössä kaikesta (mainos)seurannasta heti käyttöjärjestelmää asennettaessa (liite 2.), vaikka sillä olisi mahdollisuudet vähintään yhtä kattavaan tietojen keruuseen kuin Googlen tuoteperheellä. Windowsin mainostunnukseen tallennetut tiedot rajoittuvat käytettäväksi vain Windowsin sovelluskaupan tuotteisiin sekä Microsoftin omiin tuotteisiin kuten Edge-selaimen ja Bing-hakukoneeseen. Myöskään seurannasta, telemetriasta tai Microsoft-tilistä kieltäytymisellä ei ole mitään negatiivisia vaikutuksia Windowsin käyttökokemukseen, eikä Microsoft rankaise käyttäjiä, jotka seurannan pyrkivät minimoimaan.

Kun Microsoft omistaa työpöytäkoneista 74.14 % [34], ei heillä ole mitään syytä käyttäjiensä tehovalvontaan, vaikka he siihen pystyisivätkin.

## 2.4 Android

Android ei omista omaa tietosuojalausekettaan, vaan se rinnastetaan Google-tilin kanssa saman lausekkeen piiriin. Googlen keräämän henkilökohtaisen datan myynti ja mainosten kohdentaminen on tuottanut niin paljon erilaista lähdeaineistoa, että siitä saisi ihan oman tutkielmansa. Erilaisia oikeuskanteita, tuomiota ja teknisiä raportteja löytyy runsaasti.

Eräs kattavimpia selvityksiä Androidin seurannasta on tehty 2018 Vanderbiltn yliopistossa. Seuraavat kappaleet tiivistävät Professori Douglas C. Schmidtin viisikymmensivuisen artikkelin pääkohdat. Koko artikkeli on luettavissa ilmaiseksi verkossa ”Digital Content Next”-järjestön julkaisemana [35].

Tämän Androidia käsittelevän osion aikana Schmidtin paperiin viitataan yläindekseillä, jossa numero täsmää artikkelin kappalenumerointiin. Näitä kappaleita on yhteensä 136.

**Suurin osa Androidin tietojenkeruusta tapahtuu ilman käyttäjän vuorovaikutusta<sup>4.a</sup>.**

Käyttäjän oman vuorovaikutuksen perusteella kerätyt tiedot ovat helposti nähtävissä Googlen MyActivity- ja Takeout-sivustoilla. Vähemmän itsestään selvää on passiivisen tiedon keruun määrä, eli tieto, minkä Google saa ilman käyttäjän tietoisia toimia. Tämän selvittämiseksi tutkimusasetelmasa luotiin VPN-yhteys puhelimen ja verkkoyhteyden välille väliintulohyökkäyksen muodossa (man-in-

the-middle attack, MITMA)<sup>128</sup>. Koe kesti 24-tuntia, puhelimen ollessa ilman käyttöä. Android-puhelimessa oli taustalla Chrome-selain ja vertailun vuoksi koe toistettiin iPhonella, jossa oli puolestaan Safari-selain avattuna<sup>22</sup>. MITMA:lla kaapatut tiedostot olivat ".proto"-muotoa, kyseessä on Googlen kehittämän Protobuf -formaatti jäsenneyille datalle. Tämän tiedoston purkaminen paljasti Googlen seuraavan sijaintiasi lähellä olevien Wlan-asemien MAC-osoitteiden perusteella [36]. Protobuf-tiedostojen lähettämän datan erittelystä<sup>129</sup> selviää, että Google pystyy ennustamaan myös liikkeesi tyyppin(kuva 6). Puhelin selvittää nopeutesi ja ennustaa pyöräiletkö, juoksetko vaiko ajatko.

```

"activityReadings": [
  {
    "activities": [
      {
        "confidence": 99,
        "type": "onFoot"
      },
      {
        "confidence": 99,
        "type": "walking"
      },
      {
        "confidence": 1,
        "type": "unknown"
      }
    ],
    "timestampMs": 1527095517507
  },

```

Kuva 6: Protobuf-tiedosto purettuna ihmiselle luettavaan muotoon. Käyttämällä puhelimen sisäänrakennettuja sensoreita, Android lähettää prosentuaalisen arvion henkilön liikkeen tyyppistä.<sup>20</sup>

Google saa myös sijaintitietosi paikannuspalveluiden ollessa pois päältä. He pystyvät seuraamaan sijaintiasi vaikka puhelimesiasi ei ole SIM-korttia, Wlan-yhteys sammutettuna, mobiilidata pois päältä ja lentokonetila käytössä. Android kerää nämä tiedot siinä missä normaalistikin, mutta kun lopulta joudut nettiyhteyttä käyttämään, lähetetään kerätyt tiedot Googlelle [37].

Passiivisen tietojenkeruun kokeessa havaittiin Googlen seuraavan myös iPhonea. Sijaintitietoja Google ei kerännyt, mutta mainostajille tietoa kyllä lähetettiin 152 kilotavua<sup>fig.6</sup>. 152 kilotavua \* 1024 = 155648 tavua. Yksi megatavu tekstiä on 1200 merkkiä ilmitekstiä (plain text) [38]. Vaihtamalla megatavut tavuiksi saadaan 1200/1 000 000=0,0012 merkkiä per tavu. Lopuksi kertomalla 155648\*0,0012 päästään ≈187 merkkiin. iPhonelta lähtee siis ilman käyttäjän vuorovaikutusta noin kahden virkkeen verran dataa Googlelle päivässä. iPhoneen yhteydenotot Googlen suuntaan tapahtuivat

noin kerran tunnissa (0,73 pyyntöä per tunti).

Android lähetti tietoa 40,2 kertaa tunnissa, jonka lopputuloksena oli 4,4 megatavua päivässä. Näistä megatavuista 31 % oli sijaintitietoja päivän aikana ja mainostajiin otettiin yhteyttä 1,2 kertaa tunnissa. Edellistä kaavaa soveltamalla saadaan 1637 merkkiä ilmitekstiä, tai puoli sivua tämän dokumentin putkeen kirjoitettua tekstiä sijaintitietoja päivässä. Mainostajille lähetetyn datan tavumäärä päivässä oli pyöristetty nolnaan, mutta vain siksi koska kyseessä oli koe passiivisesta datan keruusta. Passiivisessa datassa onkin paljon tärkeämpää se missä mahdolliset asiakkaat ovat milläkin hetkellä, kuin mitkä heidän kiinnostuksen kohteensa ovat.

Mikko Hyppösen mukaan Google maksaa Applle yli kaksi miljardia vuodessa, jotta Google pysyy Applen vakioselaimena [39], sekä pitääkseen Applen kehittämästä omaa kilpailevaa selainta. Tämän kokeen tulokset vahvistavat Hyppösen sanat, lisäksi asiasta on nostettu joukkokanne Googlea vastaan [40].

### **Google pystyy seuraamaan Androidin tai iPhoneen käyttäjää, vaikkei hän käyttäisi mitään Googlen palveluista<sup>4.e,4.f</sup>.**

Kuten edellisessä luvun kokeessa osoitettiin, Google seuraa myös iPhoneen passiivista verkkoliikennettä. Kun koe toistettiin aktiivisella käytöllä, pyrittiin käyttämään Googlen tuotteita niin vähän kuin mahdollista<sup>60</sup>. Ainoa sallittu Googlen tuote oli Chrome-selain. Kokeen päätyttyä oli Android puhelimen sijainti haettu ~450 kertaa (19 kertaa/tunti), kun taas iPhone paikannettiin ~12 kertaa päivän aikana, tai kerran kahden tunnin välein<sup>fig.12</sup>.

Vaikka Google sai iPhoneen sijainnin vain muutamia kertoja Androidiin verrattuna, molemmat puhelin tyypit ottivat Googlen mainosalustoihin suunnilleen saman verran yhteyttä. Android 42 kertaa ja iPhone 45 kertaa.

Kuitenkaan Applen omiin mainosalustoihin ei otettu kertaakaan yhteyttä iPhone puhelimesta. Tämä oli siis vuonna 2018, koe olisi syytä toistaa näin Applen mainontakäytännön muututtua.

### **Googlen pystyy profiloimaan anonyymien käyttötietojen yksittäisiin ihmisiin<sup>4.g</sup>.**

Vaikka evästein kerätty tieto onkin anonyymiä, Google pystyy yhdistämään yksittäisen henkilön kerättyihin tietoihin Androidin lähettämien tunnistetietojen avulla. Tällaisia tunnistetietoja ovat muun muassa IP-osoite, IMEI-koodi, MAC-osoite sekä joukko Googlen itsensä kehittämiä tunnisteteita<sup>table 1</sup>.

Google myöntää tekevnsä tätä tietosuojalausekkeessaan, tosin ilman aihetta käsittelevää alaotsikkoa ja linkin taakse piilotettuna [41]. Osaa tästä tunnisteilla yhdistetystä datasta voi hallita ”Toiminnan hallinta”-sivulla<sup>1</sup>, joka myöskään ei ole selkeästi näkyvässä vaan se on erikseen ymmärrettävä hakea Google-tilin asetuksista<sup>2</sup>. Raportti sisältää myös tarkemman kuvauksen anonyymien datan profiloinnin teknisestä puolesta<sup>44</sup>.

Luvussa 1.5 mainitaan Googlea vastaan nostettu joukkokanne, joka osoittaa miten RTB-järjestelmä mahdollistaa yksittäisen henkilön profiloinnin väitetysti anonyymista datasta.

---

<sup>1</sup> <https://myactivity.google.com/activitycontrols?pli=1>

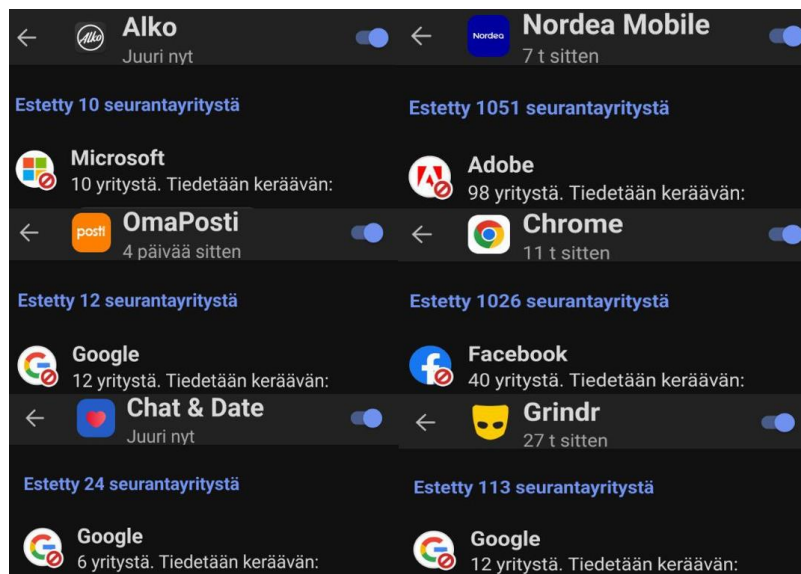
<sup>2</sup> [https://myaccount.google.com/?utm\\_source=my-activity&utm\\_medium=logo&hl=fi](https://myaccount.google.com/?utm_source=my-activity&utm_medium=logo&hl=fi)

### 3 Tulokset ja analyysi

#### 3.1 Mobiiliseurannalta suojautuminen DuckDuckGo:lla

”Google data collection”-raportissa esitettiin, kuinka väliintulohyökkäyksellä onnistuttiin suodattamaan iPhoneen ja Androidin Googlelle lähettämää dataa. Molemmat puhelimet sisältävät valmiiksi mahdollisuuden VPN-yhteyden muodostamiseen. Koeasetelmassa puhelimet yhdistettiin internetiin MITMA-saastuneen VPN-palvelimen kautta.

DuckDuckGo (DDG) on samannimistä yksityistä hakukonetta tarjoava yritys, jolla on myös mobiiliselain Androidille ja iPhoneille. Androidille tarjotussa mobiiliselaimessa on lisäosa, joka estää sovelluksia lähettämästä henkilökohtaista dataa mainostajille (kuva 7). Se toimii väliintulohyökkäyksen lailla asettaen itsensä VPN-yhteyden tilalle ja estämällä mainostajille hyödyllisen liikenteen laitteesta pois.



Kuva 7: Tuloksia DuckDuckGo:n mainos seurannan estosta. Tutkimusta varten asennettiin monia sovelluksia, joiden keräämä tieto olisi mahdollisimman arvokasta mainostajille. Googlen ja sen kanssa yhteistyötä tekevät tahot ovat läsnä kaikessa mitä puhelimella teet.

Olellaisena nostona kuvan 7 sovelluksista on Alkon ja Postin sovellukset. Postin tietosuojalauseke myöntää lähettävänsä tietojasi ulkomaille, mikäli tietojen vastaanottajat ovat allekirjoittaneet ”EU-komission hyväksymät vakiolausekkeet sisältävän sopimuksen” [42]. Alko väittää ettei

”Henkilötietojasi ei luovuteta käsiteltäväksi Euroopan unionin ja Euroopan talousalueen ulkopuolelle”

[43]. Nämä voidaan molemmat tulkita valheeksi.

Googlen tietosuojalausekkeessa ei missään kohtaan mainita sanaa ”GDPR”, eivätkä he suoraan myönnä sitä noudattavansa. He puhuvat vain yleisesti ”Euroopan unionin (EU:n) tai Yhdistyneen kuningaskunnan tietosuojalainsäädännöstä”, jonka perusteella he antavat käyttösi yksityisyyden hallintapaneelin [44]. He eivät teknisesti valehtele, mutta eivät he tottakaan puhu.

Alkon tietosuojalauseke valehtelee käyttäjälleen. DuckDuckGo:n sovellusten seurantasuojaus osoittaa, että Microsoft, Euroopan talousalueen ulkopuolisena yrityksenä, kerää heidän sovelluksensa kautta tietoja.

Tarkemmin julkisen sektorimme sovellusten tiedonkeruusta ja kyseenalaisista tietoturvakäytännöistä on tehty Turun Yliopistossa. Hekin käyttivät samanlaista MITMA-analyysiä tulosten saamiseksi [45].

### 3.2 Yksityisyyden säilyttäminen internetissä

Aikaisemmissa kappaleissa osoitettiin, kuinka Google ja heidän mainosverkostonsa ovat väistämättömästi läsnä internetissä. Kaikista älypuhelimista Androideja oli vuoden 2022 toisella neljänneksellä 72 % ja vuoden 2021 lopussa kolme miljardia [46]. Kun vielä huomioidaan, että Googella on todistetusti kyky seurata myös Applen puhelimia, on todellisen yksityisyyden saavuttaminen käytännössä mahdotonta.

Toki on olemassa monia äärimmäisyyksiin meneviä keinoja niille, jotka pyrkivät todelliseen anonymiteettiin, mutta siihen vaadittava aika ja vaiva ei ole monenkaan peruskäyttäjän kannalta uskottavaa. Ainoa mitä peruskäyttäjä voi realistisesti tehdä, on minimoida tätä seurannan määrää selain valinnoilla, hakukoneilla, selainlaajennuksilla ja tietosuoja-asetusten kiristämällä.

Tammikuussa 2023 Yhdysvaltain oikeusministeriö (Department of Justice) julkaisi 140-sivuisen haasteen Googlea vastaan heidän monopoli asemansa väärinkäytöstä [47]. Siinä missä yksittäisen ihmisen keinot ovat vähäiset, ovat vastaavat oikeustapaukset paras keino yksilön tietosuojan edistämiseksi. Vaikka olisitkin valmis elämään täysin Googletonta elämää, se ei tule onnistumaan. Heidän mainoskumppaninsa yltyvät lähes jokaiselle mainossivulle ja vaikka estäisit kaikki mainontaan käytettävät evästeet, Google pystyy silti tunnistamaan sinut älylaitteiden lähettämien tunnisteiden avulla. Alla lainaus Hyppösen yrityksestä elää ilman Googlea:

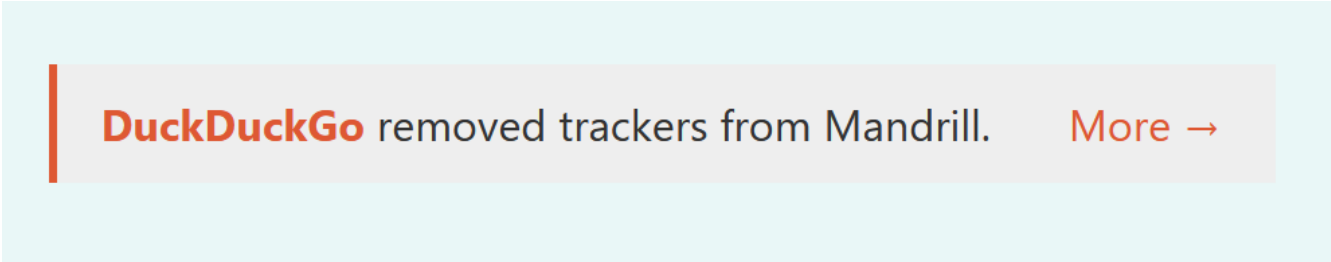
Testasin pari vuotta sitten elämää ilman Googlea. Se ei onnistunut. Google-haun korvaaminen muilla hakukoneilla oli vielä helppoa. Samoin Googlen selaimelle ja kännykkäjärjestelmälle löytyi korvaajia, mutta Googlen mainokset ja analytiikat löytyvät melkein joka verkkosivulta. YouTubea on vaikea välttää, samoin karttoja ja

toimistosovelluksia. Googlella on töissä huippuosaajia, ja heidän tuotteensa ovat todella hyviä. Toivoisin vain, että voisin maksaa niistä rahalla, sen sijaan että minun pitää maksaa niistä yksityisyydelläni. -Mikko Hyppönen, Internet, s.164

### 3.3 Sähköpostin yksityisyyden lisääminen

Siinä missä evästeillä seurataan käyttäytymistämme verkossa, myös sähköpostejamme seurataan mainosanalytiikalla. Esimerkiksi ostettuasi jotain netistä, saattaa kuitenkin mukana vastaanottajalle näkymättömiä seurantapikseleitä. Mainostajat käyttävät näitä markkinointinsa tehokkuuden selvittämiseen mittaamalla muun muassa laitteen, jolla viesti katsottiin, kauanko viesti oli auki, mitä linkkejä avattiin ja montako kertaa viesti avattiin.

Tämä on myös yksi tapa miten ihmiset joutuvat roskapostiyrietysten postituslistoille. On täysin mahdollista ohjelmoida seurantapikseliin lyhyt ohjelmakoodi, joka lähettää viestin avanneen ihmisen sähköpostiosoitteen eteenpäin. Sähköpostiohjelmat estävät kuvien lataamisen oletuksena juuri tästä syystä. Asiaa vastaan on myös jälleen kerran monia ilmaisia palveluja. Yksi tällainen on DuckDuckGo:n tarjoama sähköpostisuojaus, jossa yhdistät sähköpostisi heidän tarjoamaan osoitteen kanssa. DDG:n sähköpostiin lähetetyt viestit seulotaan seurantapikseleiltä ja välitetään eteenpäin alkuperäiseen sähköpostiisi ilman seurantaa(kuva 8).



**DuckDuckGo** removed trackers from Mandrill. [More →](#)

Kuva 8: DuckDuckGon:n mainosseurannan eston leima. DDG:n suodattamissa sähköposteissa näytetään poistetut seurantaominaisuudet.

Henkilön sähköpostiosoite on yksi yleisimmistä tiedoista, joihin datameklarit pääsevät käsiksi. Kun saman sähköpostiosoitteen tunnistaa useassa palvelussa, ei ole vaikeaa selvittää millainen ihminen on kyseessä. Tätä sähköpostin kautta tapahtuvaa profiloointia voi vähentää Incogni nimisen palvelun avulla. Kuukausimaksua vastaan he ottavat lakiteitse yhteyttä datameklareihin ja tietokantojen ylläpitäjiin ja vaativat tietojesi poistamista antamaasi sähköpostiosoitetta vastaan. Liitteessä 5 on nähtävissä sopimus, jonka Incognin kanssa allekirjoitat. Sopimuksen luonteen ja sitovuuden takia ei ole mahdollista vaihtaa sähköpostiosoitetta, jonka tilin luonnin yhteydessä valitset.

## 4 Yhteenveto

Tutkimuksessa selvitettiin kolmen FANMAG-yrityksen harjoittamaa mainosseurantaa ja siihen liittyvää profilointia peruskäyttäjän arjessa. Yrityksistä valittiin Apple, Google ja Microsoft, koska heidän tarjoamat laitteistot ja ohjelmistot ovat välittömästi läsnä meidän kaikkien arjessa. Kun seurannan kattavuutta jaoteltiin, selvisi Googlen osuus olevan ylivoimaisesti suurin. Heti perässä seurasi Microsoft ja vähiten tietoa oli Applella.

Koska tutkimusta teknologian suuryritysten tietojenkeruun määrästä ja tarkkuudesta ei juurikaan ollut, piti tieto hankkia muista lähteistä. Näitä lähteitä olivat oikeushaasteet, tietosuojalausekkeet, tutkivan journalismin artikkelit, tekniset raportit, omien sekä muutamien tuttavieni tietosuojan koontinäytöt, viestit Microsoftin tietosuojavaltuutetun kanssa ja omien tietojen pyyntö Microsoftilta ja Googlelta. Osallistuin myös Mikko Hyppösen Hyvä ja paha internet-seminaariin, sekä luin samaista aihetta käsittelevän kirjan nimeltä Internet.

### 4.1 Mallikäyttäjistä tiedetyt tiedot

Johdannossa esitellystä mallikäyttäjistä ylivoimaisesti eniten tietää Google, vaikka tämä ei käyttäisi mitään heidän palvelujaan. Google tarjoaa My Ad Center-palvelun, josta varsin suuri osa tiedoista on saatavilla. Täältä löytyy tietoja kuten ikä, koulutus, työpaikka, sukupuoli, asumismuoto, addiktiot (tupakka, alkoholi, uhkapelaaminen), perhestatus, kansalaisuus, puhutut kielet, kiinnostuksen kohteet, kannatetut brändit ja monta muuta. Koska Googlen evästeet yltyvät niin poliittisille, uskonnollisille, kuin pornografisille sivustoille, on syytä uskoa heillä olevan tietoa myös näihin liittyen. Vaikka he eivät tätä mainoskeskuksessa näytäkään.

Google seuraa myös älypuhelimia. Yllättäen myös iPhonea, jossa ei ole mitään Googlen sovelluksia. Yksi eniten kerätty tieto oli laitteen sijainti, jonka Google saa Android-puhelimesta vaikka mobiilidata, wifi ja GPS-palvelu olisi pois päältä. Edes lentokonetilan käyttäminen tämän lisäksi ei estä sijainnin saamista.

Microsoft tarjoaa samanlaisen hallintapaneelin omien tietojen tarkasteluun. Yhteenvedosta ei paljastu lähellekään yhtä paljon tietoja kuin Googlen vastaavasta, joskin Googlen hallintapaneelin henkilökohtaisuus luo epäluottamusta Microsoftin keräämän tiedon rehellisyydestä. Voidaanko Microsoftiin luottaa, kun pyydät heiltä yhteenvedon heidän keräämistään tiedoista tai kun tarkastelet



tietojasi heidän hallintapaneelisti? Toisaalta Microsoftin tuloista 94 % tulee laitteistoista ja pilvipalveluista, joten heidän ei tarvitse harjoittaa kattavaa seuranta käyttäjistään. Lisäksi Microsoftin käyttämä profiloinnin mainostunnus on olemassa vain Windowsissa ja sen pohjalta näytetyt mainokset näkyvät vain Bing-selaimessa, Yahoo- ja AOL-sivuilla sekä sovelluskaupan ohjelmistoissa. Windowsissa on myös suhteellisen helppo poistaa mainostunnus sekä seurantaominaisuudet käytöstä ja jos näin teet, he eivät rankaise käyttäjää tästä mitenkään.

Apple on tyypillisesti ottanut käyttäjiensä yksityisyyden vakavasti, koska heillä on siihen ollut varaa. Heidän laitteidensa korkeat hinnat ovat mahdollistaneet heidän kieltäytyä käyttäjiensä datan myymisestä. Tähän periaatteeseen tuli kuitenkin muutos loppuvuodesta 2022 ja vain parissa kuukaudessa Apple on saanut ainakin neljä kappaletta lakihaasteita käyttäjiensä tietosuojan laiminlyönnistä. Tietoa Applen profiloinnista ei siis toistaiseksi ole tarpeeksi tutkielman kirjoitushetkellä ja aika näyttää mitä muutoksia lakihaasteet Applen toimintaan tuovat. Yksi oletettavasti tuleva muutos on vastaava koontinäyttö kuin Googella ja Microsoftilla. Tähän mennessä heillä on ollut vain tietoa sovellusten käyttöön liittyen, kuten muistiinpanoja, yhteystietoja, tilauksia tai ladattuja sovelluksia.

## **4.2 Voiko mainosseuranta välttää?**

Ei. Suurimpana syynä tähän on Google, jonka mainosverkostot ylittävät ylilaiterajojen. Ei ole merkitystä mitä selainta tai laitetta käytät, Google tietää sinusta aina jotain. Jos käyttämäsi laite on yhteydessä internetiin, on erittäin todennäköistä, että Google tai joku heidän mainosverkostoistaan on datan vastaanottajana. Ainoa mitä voit tehdä, on rajoittaa tätä seurannan määrää niillä keinoilla mitä siihen annetaan ja luottaa CPRA:n ja GDPR:n kaltaisten tietosuojalakien tekevän tehtävänsä.

## **4.3 Ongelmat ja jatkotutkimus**

Suurin ongelma oli aiheen laajuus. Tiesin kyllä, että Googella on suuri valta elämästämme ja yksityisyydestämme, mutten käsittänyt ennen tätä kuinka paljon se oikeasti on. Googlea vastaan on nostettu niin paljon syytteitä vuosien saatossa, että jo pelkästään niitä analysoimalla olisi saanut todella paljon aikaa. Esimerkiksi RTB-järjestelmästä ei tullut kirjoitettua käytännössä mitään, vaikka siihen löytyi erinomainen 150-sivuinen lakidokumentti.

Positiivisiakin yllätyksiä tuli vastaan. Olen kuullut monesti kuinka Windows on ” urkintaohjelmisto”, jota tulisi välttää kaikin keinoin. Mutta kun olin lukenut heidän tietosuojalausekkeensa läpi, todennut kuinka helpoksi he tekevät telemetriasta ja mainostunnuksesta kieltäytymisen ja kuinka mainostunnus on vain Windowsin sisäinen ominaisuus, en olisi turhan huolissani. Microsoft on rakentanut niin ison valta-aseman käyttöjärjestelmällään, että sen totaalinen pilaaminen Googlen tasoisella urkinnalla ei olisi millään lailla kannattavaa.

Jatkotutkimuksena maisterivaiheeseen voisin keskittyä vain Windowsin tietojenkeruuseen. Haluan selvittää, olenko oikeassa luottaessani siihen, vai onko kyseessä vain tämä tutkielman aiheuttama ajatusvinouma. Käyttäisin samanlaista väliintulohyökkäys-analyysiä, kuin Turun Yliopistossa tehdyssä tutkimuksessa julkisen sektorin mobiilisovellusten yksityisyydestä. Kyseinen menetelmä tuli jopa kolme kertaa vastaan tutkimustyön aikana, joten sen soveltaminen olisi sopiva myös Windowsin verkkoliikenteen selvittämiseen.

## 5 Lainatut lähteet

- [1] CNBC, "Google Chairman Eric Schmidt - CNBC Interview," 11 12 2009. [Online]. Available: [https://www.youtube.com/watch?v=BreJfzpbwm0&ab\\_channel=ScroogledTruth](https://www.youtube.com/watch?v=BreJfzpbwm0&ab_channel=ScroogledTruth). [Haettu 22 2 2023].
- [2] C. Elinor Mills, "Google balances privacy, reach," 3 8 2005. [Online]. Available: <https://www.cnet.com/tech/services-and-software/google-balances-privacy-reach-1/>. [Haettu 22 2 2023].
- [3] united nations, "Universal Declaration of Human Rights, Article 12," [Online]. Available: <https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf>. [Haettu 22 2 2023].
- [4] u. s. d. court, "documentcloud.org," 5 5 2021. [Online]. Available: <https://www.documentcloud.org/documents/21046592-google-do-not-sell-lawsuit>. [Haettu 21 1 2023].
- [5] M. Hyppönen, Internet, Helsinki: WSOY, 2022.
- [6] T. M.-D. C. C. Lukasz Olejnik, "Selling Off Privacy at Auction," 2013. [Online]. Available: <https://hal.inria.fr/file/index/docid/915249/filename/SellingOffPrivacyAtAuction.pdf>. [Haettu 14 2 2023].
- [7] B. Standard, "Amazon hit with \$886 million European Union data privacy fine," 30 7 2021. [Online]. Available: [https://www.business-standard.com/article/technology/amazon-hit-with-886-million-european-union-data-privacy-fine-121073001176\\_1.html](https://www.business-standard.com/article/technology/amazon-hit-with-886-million-european-union-data-privacy-fine-121073001176_1.html). [Haettu 9 1 2023].
- [8] Apple, "Apple Advertising & Privacy," 12 12 2022. [Online]. Available: <https://www.apple.com/au/legal/privacy/data/en/apple-advertising/>. [Haettu 9 1 2023].
- [9] Apple, "Apple does not sell your personal data including as "sale" is defined in Nevada and California. Apple also does not "share" your personal data as that term is defined in California.," 22 12 2022. [Online]. Available: <https://www.apple.com/legal/privacy/en-ww/>. [Haettu 7 1 2023].
- [10] Greenberg Traurig, "'Share," "shared," or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business," 1 1 2023. [Online]. Available: <https://cpra.gtlaw.com/definitions/>. [Haettu 1 7 2023].
- [11] appleinsider, "Fourth class-action lawsuit filed against Apple for alleged privacy violations," 30 1 2023. [Online]. Available: <https://appleinsider.com/articles/23/01/30/fourth-class-action-lawsuit-filed-against-apple-for-alleged-privacy-violations>. [Haettu 2 2 2023].
- [12] C. n. d. l. e. d. libertés, "sanction de 8 millions d'euros à l'encontre de APPLE DISTRIBUTION INTERNATIONAL," 4 1 2023. [Online]. Available: <https://www.cnil.fr/fr/identifiant-publicitaire-sanction-de-8-millions-deuros-lencontre-de-apple-distribution-international>. [Haettu 2 2 2023].

- [13 United States District Court of California, "Julia Cima vs APPLE INC.," 26 1 2023. [Online]. Available:  
] <https://www.scribd.com/document/622815920/Apple-Privacy-Lawsuit-4#>. [Haettu 27 2 2023].
- [14 United States District Court of Pennsylvania, "Joaquin Serrano vs APPLE INC.," 6 1 2023. [Online].  
] Available: <https://www.scribd.com/document/618921921/Serrano-vs-Apple-Privacy-Class-Action>. [Haettu  
27 2 2023].
- [15 United States District Court of New York, "Barry Robinson vs APPLE INC.," 2 2 2023. [Online].  
] Available: <https://www.classaction.org/media/robinson-v-apple-inc.pdf>.
- [16 Microsoft, "Windows generates a unique advertising ID for each person using a device, which app  
] developers and advertising networks can then use for their own purposes," 1 11 2022. [Online]. Available:  
<https://privacy.microsoft.com/en-us/privacystatement>. [Haettu 2 1 2023].
- [17 Microsoft, "Microsoft collects the advertising ID for the uses described here only when you choose to enable  
] the advertising ID as part of your privacy setting.," 1 11 2022. [Online]. Available:  
<https://privacy.microsoft.com/en-us/privacystatement>. [Haettu 2 1 2022].
- [18 Microsoft, "Partner directory," [Online]. Available: [https://about.ads.microsoft.com/en-  
\] us/resources/microsoft-advertising-partner-program/partner-  
directory?Filter=1&page=1&Filter\\_Services=&Filter\\_Location=&Filter\\_Industry=&Filter\\_PartnerType=&F  
ilter\\_SearchText=](https://about.ads.microsoft.com/en-us/resources/microsoft-advertising-partner-program/partner-directory?Filter=1&page=1&Filter_Services=&Filter_Location=&Filter_Industry=&Filter_PartnerType=&Filter_SearchText=). [Haettu 8 1 2023].
- [19 Microsoft, "Third party cookie inventory," [Online]. Available: [https://support.microsoft.com/en-  
\] us/topic/third-party-cookie-inventory-81ca0c3d-c122-415c-874c-55610e017a6a](https://support.microsoft.com/en-us/topic/third-party-cookie-inventory-81ca0c3d-c122-415c-874c-55610e017a6a). [Haettu 8 1 2023].
- [20 Microsoft, "Microsoft does not use what you say in email, chat, video calls, or voice mail, or your  
] documents, photos, or other personal files to target ads to you.," [Online]. Available:  
<https://privacy.microsoft.com/en-us/privacystatement>. [Haettu 8 1 2023].
- [21 Microsoft, "Report a Privacy Concern," [Online]. Available: [https://www.microsoft.com/fi-  
\] fi/concern/privacy?ref=amc.privacy-landing?ref=amc.privacy-landing](https://www.microsoft.com/fi-fi/concern/privacy?ref=amc.privacy-landing?ref=amc.privacy-landing). [Haettu 8 1 2023].
- [22 Microsoft, "Diagnostiikkatietojen katseluohjelman yleiskatsaus," [Online]. Available:  
] <https://learn.microsoft.com/fi-fi/windows/privacy/agnostic-data-viewer-overview>. [Haettu 8 1 2023].
- [23 Microsoft, "If you opt out of interest-based advertising, we store your opt-out preference in a cookie on  
] your device.," [Online]. Available: <https://privacy.microsoft.com/en-us/privacystatement>. [Haettu 9 1 2023].
- [24 B. Valtysson, R. F. Jørgensen ja J. L. Munkholm, "Unpacking Google's privacy policy and terms of  
] service," 2021. [Online]. Available: <https://sciendo.com/pdf/10.2478/nor-2021-0033>. [Haettu 25 1 2023].
- [25 T. Verge, "Google's controversial new privacy policy now in effect," 1 3 2012. [Online]. Available:  
] <https://www.theverge.com/2012/3/1/2835250/google-unified-privacy-policy-change-take-effect>. [Haettu 25

1 2023].

- [26 E. D. P. Board, "CNIL imposes a financial penalty of 50 Million euros against GOOGLE," 21 1 2019. [Online]. Available: [https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros\\_en](https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en). [Haettu 25 1 2023].
- [27 E. unioni, "GDPR-lain määritelmä suostumuksen annolle,," [Online]. Available: <https://gdpr.eu/gdpr-consent-requirements/>. [Haettu 2023 1 25].
- [28 Microsoft, "CCPA transparency report," 1 12 2022. [Online]. Available: <https://privacy.microsoft.com/en-us/ccpa>. [Haettu 1 2 2023].
- [29 Microsoft, "Microsoft's commitment to GDPR, privacy and putting customers in control of their own data," 21 5 2018. [Online]. Available: <https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/>. [Haettu 2 1 2023].
- [30 Microsoft, "Microsoft Advocates Comprehensive Federal Privacy Legislation," 3 11 2005. [Online]. Available: <https://news.microsoft.com/2005/11/03/microsoft-advocates-comprehensive-federal-privacy-legislation/>. [Haettu 1 2 2023].
- [31 K. Franek, "Microsoft Revenue Breakdown," 30 9 2022. [Online]. Available: <https://www.kamilfranek.com/microsoft-revenue-breakdown/>. [Haettu 2 1 2023].
- [32 Microsoft, "About ad distribution," [Online]. Available: <https://help.ads.microsoft.com/#apex/ads/en/50871/0>. [Haettu 1 2 2023].
- [33 Microsoft, "Yhteenveto Windowsin tietojen keräämisestä," 1 10 2022. [Online]. Available: <https://privacy.microsoft.com/fi-FI/data-collection-Windows>. [Haettu 5 2 2023].
- [34 Statcounter.com, "Desktop Operating System Market Share Worldwide," 1 1 2023. [Online]. Available: <https://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-202301-202301-bar>. [Haettu 1 1 2023].
- [35 V. U. Professor Douglas C. Schmidt, "Google Data Collection," 15 8 2018. [Online]. Available: <https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf>. [Haettu 7 2 2023].
- [36 Eshter, "Eshter codes," 1 20 2018. [Online]. Available: <https://web.archive.org/web/20180213201547/https://esther.codes/reverse-engineering-google-location-gms-specification/>. [Haettu 7 2 2023].
- [37 B. Larson, "Google tracking phones even when they are disconnected?," 11 1 2018. [Online]. Available: <https://www.foxnews.com/video/5731183327001#sp=show-clips>. [Haettu 12 2 2023].
- [38 Computer Hope, "How much is 1 byte, kilobyte, megabyte, gigabyte, etc.?,," 31 8 2020. [Online]. Available:




- ] <https://www.computerhope.com/issues/chspace.htm>. [Haettu 12 2 2023].
- [39 M. Hyppönen, ”Hyvä ja paha internet,” TEK, 29 11 2022. [Online]. Available:  
 ] <https://www.tek.fi/fi/tapahtumat/mikko-hypponen-hyva-ja-paha-internet>. [Haettu 12 2 2023].
- [40 Alioto Law Firm, ”Class action lawsuit filed in California alleging Google is paying Apple to stay out of the  
 ] search engine business,” 3 1 2022. [Online]. Available: <https://www.prnewswire.com/news-releases/class-action-lawsuit-filed-in-california-alleging-google-is-paying-apple-to-stay-out-of-the-search-engine-business-301453098.html>. [Haettu 12 2 2023].
- [41 Google, ””toimintasi muilla sivustoilla ja muissa sovelluksissa,” [Online]. Available:  
 ] <https://policies.google.com/privacy/example/your-activity-on-other-sites-and-apps>. [Haettu 14 2 2023].
- [42 Posti, ”Turvallinen tietojen luovutus,” 1 1 2023. [Online]. Available:  
 ] <https://www.posti.fi/fi/asiakastuki/ehdot-ja-tietosuoja/tietosuoja/tietosuojaselosteet/postin-sahkoisten-kuluttajapalveluiden-asiakasrekisteri>. [Haettu 15 2 2023].
- [43 Alko, ”Tietojen luovuttaminen ja siirtäminen,” 3 11 2021. [Online]. Available:  
 ] <https://www.alko.fi/verkkokaupan-tietosuojaseloste>. [Haettu 15 2 2023].
- [44 Google, ”Eurooppalaiset vaatimukset,” 15 12 2022. [Online]. Available:  
 ] <https://policies.google.com/privacy?hl=fi#europeanrequirements>. [Haettu 15 2 2023].
- [45 T. H. L. K. V. L. C. Sampsa Rauti, ”Where Does Your Data Go? Comparing Network Traffic and Privacy  
 ] Policies of Public Sector Mobile Applications,” 11 5 2022. [Online]. Available:  
[https://link.springer.com/chapter/10.1007/978-3-031-04826-5\\_21](https://link.springer.com/chapter/10.1007/978-3-031-04826-5_21). [Haettu 15 2 2023].
- [46 D. Curry, ”Android Statistics (2023),” 9 1 2023. [Online]. Available:  
 ] <https://www.businessofapps.com/data/android-statistics/>. [Haettu 19 2 2023].
- [47 US, Department of Justice, ”Google DOJ advertising lawsuit,” 24 1 2023. [Online]. Available:  
 ] <https://www.documentcloud.org/documents/23584913-google-doj-advertising-lawsuit?responsive=1&title=1>. [Haettu 19 2 2023].
- [48 CNIL, ”Identifiant publicitaire : sanction de 8 millions d’euros à l’encontre de APPLE DISTRIBUTION  
 ] INTERNATIONAL,” 4 1 2023. [Online]. Available: <https://www.cnil.fr/fr/identifiant-publicitaire-sanction-de-8-millions-deuros-lencontre-de-apple-distribution-international>. [Haettu 27 2 2023].

## Liitteet

### Liite 1. Esimerkki tyypillisestä Googlen profiloinnista






**Google-tilin tiedot**

Näitä tietoja käytetään mainosten personointiin jakamiesi tai arvaamiemme tietojen perusteella. [Ylläpidä Google-tilillä](#)

 Sukupuoli Mies	 Ikä 25–34-vuotias	 Kieli 2 kieltä
---	--	---




**Kategoriat, joihin liittyviä mainoksia näet**


Voit nähdä mainoksia, jotka on tarkoitettu näihin Google-toimintaasi perustuviin kategorioihin sisältyville henkilöille. Voit nähdä mainoksia toisesta kategoriasta tai laittaa pois päältä kategoriat, joiden mainoksia et halua nähdä.


 Käytetään Ihmissuhteet Parisuhteessa	 Käytetään Koulutus Korkeakouluopisk...	 Käytetään Toimiala Ei tarpeeksi tietoa	 Käytetään Työnantajayritys... Suuryritysten (he...	 Käytetään Asumismuut... Vuokra-asuja
--	--	--	--	--

**Mainosten personointiin vaikuttava toiminta**

Googlen sivustoilla ja sovelluksissa tekemiäsi asioita ja sitä karkeaa aluetta, jolla olet ollut käyttäessäsi niitä, voidaan käyttää näkemiesi mainosten personointiin.

 Verkko- ja sovellustoiminta Käytetään	 YouTube-historia Käytetään
 Alueet joilla olet käyttänyt Googlea Ei käytetä	

 Näet My Ad Centerissä tekemäsi asiat [Omista tapahtumista.](#)

 Suojellemme yksityisyyttäsi. Driven, Gmailin ja Kuvien sisältöä ei koskaan käytetä mainostarkoituksiin.

## Liite 2. Windowsin seurannan poisto asennuksen yhteydessä

**Choose privacy settings for your device**

Microsoft puts you in control of your privacy. Choose your settings, then select 'Accept' to save them. You can change these settings at any time.

**Location**  
Get location-based experiences like directions and weather. Let Windows and apps request your location and allow Microsoft to use your location data to improve location services.  
 Yes

**Diagnostic data**  
Send info about the websites you browse and how you use apps and features, plus additional info about device health, device activity, and enhanced error reporting. Required diagnostic data will always be included when you choose to send Optional diagnostic data.  
 Send Required and Optional diagnostic data

**Tailored experiences**  
Let Microsoft use your diagnostic data, excluding information about websites you browse, to offer you personalized tips, ads, and recommendations to enhance your Microsoft experiences.  
 Yes

**Find my device**  
Turn on Find my device and use your device's location data to help you find your device if you lose it. You must sign in to Windows with your Microsoft account to use this feature.  
 Yes

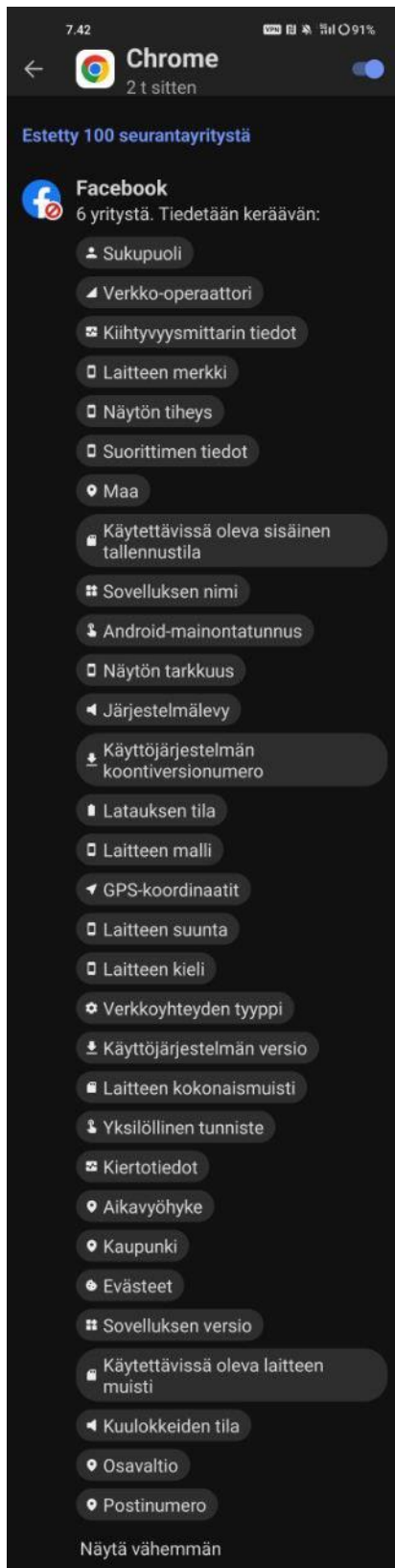
**Inking & typing**  
Send optional inking and typing diagnostic data to Microsoft to improve the language recognition and suggestion capabilities of apps and services running on Windows.  
 Yes

**Advertising ID**  
Apps can use advertising ID to provide more personalized advertising in accordance with the privacy policy of the app provider.  
 Yes

[Learn more](#) [Accept](#)



### Liite 3. Chrome selaimen lähettämät tiedot Facebookille



#### Liite 4. Sopimus Incognin kanssa

I, \_\_\_\_\_, residing at \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_,  
 \_\_\_\_\_, email address \_\_\_\_\_ hereby authorize Surfshark B.V., with registered address at Kabelweg 57, 1014BA Amsterdam, the Netherlands, Company number: 81967985 (the 'Agent'), to perform all lawful actions that are necessary to exercise, on my behalf, my following rights under applicable privacy legislation, including (but not limited to) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ('GDPR') (the "Privacy Laws"), and submit requests for implementation of these rights to any legal and natural persons governed by the Privacy Laws:

1. To obtain erasure (deletion) of my personal data (information);
2. To withdraw any consent I have given to the processing of my personal data (information);
3. To object to processing of personal data (information) concerning me, including but not limited to profiling and direct marketing.