Lassi Lehtovaara

# KULUTTAJAN YKSITYISYYSHUOLIEN VAIKUTUS MOBIILISOVELLUSTEN KÄYTÖN MUUTOKSIIN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

# TIIVISTELMÄ

Lehtovaara, Lassi
Kuluttajan yksityisyyshuolien vaikutus mobiilisovellusten käytön muutoksiin
Jyväskylä: Jyväskylän yliopisto, 2022, 68 s.
Tietojärjestelmätiede, pro gradu-tutkielma
Ohjaaja(t): Salo Markus, Hämäläinen Antti

Tutkielman tarkoituksena on tutkia sitä, miten yksityisyyshuolet vaikuttavat mobiilisovellusten käyttöön ja sen muutoksiin. Mobiililaitteet ja niissä olevat sovellukset ovat tulleet osaksi melkein kaikkien arkipäivää ja niissä liikkuu valtavat määrät käyttäjien henkilökohtaista dataa. Datan keruu ja sen käyttö on nostanut monilla käyttäjillä yksityisyyshuolia siitä, mitä dataa kerätään ja mihin sitä saatetaan käyttää. Tutkimuksen alussa suoritettiin kirjallisuuskatsaus, jossa tarkasteltiin aiempaa tutkimusta yksityisyydestä ja mobiilisovellusten käytöstä. Aiemman tutkimuksen perusteella pyrittiin luomaan tutkielmalle vahva teoreettinen pohja, jonka päälle tutkielman empiirinen osuus voitiin rakentaa. Tutkielman empiirinen osuus toteutettiin kvalitatiivisena haastattelututkimuksena. Haastatteluissa pyrittiin selvittämään onko käyttäjä kokenut yksityisyyshuolia käyttäessään mobiilisovelluksia, millaisia huolia haastateltava on kokenut ja miten ne vaikuttivat sovelluksen käyttöön. Haastattelujen kysymysrungon pohjana käytettiin MUIPC-tutkimusmallin kysymyksiä ja sen päälle lisättiin muutama aiheeseen liittyvä olennainen kysymys. Haastattelujen ja aiemman tutkimuksen perusteella tunnistettiin, että käyttäjät kokevat hyvin monenlaisia yksityisyyshuolia, mutta yksityisyyshuolet eivät kohdistu kaikkiin sovelluksiin yhtä vahvasti. Yksityisyyshuolten seurauksena joillakin käyttäjillä käyttö voi vähentyä, jotkut saattavat muokata sovelluksen asetuksia, jotkut vaihtavat toiseen parempaa yksityisyyttä tarjoavaan palveluun ja jotkut lopettavat palvelun käytön kokonaan. Tutkielmassa myös tunnistettiin mahdollisia jatkotutkimus kohteita. Esimerkiksi tarkempaa tutkimusta siitä mitkä tekijät vaikuttavat koettuihin yksityisyyshuoliin ja miten eri vahvuiset yksityisyyshuolet vaikuttavat mobiilisovellusten käyttöön.

Asiasanat: yksityisyys,yksityisyyshuolet, mobiilisovellukset

# ABSTRACT

Lehtovaara, Lassi
Effect of consumer's privacy concerns on mobile application usage
Jyväskylä: University of Jyväskylä, 2022, 68 pp.
Information Systems, Master's Thesis
Supervisor(s): Salo Markus, Hämäläinen Antti

The purpose of this thesis is to investigate how privacy concerns affect the use of mobile applications. Mobile devices and the applications in them have become a core part of everyday life and they collect huge amounts of users personal data. The collection and use of the data has raised privacy concerns among many users about what data is collected and where it may be used. At the beginning of the study, a literature review was conducted to review previous research on privacy and the usage of mobile applications. Based on previous research, the aim was to create a strong theoretical background for the dissertation, on which the empirical part of the dissertation can be constructed on. The empirical part of the dissertation was carried out as a qualitative interview study. The interviews sought to find out if the user had experienced privacy concerns while using mobile applications, what concerns the interviewee had experienced, and how the application usage had changed as a result of the privacy concerns. The questions were based on the questions of the MUIPC research model and were supplemented with a few relevant questions related to the topic. Based on interviews and previous research, it was identified that users experience a wide range of privacy concerns, but not all applications generate the same level of privacy concerns for the user. As a result of privacy concerns, some users may experience reduced use, some may change their usage in various ways, some may switch to another service that provides more privacy, and some may stop using the service altogether. The dissertation also identified possible areas for further research. For example, a more detailed study of what factors affect perceived privacy concerns and how different levels of privacy concerns affect the use of mobile applications.

Keywords: privacy, privacy concerns, mobile applications

## KUVIOT

KUVIO 1 IPPR-malli…….....27

## TAULUKOT

TAULUKKO 1 Tutkimusmallien vertailu..... 25

# SISÄLLYS

TIIVISTELMÄ……..2

ABSTRACT……..3

KUVIOT……... 4

TAULUKOT……4

SISÄLLYS…… 5

1 JOHDANTO…… 7

2 MOBIILISOVELLUSTEN KÄYTTÖ JA SEN MUUTOKSET…….. 10
2.1 Mobiilisovelluksien määritelmä…… 10
2.2 Mobiilisovellusten tuottama arvo käyttäjälle…….. 11
2.3 Sovellusten käyttö ja sen muutokset……12
2.3.1 Käytön muokkaaminen……... 12
2.3.2 Vaihtaminen…….. 13
2.3.3 Tauon pitäminen käytöstä……... 14
2.3.4 Lopettaminen…… 15

3 YKSITYISYYS MOBIILISOVELLUKSISSA……... 16
3.1 Yksityisyyden määritelmä……..16
3.2 Yksityisyyteen kohdistuvat uhkat……17
3.3 Yksityisyyshuolet……18
3.4 Kontekstuaalinen integriteetti……... 20
3.5 Yksityisyyshuolien tutkimusmallit……... 21
3.5.1 CFIP…… 21
3.5.2 IUIPC……... 22
3.5.3 MUIPC……23
3.5.4 Tutkimusmallien vertailu…… 24
3.6 Yksityisyyden hallinta…… 25

4 EMPIIRINEN TUTKIMUS……...29
4.1 Tutkimuskysymys ja sen rajaus……29
4.2 Tutkimusmenetelmän valinta…… 30
4.3 Tutkimuksen toteutus…… 31
4.4 Tutkimuksen toteutuksen arviointi……...33
4.5 Aineiston analyysi……... 34

5 TULOKSET…… 35
5.1 Haastateltavien kokemat yksityisyyshuolet ja niiden syyt……... 35
5.1.1 Aikaisemmat yksityisyyskokemukset……... 37
5.1.2 Koettu valvonta……39
5.1.3 Tietojen toissijainen käyttö……... 40
5.2 Haastateltavien käytön muutokset……... 41

5.2.1 Käytön muokkaaminen..... 41
5.2.2 Tauon pitäminen käytöstä..... 43
5.2.3 Vaihtaminen..... 44
5.2.4 Poistaminen..... 46
5.2.5 Ennaltaehkäisevä toiminta..... 47
5.3 Muutoksia estävät tekijät..... 48

6 POHDINTA..... 51
6.1 Johtopäätökset teorian ja tutkimuksen kannalta..... 51
6.2 Johtopäätökset käytännön kannalta..... 57
6.3 Tutkimuksen rajoitteet..... 57
6.4 Jatkotutkimusaiheet..... 58

7 YHTEENVETO..... 59

LÄHTEET..... 61

LIITE 1 HAASTATTELURUNKO..... 67

# 1 JOHDANTO

Mobiililaitteet ja -sovellukset ovat nousseet valtavaan suosioon ja lähes jokainen suomalainen omistaa älypuhelimen. Vuonna 2018 Tilastokeskus selvitti, että 80% suomalaisista omistaa älypuhelimen (Kohvakka, 2018). On vaikea kuvitella enää sellaista maailmaa, jossa ei olisi mobiilisovelluksia ja niiden tarjoamia palveluita. Nykyään melkein jokaiseen arjen ongelmaan on olemassa mobiilisovellus. Ihmiset ovat valmiita lataamaan ja käyttämään sovelluksia, koska ne yleensä ratkaisevat konkreettisia arjen haasteita. Mobiilisovellusten, kuten minkä tahansa muun IT-palvelun käytöstä kuitenkin muodostuu valtava määrä dataa joihin sovelluskehittäjät pääsevät helposti käsiksi. Xu ym. (2012) mukaan yksityisyys onkin noussut kriittiseksi kysymykseksi varsinkin mobiilisovellusten kohdalla. Mobiilisovellusten valmistajat pystyvät rakentamaan hyvinkin tarkkoja malleja siitä, mistä asioista heidän käyttäjänsä pitävät ja mikä saa heidät esimerkiksi ostamaan jotain tuotteita tai jatkamaan palvelun käyttöä pidempiä aikoja. Shklovski ym. (2014) mainitsee, että usein tietojen kerääminen ei välttämättä tähtää salakavaliin tarkoituksiin, vaan yritykset yrittävät tarjota parempia palveluita asiakkailleen. He kuitenkin mainitsevat, että vaikka tietojen keräämisen lähtökohdat olisivat asiakkaan kannalta mieluisia, monet ihmiset pitävät tietojen keräämistä silti epäilyttävänä. Käyttäjille voi nousta tiedon keräyksen ja käytön takia yksityisyyshuolia siitä, millaista dataa kerätään, mihin se päätyy ja miten sitä käytetään.

Tämän tutkielman tarkoituksena on tutkia sitä, miten yksityisyyshuolet muuttavat sovelluksien käyttöä käyttäjän näkökulmasta. Tutkielman kirjallisuuskatsausta tehdessä tunnistettiin selvä aukko tämänhetkisessä tutkimustiedossa. Monet tutkimukset ovat keskittyneet yksityisyys kysymyksiin ja toinen osa mobiilisovellusten käyttöön. Tutkimuksia, joissa tarkasteltiin yksityisyyden vaikutusta sovellusten käyttöön ei löytynyt suuria määriä. Esimerkiksi Barth ym. (2019) mainitsevat, että tutkimusta on tehty paljon käyttäjien toiminnan aikomuksiin liittyen, mutta ei varsinaisesti miten käyttäjät ovat oikeasti toimineet. Aikomuksen ja käytännön toiminnalla voi olla merkittäviä eroja, koska käyttäjät saattavat esittää aikomuksen muuttaa toimintaa, mutta he eivät loppujen lopuksi päädy tekemään niin. Tämän tutkielman kannalta on olennaista tarkastella, miten toiminta muuttui konkreettisesti. Tämä tutkielma siis selvittää, miten käyttäjän yksityisyyshuolet vaikuttavat mobiilisovellusten käytön muutoksiin. Tämän perusteella

tutkielmalle on luotu yksi tutkimuskysymys, johon tutkielmassa pyritään vastaamaan:

- Miten käyttäjän yksityisyyshuolet vaikuttavat mobiilisovellusten käytön muutoksiin?

Tutkielman teoriaosuus on toteutettu kirjallisuuskatsauksena, jossa tutustutaan tarkemmin aikaisempaan tutkimukseen ja teorioihin. Tutkielmaan valittuja lähteitä on arvioitu kriittisesti, jotta ne ovat tieteellisten standardien mukaisia ja tarpeeksi laadukkaita. Tutkielman empiirinen osuus suoritettiin laadullisena tutkimuksena. Tiedonkeruu menetelmäksi valikoitui puolistrukturoitu teemahaastattelu. Haastattelu todettiin kaikkein tehokkaimmaksi ratkaisuksi ottaen huomioon tutkielman tekoon saatavilla olevat resurssit. Haastatteluissa käytetty kysymysrunko pohjautuu Xu ym. (2012) MUIPC-tutkimusmallin kysymyksiin. Haastatteluun osallistui kahdeksan (n=8) henkilöä, jotka löytyivät tutkijan henkilökohtaisista verkostoista.

Tämä tutkimus on olennainen niin yritysten, kuluttajien kuin tutkimuksen kannalta seuraavilla tavoilla. Yrityksille ja palveluita tarjoaville organisaatioille tämä tutkielma auttaa ymmärtämään, millaisia muutoksia sovelluksien käytössä voidaan havaita käyttäjän kokiessa yksityisyyshuolia yrityksen sovellusta käytettäessä. Tällä tavoin voidaan suunnitella sovelluksia, jotka ovat avoimempia mahdollisesta tiedonkeruusta tai muuten käyttäjien yksityisyyshuolet huomioonottavia. Käyttäjille tämä tutkielma tarjoaa mahdollisuuden tutkia, millaisia riskejä ja yksityisyysuhkia sovelluksissa ja niiden käytössä voi olla. Tutkimuksen kannalta tämä tutkielma pyrkii yhdistelemään teemoja niin yksityisyyden tutkimuksesta, kuin IT:n käytön tutkimuksesta sekä miten yksityisyys vaikuttaa kuluttajan valintoihin sovellusympäristössä.

Tutkielma koostuu seitsemästä kappaleesta sisältäen myös johdannon. Johdannon jälkeen seuraa teoriaosuus, jossa käsitellään mobiilisovelluksia, niiden käyttöä ja käytön muutoksia. Tutustutaan mobiilisovellusten tuottamaan arvoon ja erilaisiin käytön muutoksiin, joita aikaisemmissa tutkimuksissa on havaittu mobiilisovellusten ja -palveluiden kontekstissa. Tutkielman kolmas luku käsittelee yksityisyyttä ja käyttäjien kokemia yksityisyyshuolia. Kappaleessa määritellään ensin, mitä yksityisyydellä tämän tutkielman kontekstissa tarkoitetaan, jonka jälkeen selvitetään, mikä uhkaa käyttäjän yksityisyyttä mobiilisovelluksia käytettäessä. Viimeisenä kappaleessa esitellään yksityisyyshuolten tarkasteluun suunniteltuja tutkimusmalleja. Tutkielman neljäs luku käsittelee tutkielman empiirisen osuuden toteutusta. Luvussa kerrotaan laadullisen tutkimusmenetelmän valinnasta ja miksi päädyttiin valitsemaan puolistrukturoitu haastattelu tiedonkeruumenetelmäksi. Luvussa tarkastellaan myös tutkimuksen käytännön toteutusta esimerkiksi, miten haastattelut toteutettiin ja ketkä siihen osallistuivat. Tutkielman viidennessä luvussa käydään läpi haastattelujen perusteella saatuja vastauksia, jotka on jaettu teemojen mukaan. Viimeisenä asiakappaleena on pohdinta, joka tarjoaa kaikkein konkreettisimpia vastauksia siihen, miten mobiilisovellusten käyttö

voi muuttua ihmisillä eri tavoilla yksityisyyshuolista johtuen. Verrataan empiirisestä tutkimuksesta saatuja tuloksia aiempaan kirjallisuuteen ja tehdään johtopäätöksiä nojaten tähän kirjallisuuteen sekä empiiriseen aineistoon. Pohdintakappaleessa esitetään myös mahdollisia jatkotutkimuskohteita, joita voidaan hyödyntää tulevassa tutkimuksessa. Viimeisenä tässä luvussa tarkastellaan kriittisesti tutkimuksen mahdollisia rajoitteita ja kohdattuja ongelmia. Tutkielma päättyy yhteenvetoon, jossa esitellään tiivistettynä tutkielman lähtökohdat ja tärkeimmät löydökset.

# 2 MOBIILISOVELLUSTEN KÄYTTÖ JA SEN MUUTOKSET

Tässä kappaleessa esitellään lyhyesti, mitä mobiilisovelluksilla tämän tutkielman kontekstissa tarkoitetaan ja millaisia käytön muutoksia mobiilisovelluksiin kohdistuu. Ensimmäinen alaluku määrittelee mobiilisovellukset tarkemmin, toinen alaluku käsittelee sovellusten tuottamaa arvoa ja kolmas luku erilaisia käytön muutoksia, joita kirjallisuudessa on esitelty mobiilisovelluksille ja muille IT-palveluille. Kappale on tutkimuksen kannalta olennainen, koska siinä pyritään selvittämään aikaisemmassa kirjallisuudessa käsiteltyjä mahdollisia IT-käytön muutoksia. Tämän tutkimuksen kontekstissa käytön muutoksia halutaan tutkia sen jälkeen, kun käyttäjän tietoon on tullut jokin yksityisyysuhka ja miten käyttäjä tähän uhkaan on reagoinut.

## 2.1 Mobiilisovelluksien määritelmä

Mobiilisovellukset ovat älypuhelimille, tableteille ja älykelloille luotuja ohjelmistotuotteita, jotka tarjoavat käyttäjilleen palveluita ja toimintoja. Esimerkkejä mobiilisovellusten tuottamista palveluista ovat terveyden seuranta, viihde, yhteydenpito, yhteisöpalvelut ja verkko-ostokset (Doub ym., 2015). Nykyään voidaan yleisesti ajatella hyvin moniin arkipäivän ongelmiin löytyvän mobiilisovelluksia, jotka voivat ratkaista nämä ongelmat. Tutkielma on rajattu koskemaan ainoastaan tavallisille kuluttajille sovelluskaupoista löytyviä sovelluksia eikä esimerkiksi yritysosvelluksia, jotka ovat ladattavissa sovelluskauppojen ulkopuolelta. Erilaisia mobiilisovelluksia on tarjolla miljoonia suurissa sovelluskaupoissa, kuten Apple App Storessa ja Google Play Storessa (Doub ym., 2015). Vuonna 2021 mobiilisovellusmarkkinoiden arvon arvioitiin olevan noin 6.3 triljoonaa dollaria (Wang ym., 2019). Mobiilipalvelut eroavat perinteisistä palveluista siinä, että ne eivät ole riippuvaisia ajasta tai paikasta (Heinonen & Pura, 2008). Yritykset ja mainostajat ovat myös tajunneet mobiilisovellusten kyvyn tuottaa asiakkailleen enemmän arvoa ja hyötyä

verrattuna perinteisiin keinoihin (H. 'Chris' Yang, 2013). Sovellusten tarjoamat mahdollisuudet ovatkin aiheuttaneet markkinoiden ruuhkautumisen ja käyttäjien huomiosta kilpaillaan koko ajan entistä kovemmin (Ding & Chai, 2015). Jotta palveluntarjoajat pystyvät tuottamaan hyvää, helposti saatavaa ja kontekstitietoista palvelua, keräävät sovellukset käyttäjältään erilaista dataa, kuten sijainnin, henkilötietoja, kiinnostuksen kohteita ja muuta puhelimesta saatavaa dataa (Pentina ym., 2016).

## 2.2 Mobiilisovellusten tuottama arvo käyttäjälle

Aikaisempi tutkimus on osoittanut, että käyttäjän kokema hyöty palvelun käytöstä voidaan jakaa utilitaristiseen ja hedonistiseen arvoon (Chandon ym., 2000). Heinonen ja Pura (2008) määrittelevät utilitaristisen arvon liittyvän ulkoiseen motivaatioon käyttää palvelua, kun halutaan saavuttaa jokin tavoite. Hedonistisen arvon Heinonen ja Pura (2008) määrittävät sisäisenä motivaationa, joka kohdistuu viihdyttävään tai nautittavaan palvelun käyttöön. Heinonen ja Pura (2008) selittävät myös, että informaatiota tarjoavat palvelut, kuten uutiset, sää tai hakukoneet tarjoavat käyttäjälleen korkeaa utilitaristista arvoa, kun taas hedonista arvoa tuottavat sovellukset, kuten pelit tai musiikkisovellukset. Joidenkin sovellusten voidaan myös katsoa tuottavan sekä utilitaristista, että hedonistista arvoa käyttäjilleen. Heinonen ja Pura (2008) esittävät myös palveluita, jotka tuottavat hyvin vähän kumpaakaan arvoa. Tällaiset palvelut he määrittelevät "nice to have" ominaisuuksina, joita ilman käyttäjä pystyy pärjäämään hyvin. Tämän tutkielman kannalta on oleellista pohtia, miten sovelluksen tuottama arvo käyttäjälle vaikuttaa palvelun käyttöön suhteessa käyttäjän yksityisyyshuoliin. Barth ym. (2019) tulivat päätelmään, jossa mobiilisovelluksen käyttö hedonistiseen tai utilitaristiseen käyttötarkoitukseen voi johtaa eroihin siinä, miten käyttäjä arvioi yksityisyyden kyseisessä sovelluksessa (Barth ym., 2019).

Käyttäjän kokema arvo voidaan myös nähdä vertailuna hyötyjen ja mahdollisten uhrausten tuloksena (Woodall, 2003). Woodall (2003) on esittänyt kattavan jaon hyötyjen ja uhrausten tyypeistä. Woodallin mukaan tuote voi tarjota käyttäjälleen hyötyjä sen ominaisuuksien kautta esimerkiksi palvelun laadun tai räätälöinnin seurauksena. Woodallin mallissa uhraukset on jaettu rahassa mitattaviin ja ei-rahassa mitattaviin uhrauksiin. Rahallisia uhrauksia on esimerkiksi hinta. Tämän tutkielman kontekstissa myös tuotteen keräämät henkilötiedot, joita käytetään esimerkiksi mainos tarkoituksiin, voidaan ajatella olevan rahassa mitattavia uhrauksia. Ei-rahassa mitattavia uhrauksia taas voi olla esimerkiksi tuotteen käyttöön käytetty aika ja vaiva.

## 2.3 Sovellusten käyttö ja sen muutokset

Sovelluksien, kuten muidenkin IT-tuotteiden ja palveluiden käyttöön, kohdistuu aina muutoskäyttäytymistä. Tässä kappaleessa esitellään, millaisia käytön muutoksia aikaisemmassa tutkimuksessa on esitetty. Salo ym. (2022) esittelevät neljä kategoriaa käytön muutoksille, joita he käyttivät tutkiessaan teknostressin hallintakeinoja ja sitä, miten teknostressi vaikuttaa palveluiden käyttöön. Kategorioita voidaan pitää hyvin relevantteina myös tämän tutkimuksen kannalta, koska esimerkiksi Ayyagari ym. (2011) mainitsee yksityisyyshuolet yhdeksi teknostressin aiheuttajaksi (Ayyagari ym., 2011). Salo ja muut tunnistivat neljä kategoriaa käytön muutokselle: käytön muokkaaminen, palvelun vaihtaminen korvaavaan, väliaikaisen tauon pitäminen ja käytön lopettaminen kokonaan (Salo ym., 2022).

### 2.3.1 Käytön muokkaaminen

Salo ym. (2022) määrittelevät käytön muokkaamisen toimintana, jossa käyttäjä esimerkiksi muokkaa sovelluksen yksityisyysasetuksia, muokkaa sovelluksen käyttöä esimerkiksi poistamalla ihmisiä ja sivuja, joita seuraa tai vähentää sovelluksen käyttöä (Salo ym., 2022). Seuraavaksi mainitut käytön muutokset voitaisiin osittain laskea käytön muokkaamiseksi, koska esimerkiksi käytön vähentäminen on hyvin lähellä käytön muokkaamisen määritelmää.

Tämän tutkielman kontekstissa käytön muokkaamiseen voidaan laskea mukaan myös kaikki sellainen toiminta, joka johtuu käyttäjän yksityisyyshuolista tai missä käyttäjä pyrkii suojaamaan omaa tai muiden yksityisyyttä. Olennaista on myös ymmärtää, että käytön muutokset ovat käytännössä yksityisyyden suojaamisen keinoja, mitä yksilö ottaa käyttöön. Yang ja Wang (2009) antavat esimerkit väärien tietojen luovuttamisesta, vaatimuksen poistaa palvelun keräämät tiedot tai kieltäytyä tietojen luovuttamisesta (S. Yang & Wang, 2009). Sovelluksen yksityisyysasetusten muuttaminen voidaan nähdä toimintana, jossa käyttäjä kieltäytyy luovuttamasta tietoja sovelluksen käyttöön. Käytön muokkaaminen voi olla myös käytön jatkamista, mutta yksityisyys tarkemmin huomioiden esimerkiksi jakamalla kuvia, joissa ei näy kasvoja tai lähettämällä viestejä, joissa ei ole mitään yksityisyyttä vaarantavia esimerkiksi pankkitietoja.

### 2.3.2 Vaihtaminen

Salo ym. (2022) määrittelevät vaihtamisen toiseen palveluun toimintana, jossa käyttäjä vaihtaa käytön vaihtoehtoiseen sovellukseen tai vaihtaa saman palvelun käytön erilaiseen versioon esimerkiksi mobiilisovelluksesta selainpohjaiseen sovellukseen (Salo ym., 2022).

IT-tuotteiden ja palveluiden vaihtamista on tutkittu laajasti tietojärjestelmätieteen tutkimuksessa, jossa eniten käytetyksi malliksi on noussut Push-Pull-Mooring malli. Malli on alun perin kehitetty muuttoliikkeiden selittämistä varten. Bansal (2005) tutki Push-Pull-Mooring mallin soveltuvuutta palveluiden vaihtamisen kontekstiin ja huomasi niillä olevan suuria yhteneväisyyksiä. Malli koostuu kolmesta tekijästä (Bansal, 2005):

- Push-tekijöillä tarkoitetaan sellaista tekijää, joka työntää käyttäjiä pois lähtöpisteestä. Push-tekijöinä voidaan nähdä esimerkiksi palvelun heikko laatu, hinta ja luottamus palveluntarjoajaan.
- Pull-tekijöillä tarkoitetaan positiivisia tekijöitä, jotka vetävät käyttäjiä puoleensa. Pull-tekijöitä ovat esimerkiksi vaihtoehdon houkuttelevuus.
- Mooring-tekijöillä tarkoitetaan yksilön tilanteeseen ja kontekstiin liittyviä tekijöitä, jotka saattavat viedä muuttopäätöstä suuntaan tai toiseen. Mooring-tekijöinä voidaan nähdä Bansalin mukaan esimerkiksi käyttäjän kokemat vaihtokustannukset. Vaihtokustannukset voivat olla taloudellisia, psykologisia tai tunnepohjaisia, jotka saattavat ilmentyä ennen vaihtoa, sen aikana tai sen jälkeen (Kim ym., 2006). Mooring-tekijät lisättiin malliin, sillä huomattiin, että pelkät push ja pull-tekijät eivät tarpeeksi hyvin selitä ihmisten muuttoaikeita.

Tämän tutkielman kontekstissa on hyvä tarkastella, millaiset yksityisyyteen liittyvät tekijät voivat toimia push, pull tai mooring tekijöinä. Esimerkiksi käyttäjän turvallisuushuolet voidaan nähdä negatiivisena mooring-tekijänä käyttäjän palvelun vaihdon kannalta (Bhattacherjee & Park, 2014). Esimerkki yksityisyyteen liittyvästä push-tekijästä on käyttäjän tyytymättömyys palvelun yksityisyyden suojaan ja esimerkki pull-tekijästä on toisen palvelun koettu yksityisyyden suoja (Schreiner & Hess, 2015b). Schreiner ja Hess (2015) tunnistivat puoleensavetäväksi ominaisuudeksi myös ryhmäpaineen tutkiessaan käyttäjien vaihtokäyttäytymistä Whatsappista, Threema-viestipalvelun käyttäjäksi. Threema palveluun vaihtaneet käyttäjät siis houkuttelivat Whatsapp käyttäjiä vaihtamaan palvelua. Tämä voidaan myös nähdä käänteisesti, mitä Schreiner ja Hess eivät maininneet. Eli käyttäjän halutessa vaihtaa Threeman käyttäjäksi esimerkiksi paremman yksityisyyden perässä, mutta hänellä ei ole ystäviä, jotka käyttävät kyseistä palvelua on tällä varmasti negatiivinen vaikutus käyttäjän vaihto aikeisiin. Kuten Schreiner ja

Hess (2015) mainitsevat, käyttäjät oletettavasti käyttävät samaa palvelua, kuin heidän lähipiirinsä. Tästä voidaan johtaa ajatus, että viestintäpalvelun käytössä voi mooring-tekijä olla positiivinen tai negatiivinen vaihdon kannalta. Tällainen tilanne, jossa käyttäjä käyttää palvelua, jonka pääasiallisena tarkoituksena on viestiä lähipiirin kanssa ei käyttäjällä ole varsinaisesti muuta vaihtoehtoa kuin käyttää kyseistä palvelua. Käyttäjällä saattaa olla mahdollisuus vaikuttaa käytössä olevan palvelun valintaan, mutta edellä mainittua tilannetta voidaan pitää vaihtamisen esteenä. Vaihtamisen esteellä tarkoitetaan käyttäjän kokemaa tunnetta, jossa hänet on lukittu johonkin suhteeseen, koska vaihtaminen aiheuttaisi jonkinlaisia taloudellisia, sosiaalisia tai psykologisia kustannuksia käyttäjälle (H.-T. Tsai & Huang, 2007). Edellisessä esimerkissä siis vaihtamisen esteenä toimi käyttäjän lähipiirin oleminen toisessa viestipalvelussa. Tällöin käyttäjä joutuu valitsemaan haluaako viestitellä lähipiirinsä kanssa vai käyttää toista viestipalvelua, joka luultavasti johtaisi uuden sovelluksen käytön loppumiseen.

### 2.3.3 Tauon pitäminen käytöstä

Salo ym. (2022) määrittelevät tauon pitämisen yhdeksi käytön muutokseksi. Sovelluksen käytön kokonaan lopettamisen sijaan käyttäjä saattaa pitää tauon sovelluksen käytöstä. Tauko voi tarkoittaa sovelluksen säilyttämistä puhelimessa, mutta sen avaamatta jättämistä tietyn ajan. Käyttäjä saattaa myös poistaa sovelluksessa olevan käyttäjätilinsä väliaikaisesti. Tällöin käyttäjä saattaa edelleen pitää sovelluksen laitteessaan tai poistaa sen. Käyttäjä saattaa poistaa koko sovelluksen, mutta jättää palveluun esimerkiksi käyttäjätilin ja muita tietoja (Salo ym., 2022). York ja Turcotte (2015) kuvailevat tutkimuksessaan ilmiötä, jossa käyttäjät pitävät väliaikaisen tauon Facebookin käytöstä, mutta saattavat kuitenkin palata käyttämään Facebookkia myöhemmin. Tällöin he eivät hylkää palvelua kokonaan, mutta pitävät siitä taukoa vedoten esimerkiksi Facebookin aiheuttamaan stressiin tai henkilökohtaiseen ajanpuutteeseen (York & Turcotte, 2015). He kuvailevat toimintaa erilaiseksi kuin vaihtamista tai lopettamista, koska käyttäjä pitää “lomaa” palvelusta, mutta saattaa palata sen pariin jossain vaiheessa uudelleen. He kertoivat myös, että tällaisessa tilanteessa oli hyvin epätodennäköistä, että käyttäjä vaihtaisi johonkin samanlaiseen palveluun tauon aikana. Tämä viittaa käyttäjän kokemuksiin tauon taustalla. Käyttäjät eivät etsi varsinaisesti korvaajaa palvelulle vaan haluavat syystä tai toisesta pitää käytöstä taukoa. Suurin osa heidän tutkimuksen vastaajista kertoi ajanpuutteen olevan suurin syy pitää taukoa palvelun käytöstä.

### 2.3.4 Lopettaminen

Lopettamisella tarkoitetaan tämän tutkielman kontekstissa sitä, että käyttäjällä on ollut käytössään jokin mobiilisovellus, mutta esimerkiksi yksityisyyshuolista tai vähäisestä koetusta hyödystä johtuen käyttäjä päättää lopettaa sovelluksen käytön kokonaan ja poistaa sen laitteestaan. Lopettaminen on tässä tutkielmassa mainituista käytön muutoksista selvästi dramaattisin ratkaisu, koska käyttäjä ei esimerkiksi korvaa sovellusta jollain vastaavalla sovelluksella vaan sen käyttö loppuu kokonaan. Mobiilisovellusten näkökulmasta lopettamiseen voi esimerkiksi liittyä myös käyttäjätilin poistaminen ennen sovelluksen poistamista, jolloin käyttäjä pyrkii jättämään jälkeensä mahdollisimman pienen jäljen. Salo ym. (2022) huomauttaa kuitenkin, että lopettaminen ei aina välttämättä tarkoita sovelluksen poistamista kokonaan vaan sovellus saattaa joskus jäädä käyttäjän laitteeseen, mutta sitä ei avata koskaan. Tällä tavoin lopettamisella ja tauon pitämisellä käytöstä on yhtäläisyyksiä ja niiden välinen raja voi joskus olla häilyvä. Wottrich (2019) nostaa esille, että monet mobiilisovellukset eivät tarjoa käyttäjilleen mahdollisuuksia kovinkaan laajoihin yksityisyyttä suojaaviin toimiin, joten hän esittää, että monessa tapauksessa ainut tapa, jolla käyttäjä voi suojata yksityisyyttään tältä sovellukselta on poistaa se kokonaan laitteesta (Wottrich ym., 2019). Tällainen tilanne voi johtaa Wottrichtin (2019) mukaan siihen, että käyttäjän yksityisyyden suojaamisen motivaatio laskee, koska poistamisen jälkeen hänellä ei ole pääsyä sovelluksesta saatavaan tietoon tai ihmisiin, jos kyseessä on esimerkiksi viestintäpalvelu. Käyttäjä tekee siis laskelman siitä, mikä on yksityisyyden suojaamisen hinta, jos pääsyä sovelluksen tarjoamiin etuihin ei ole. Jos yksityisyyden suojaamisen hinta on liian korkea, käyttäjän motivaatio suojata yksityisyyttään voi laskea ja suojaavia toimenpiteitä ei toteuteta.

# 3 YKSITYISYYS MOBIILISOVELLUKSISSA

Tämän kappaleen tarkoituksena on esitellä yksityisyyttä ja yksityisyyshuolia käsitteinä ja ymmärtää, millaisia uhkia käyttäjän yksityisyyttä uhkaa ja miten näitä uhkia vastaan on mahdollista suojautua. Kappale on olennainen tutkimuksen kannalta, koska siinä selvitetään, mistä yksityisyyshuolet voivat käyttäjällä johtua ja miten tutkimukseen osallistuvien henkilöiden mahdollisia yksityisyyshuolia voidaan mitata.

## 3.1 Yksityisyyden määritelmä

Yksityisyys voidaan määritellä hyvin monella eri tavalla ja sitä on tutkittu eri tieteenaloilla hyvin pitkään. Koska yksityisyys voidaan määritellä näkökulmasta riippuen niin monella tavalla, ei sille ole kuitenkaan vakiintunut yksiselitteistä määritelmää. Yksinkertainen ja käytännönläheinen määritelmä yksityisyydelle on Clarken (1999) jako neljään ulottuvuuteen. Clarken yksityisyyden neljä ulottuvuutta ovat henkilön yksityisyys, joka viittaa lähinnä henkilön fyysiseen yksityisyyteen. Toinen ulottuvuus on henkilökohtaisen käytöksen yksityisyys, joka viittaa esimerkiksi uskonnollisen ja poliittisen toiminnan yksityisyyteen. Kolmas ulottuvuus on henkilökohtaisen viestinnän yksityisyys, jolla tarkoitetaan mahdollisuutta viestiä eri medioissa ilman rutiininomaista valvontaa. Neljäs ulottuvuus on henkilökohtaisen datan yksityisyys, joka tarkoittaa henkilön oikeutta hallita häneen liittyvää dataa, joka on muiden hallussa tai datan päätymistä muille (Clarke, 1999).

Kolmanteen ja neljänteen ulottuvuuteen liittyy olennaisesti informaatioyksityisyys. Belanger ym. (2011) mukaan informaatioyksityisyys tarkoittaa henkilön mahdollisuutta hallita, miten heihin liittyvää informaatiota käsitellään (Bélanger & Crossler, 2011). Informaatioyksityisyydelle on myös useita määritelmiä, mutta ne eivät eroa merkittävästi toisistaan ja kaikissa ilmenee henkilökohtaisen datan sekundäärisen käytön hallinta (Belanger ym., 2002). Sekundäärisellä käytöllä taas viitataan kerätyn datan käyttöön muissa tarkoituksissa, kuin mihin se on alun perin kerätty (Bélanger & Crossler, 2011).

Smith ym. (1996) tunnisti informaatioyksityisyyteen liittyvät neljä ulottuvuutta, jotka ovat tiedon kerääminen, valtuuttamaton informaation sekundäärinen käyttö, sopimaton pääsy informaatioon ja virheet informaatiossa (Smith ym., 1996). Informaatioyksityisyys on tämän tutkielman kannalta kaikkein relevantein käsite, johon viitataan myöhemmin tutkielmassa yksityisyydestä puhuttaessa.

## 3.2 Yksityisyyteen kohdistuvat uhkat

Käyttäjän yksityisyyteen kohdistuu nykyään monenlaisia riskejä. Nykyisten informaatio- ja viestintäteknologioiden avulla pystytään keräämään ja analysoimaan ihmisistä tietoa nopeammin ja tehokkaammin kuin koskaan aiemmin (Malhotra ym., 2004). Uusien teknologioiden myötä voidaan yksityisyysuhaksi laskea esimerkiksi identiteettivarkaus, henkilökohtaisten tietojen julkiseksi päätyminen, profiilien informaatio louhinta ja kyber-vaaninta (Cho ym., 2020). Keskeisiä trendejä yksityisyysuhissa ovat esimerkiksi sisällön personointi ja käyttöperusteinen profilointi (Toch ym., 2012). Toch ym. (2012) kertovat, että verkosta on tullut sosiaalinen paikka, jossa ihmiset käyttävät oikeita identiteettejä ja kommunikoivat lähipiirinsä kanssa. Tämän seurauksena sovellukset pystyvät keräämään käyttäjistään tietoja, jonka avulla voidaan näyttää yksilöityjä mainoksia, relevantteja hakutuloksia ja muuta yksilöityä sisältöä. Toch ym. (2012) mukaan sisällön yksilöinti sijaintiin perustuen voi paljastaa käyttäjän sijainnin ei-valtuutetuille kolmansille osapuolille. Sijaintiin liittyvä räätälöinti herättää käyttäjissä useita huolia esimerkiksi vaaninnasta, kodin sijainnin paljastumisesta, esimiehen suorittamasta seurannasta, valtion suorittamasta seurannasta ja häiritsevästä sijaintiin perustuvasta mainonnasta (J. Y. Tsai ym., 2010). Käyttöperusteinen profilointi tarkoittaa Tochin ym. (2012) mukaan sitä, että kerätään pitkäaikaisesti dataa käyttäjän toiminnasta, jota käytetään käyttäjäkokemuksen räätälöintiin. Toch ym. (2012) sanovat, että usein dataa kerätään käyttäjien tietämättä monella tavalla esimerkiksi evästeiden avulla ja muuta verkkoliikennettä seuraten. Tochin ym. (2012) ilmaisemassa tilanteessa on uhkana tiedon joutuminen vääriin käsiin tai sen julkaisemisesta, joka voi aiheuttaa yksilölle monenlaisia haittoja. Yksityisyyteen kohdistuvissa uhkissa täytyy kuitenkin huomioida, että kaikki sovellukset eivät sisällä yhtä suurta yksityisyysuhkaa vaan uhka on hyvin sovelluskohtainen. Pearson ja Benameur (2010) kertovat, että jos palvelu käsittelee julkista tietoa, voidaan sen nähdä olevan matalan riskin palvelu, mutta sellaisiin palveluihin, jotka käsittelevät esimerkiksi käyttäjän sijaintia, mieltymyksiä, kalenteria ja sosiaalisia verkostoja kohdistuu merkittävästi suurempi riski (Pearson & Benameur, 2010).

## 3.3 Yksityisyyshuolet

Käyttäjän yksityisyyshuolet voidaan määritellä usealla eri tavalla. Smith ym. (1996) määrittelee yksityisyyshuolet yksilön huolina organisaation informaatioyksityisyyden käytäntöjä kohtaan (Smith ym., 1996). Malhotra ym. (2004) määrittelevät yksityisyyshuolet yksilön subjektiivisena näkemyksenä siitä, miten reilusti tietoja käytetään informaatioyksityisyyden kontekstissa (Malhotra ym., 2004). He esittävät, että datan kerääminen sekä sallittuihin, että ei-sallittuihin tarkoituksiin on yksityisyyshuolien alku käyttäjillä**.** Dinevin ja Hartin (2004) määrittelevät yksityisyyshuolet siten, että ne edustavat käyttäjän ymmärrystä ja havaintoja siitä, miten heidän antamaansa tietoja käytetään internetissä (Dinev & Hart, 2004). Lanier ja Saini (2008) määrittelevät yksityisyyshuolet ahdistuksen tunteena henkilön omaa yksityisyyttä kohtaan (Lanier & Saini, 2008). Yksityisyyshuolille on siis hyvin monta erilaista määritelmää, mutta kaikkien niiden taustalla on käyttäjän huoli tai ahdistus siitä, miten häneen liittyviä yksityisiä tietoja käytetään tai jaetaan ja kenellä on niihin pääsy. Dinev ja Hart (2014) esittävät, että käyttäjien yksityisyyshuoliin vaikuttaa käyttäjän kokema haavoittuvuus ja käyttäjän kokema mahdollisuus hallita tietoa. Nämä kaksi tekijää yhdessä vaikuttavat siihen, miten paljon yksityisyyshuolia käyttäjä kokee, kun hänen täytyy jakaa itsestään tietoja (Dinev & Hart, 2004). Phelps ym. (2000) kertovat, että käyttäjät ovat todennäköisemmin huolissaan yksityisyydestään, jos heidän tietojaan kerätään tai käytetään ilman lupaa tai niin, että käyttäjä ei tiedä tiedonkeruusta (Phelps ym., 2000).

Käyttäjien kokemat yksityisyyshuolet voidaan Liun ym. (2014) mukaan selittää seitsemällä tekijällä:

1. Käyttäjän henkilökohtaisia tietoja kerätään hyvin paljon
2. Käyttäjältä kerätyt tiedot saattavat olla epätarkkoja tai ne voivat sisältää virheitä
3. Organisaatiot, jotka keräävät käyttäjän tietoja eivät välttämättä pysty suojelemaan tietoja ja sen johdosta ulkopuolisille saattaa avautua pääsy tarkastelemaan tietoja
4. Organisaatiot, jotka keräävät käyttäjän tietoja saattavat käyttää niitä tarkoituksiin, jotka ovat käyttäjältä salassa tai jotka ovat epäsopivia. Tällaista toimintaa kutsutaan tietojen toissijaiseksi käytöksi.
5. Organisaatiot, joiden lain mukaiset sopimukset ja selosteet eivät ole kunnossa aiheuttavat käyttäjille yksityisyyshuolia
6. Organisaation ominaisuudet ja maine vaikuttavat käyttäjien yksityisyyshuolten syntymisen
7. Organisaatiot saattavat muuttaa käyttöehtojaan usein ja muutokset voivat jäädä yksilöiltä huomaamatta, joka kasvattaa käyttäjien yksityisyyshuolia

Yksityisyyshuoliin voidaan nähdä vaikuttavan hyvin moninainen kirjo erilaisia tekijöitä. On kuitenkin selvää, että eri ihmiset näkevät yksityisyyden hyvin eri tavalla ja Liun ym. (2014) mukaan myös informaation tyypillä on vaikutusta yksityisyyshuolien syntymiseen. Esimerkiksi henkilön taloustiedot ja henkilötunnus ovat tietoja, joista käyttäjät saattavat tuntea enemmän yksityisyyshuolia kuin esimerkiksi iän tai sukupuolen julkaiseminen (Liu ym., 2014).

Useissa tutkimuksissa on huomattu, että kysyttäessä ihmiset osoittavat huomattavasti suurempaa huolta omaa yksityisyyttään kohtaan, kuin mitä heidän todellinen käyttäytymisensä osoittaa. Tätä ilmiötä on kirjallisuudessa kutsuttu nimellä yksityisyyden paradoksi. Yksityisyyden paradoksia on tutkittu melko paljon ja sitä on pyritty selittämään erilaisilla teorioilla ja malleilla. Gerber (2018) esittää kirjallisuuskatsauksessaan useita pyrkimyksiä selittää yksityisyyden paradoksia teorian avulla. Gerberin (2018) mukaan privacy calculus-teoria on yksi käytetyimmistä teorioista selittämään yksityisyyden paradoksia. Privacy calculus-teorian mukaan ihmiset tekevät yksityisyyteen liittyviä päätöksiä tasapainottamalla koettua yksityisyyteen kohdistuvaa riskiä ja tietojen jakamisesta saatavan hyödyn välillä (Dinev & Hart, 2006). Gerberin (2018) katsauksessa tietojen jakamisesta käyttäjä voi saada esimerkiksi taloudellista hyötyä erilaisten kuponkien muodossa, käytännöllistä hyötyä esimerkiksi paremman räätälöinnin seurauksena tai sosiaalista hyötyä käyttämällä erilaisia sosiaalisen median palveluita. Privacy calculus-teorian mukaan ihmiset siis jakavat tietoa, jos palvelusta saatavat hyödyt ylittävät käyttäjän kokemat riskit yksityisyyttä kohtaan. Gerberin (2018) mukaan kuitenkin privacy calculus-teoriassa täytyy huomioida se, että sen mukaan käyttäjä toimi täysin rationaalisesti arvioidessaan hyötyjen ja haittojen tasapainoa. Gerber osoittaa useisiin tutkimuksiin, joissa todetaan, että käyttäjien päätöksentekoon vaikuttavat useat ennakkoasenteet ja heuristiikat, jotka voivat vääristää käyttäjän päätöksentekoa tiedon jakamisen suhteen tai, että käyttäjät eivät aina edes tiedä, jos heiltä kerätään tietoja. Yhden näkemyksen mukaan yksityisyyden paradoksia voidaan selittää myös niin sanotun opitun avuttomuuden -mallilla. Opittu avuttomuus tarkoittaa tilannetta, jossa yksilön yksityisyyttä on loukattu jatkuvasti ja yksilöllä ei ole mahdollisuutta saada tästä minkäänlaista korvausta (Shklovski ym., 2014). Kun ihmiset eivät enää reagoi yksityisyyden loukkauksiin tai loukkauksen yrityksiin, vaikka heillä olisi keinoja puolustautua tällaista toimintaa vastaan, voidaan todeta, että käyttäjä on "oppinut avuttomaksi". Shklovski ym. (2014) esittää kaksi lainausta kyselyyn osallistuneilta käyttäjiltä, "Hyväksyin sen hiljaisesti. Kun saat minut ajattelemaan asiaa en pidä siitä, mutta seuraavan kerran, kun lataan jonkun sovelluksen, olen jo unohtanut koko jutun" ja toinen käyttäjä vastasi "se tuntuu pakolliselta pahalta tässä kohtaa. Koska se on kaikkialla läsnä en usko, että tämä asia tulee koskaan menemään pois". Molemmissa tilanteissa käyttäjä siis ajattelee yksityisyyskysymykset asioina, joihin he eivät voi vaikuttaa millään tavalla ja jotta he voivat käyttää palveluita heidän on vain hyväksyttävä tietojen kerääminen ja käyttäminen. Shklovski ym. (2014) toteaa, että suurin osa

ihmisistä protestoi tietojen keräämistä vastaan, mutta sisimmässään eivät oikeastaan välitä asiasta. Tähän liittyy myös niin sanottu tappio-positio. Uhkapelaamisesta tuttu tappio-positio on tilanne, jossa uhkapelin pelaaja on jo hävinnyt osan rahoistaan, mutta sen sijaan, että pelaaja keskittyisi minimoimaan tappioita hän pelaa lopulta kaikki rahansa. Sovelluksen käyttäjä saattaa myös ottaa suurempia riskejä tuntiessaan, että hänen henkilötietonsa ovat jo vaarantuneet, joten tämänhetkisellä toiminnalla ei ole niin paljon merkitystä (Keith ym., 2012).

## 3.4 Kontekstuaalinen integriteetti

Nissenbaum (2011) esitteli teorian kontekstuaalisesta integriteetistä. Tämän teorian mukaan ihmisten yksityisyysajattelu pohjautuu paljon enemmän kontekstiin siitä, mitä kerätään, missä tilanteessa ja mihin tarkoitukseen (Nissenbaum, 2011). Tärkeänä kysymyksenä kontekstuaalisessa integriteetissä ei ole se onko tieto, jota kerätään yksityistä tai julkista vaan enemmänkin se, että sopiiko tämä tiedonkeruu tilanteessa vallitsevaan sosiaaliseen kontekstiin. Ihmiset ovat koko ajan jonkinlaisessa vuorovaikutuksessa informaation kanssa ja tämä vuorovaikutus usein liittyy johonkin sosiaaliseen kontekstiin (Shklovski ym., 2014). Esimerkkinä tiedon kontekstisidonnaisuudesta mobiilisovelluksissa on käyttäjän sijaintitietojen keruu, jota käytetään navigointiin, mutta sijainnin pyytäminen taskulamppu sovelluksessa rikkoo tätä kontekstuaalista integriteettiä (Martin & Shilton, 2016). Kontekstuaalinen integriteetti siis säilyy, jos informaatio liikkuu ihmisten kontekstuaalisten normien mukaan (Shklovski ym., 2014). Mobiilisovelluksissa tätä voi kuitenkin olla vaikea määritellä tarkasti, koska tietojen keruusta ei aina välttämättä ole selkeää kuvaa. Jokaisella ihmisellä on myös omanlaisensa näkemys siitä, millainen tiedonkeruu on sopivaa missäkin tilanteessa.

Kontekstuaalinen integriteetti tekee siis tiedonkeruusta mobiilisovelluksissa kontekstisidonnaista, joka täytyy huomioida siinä, miten käyttäjien sovellusten käyttö muuttuu. Sovelluksen kerätessä aiemman esimerkin mukaan sijaintia karttasovelluksessa tuskin herättää käyttäjässä yksityisyyshuolia, mutta aiemmin mainittu taskulamppu saattaa herättää merkittäviä yksityisyyshuolia, joka saattaa saada käyttäjän reagoimaan tilanteeseen jollain tavalla. Tutkielman empiirisessä osuudessa pyritään selvittämään, mikä on kontekstin vaikutus yksityisyyshuolista johtuviin käytön muutoksiin.

## 3.5 Yksityisyyshuolien tutkimusmallit

Aikaisemmassa tutkimuksessa on esitetty useita malleja sille, miten käyttäjien yksityisyyshuolia voidaan mallintaa. Tässä kappaleessa käydään läpi kaikkein yleisimmin käytetyt Malhotra ym. (2004) internet users information privacy concerns -malli (IUIPC), Smithin (1996) Concern for information privacy (CFIP) -malli ja Xu ym. (2012) Mobile Users Information Privacy Concern (MUIPC) -malli. Smithin CFIP-malli on luotu ensin ja sitä on hyödynnetty useissa yksityisyyshuolia tarkastelevissa tutkimuksissa. Tutkimuksessa CFIP-malli on yleisemmin käytetty verrattuna IUIPC-malliin. Useat tutkimukset ovat käyttäneet, arvioineet ja vertailleet molempia malleja (Bélanger & Crossler, 2011; Fodor & Brem, 2015; S. Yang & Wang, 2009). Tämän tutkielman kannalta oleellisin malli on Xu ym. (2012) MUIPC-malli, koska se keskittyy mobiilipalveluihin ja sovelluksiin.

### 3.5.1 CFIP

Smith ym. (1996) kehittivät CFIP-mallin tarkastelemaan ihmisten yksityisyyshuolien eri ulottuvuuksia organisaationäkökulmasta. CFIP-malli koostuu neljästä tutkittavasta ulottuvuudesta, joita voidaan tarkastella 15 yksityisyyteen liittyvän väittämän avulla. Smithin ym. malli voidaan jakaa neljään ulottuvuuteen, jotka ovat:

- Tietojen kerääminen (collection)
    - Tietojen keräämisellä tarkoitetaan käyttäjän kokemusta siitä, miten huolestuttavana käyttäjä pitää kerätyn tiedon määrää ja näiden tietojen luovuttamista organisaatioille (Stewart & Segars, 2002)
- Virheet tiedoissa (errors)
    - Virheellisellä tiedolla tarkoitetaan tietoja, jotka organisaatiolle on luovutettu, mutta ne sisältävät virheitä tai ne eivät ole oikein merkattuja. Tällainen tilanne saattaisi johtaa esimerkiksi luottohakemuksen hylkäämiseen (Stewart & Segars, 2002).
- Tietojen luvaton toissijainen käyttö (unauthorized secondary use)
    - Sisäinen käyttö: Tietojen luvaton toissijainen käyttö organisaation sisällä tarkoittaa tilannetta, jossa käyttäjä on luovuttanut organisaatiolle tietoja johonkin tarkoitukseen, mutta tiedot saanut organisaatio käyttää tietoja alkuperäisen tarkoitusperän lisäksi myös muihin tarkoituksiin. Esimerkiksi tällaista toimintaa on henkilötietojen käyttäminen organisaation markkinoinnissa.

    - Ulkoinen käyttö: Tietojen luvaton toissijainen käyttö organisaation ulkopuolella tarkoittaa tilannetta, jossa käyttäjä on luovuttanut organisaatiolle tietoja johonkin tarkoitukseen, mutta tiedot saanut organisaatio luovuttaa tietoja jollekin ulkopuoliselle toimijalle, jolloin tietoja käytetään muihin tarkoitusperiin mihin ne oli alunperin luovutettu. (Stewart & Segars, 2002)
- Luvaton pääsy tietoihin (improper access)
    - Organisaatiot ovat määritelleet sisäisesti kenellä organisaation sisällä on pääsy joihinkin tietoihin tai mahdollisesti jopa kenellä ulkopuolisella on pääsy tietoihin. Käyttäjällä, joka luovuttaa tietoa, ei välttämättä ole selvää näkyvyyttä siihen, kenellä on pääsy näihin tietoihin ja miten helposti näihin tietoihin joku voisi päästä käsiksi (Stewart & Segars, 2002)

Vaikka CFIP-mallia on käytetty eniten mittaamaan käyttäjien yksityisyyshuolia, voidaan sitä pitää vähemmän sopivana vaihtoehtona mittaamiselle mallin ollessa alun perin suunniteltu yksityisyyshuolille, jotka kohdistuvat organisaation tiedonkeruuta kohtaan (Xu ym., 2012).

### 3.5.2 IUIPC

CFIP-mallin rinnalle kehitettiin toinen malli, joka pohjautuu sosiaalisen sopimuksen teoriaan ja keskittyy tutkimaan käyttäjien yksityisyyshuolia oikeudenmukaisuuden näkökulmasta. Malhotra ym. kehittivät IUIPC-mallin CFIP-mallin pohjalta, mutta muokkasivat sitä CFIP-mallin alkuperäisestä kontekstista soveltumaan paremmin juuri internetin kontekstiin (Xu ym., 2012). IUIPC-malli koostuu kolmesta ulottuvuudesta, joita voidaan mitata 10 kohtaisella mittaristolla (Malhotra ym., 2004). IUIPC-mallin kolme ulottuvuutta ovat:

- Tietojen kerääminen (collection)
    - IUIPC-mallissa tietojen kerääminen liittyy ajatukseen siitä, miten reilua ja hyödyllistä tietojen luovuttaminen organisaatiolle on. Esimerkkinä tästä on verkkokaupan käyttäminen, missä käyttäjä arvioi riskin ja hyödyn suhteen. Jos riski on pieni, on käyttäjä halukkaampi luovuttamaan tietojaan (Malhotra ym., 2004).
- Tietojen hallitseminen (control)
    - Tietojen hallinta tarkoittaa tietoja luovuttaneen käyttäjän kykyyn vaikuttaa tietojen käyttöön ja halutessaan niiden poistamiseen palveluntarjoajalta. Malhotran mukaan hallinnan puute omien tietojen suhteen lisää käyttäjien yksityisyyshuolia (Malhotra ym., 2004)
- Tietoisuus siitä, miten tietoja käytetään (awareness)

- Käyttäjä antaa aina tietojaan johonkin tarkoitukseen esimerkiksi verkkokauppaostoksen toteuttamiseen. Jos tiedot saanut organisaatio käyttää tietoja johonkin muuhun tarkoitukseen tai esimerkiksi jakaa sen, voi käyttäjä pitää tätä toimintaa epäoikeudenmukaisena, koska tietoja ei tähän tarkoitukseen oltu luovutettu. Tähän ulottuvuuteen liittyy myös käyttäjän käsitys siitä, miten tiedot saanut organisaatio säilyttää ja käsittelee tietoja turvallisesti (Malhotra ym., 2004).

IUIPC-malli ei ole saanut välttämättä niin suurta käyttöä, koska joissain tutkimuksissa on kuvattu, että esimerkiksi IUIPC-mallin avulla on vaikea nähdä sitä, miten luottamus palveluntarjoajaan vaikuttaa käyttäjien halukkuuteen jakaa tietoa (Fodor & Brem, 2015). IUIPC-mallin vähäinen käyttö voi Belangerin ja Crosslerin (2011) mukaan johtua myös siitä, että monet tutkimukset olivat ehtineet jo alkaa ennen IUIPC-mallin julkaisua. CFIP-mallia pidetään tutkimuksessa *de facto* mallina, joten sitä ei ole haluttu lähteä vaihtamaan IUIPC-malliin.

### 3.5.3 MUIPC

Kolmas malli, joka tarkastelee käyttäjien yksityisyyshuolia, on MUIPC-malli, on luotu CFIP- ja IUIPC-mallien pohjalta soveltumaan paremmin käyttäjien yksityisyyshuolten tutkimiseen juuri mobiilipalveluiden kontekstissa. MUIPC-malli koostuu kolmesta vaikuttavasta tekijästä: koetusta valvonnasta (perceived surveillance), koetusta tunkeutumisesta (perceived intrusion) ja tietojen toissijainen käyttö (secondary use of information) (Xu ym., 2012). Koetulla valvonnalla tarkoitetaan MUIPC-mallissa kaikkea toimintaa, jossa käyttäjää seurataan tai profiloidaan käyttäessään mobiilipalvelua. Xu ym. (2012) mukaan koettu valvonta on keskeistä, koska sovellukset käyttävät hyvinkin aggressiivisia tiedonkeruumenetelmiä käyttäjiä kohtaan. Heidän mukaansa tämä johtaa avoimeen toimintaympäristöön, jossa tiedon läpäisevyys on hyvin korkeaa. Tämä tarkoittaa sitä, että sovellusten valmistajat pystyvät keräämään valtavia määriä dataa ilman rajoituksia tai esteitä keruulle. Tunkeutumisella tarkoitetaan Xun ym. (2012) mukaan tilannetta, jossa datan saaja, eli tässä tapauksessa jokin organisaatio, pystyy tekemään itsenäisiä päätöksiä siitä, mitä tiedolla tehdään. Tällaisessa tilanteessa voidaan nähdä, että organisaatio loukkaa tiedon omistajan eli käyttäjän oikeutta hallita tietojaan sovelluksissa. Xu:n ym (2012) mukaan tunkeutuminen liittyy vahvasti käyttäjän henkilökohtaiseen tilaan. Kolmas malli, joka liittyy tunkeutumiseen, on tietojen toissijainen käyttö. Smith ym. (1996) määrittelevät toissijaisen käytön sellaisena toimintana, jossa tiedot saanut organisaatio käyttää saatuja tietoja ilman lupaa muihin tarkoituksiin, kuin mihin ne oli alun perin annettu. Tällainen tilanne voi nostaa merkittäviäkin yksityisyyshuolia käyttäjälle hänen havaitessa niin

sanotun “linkin” aikaisemmin kerättyyn tietoon, jota nyt käytetään toisessa kontekstissa toiseen tarkoitukseen. Käytännön esimerkkinä voidaan antaa yleisesti keskusteltu aihe siitä kuuntelevatko sosiaalisen median palvelut käyttäjiään. Linkki muodostuu käyttäjälle, kun he ovat esimerkiksi ystävien kanssa keskustelleet ruoan verkkokaupoista. Hetken kuluttua heille ilmestyy tällaisten verkkokauppojen mainoksia sosiaalisessa mediassa. Tässä tilanteessa käyttäjän mielessä syntyy linkki, että tietoa on kerätty ja käytetty sellaisella tavalla, johon käyttäjä ei välttämättä tietoisesti ollut antanut lupaa. Tärkeää on huomioida se, että käyttäjä on luultavasti hyväksynyt käyttöehdot ja tiedonkeruu on täysin tämän sopimuksen mukainen, mutta usein käyttäjät eivät välttämättä koe asian olevan niin.

### 3.5.4 Tutkimusmallien vertailu

Tässä luvussa koostetaan yhteen yksityisyyshuolien tutkimusmallit. Kaikki kolme mallia lähestyvät yksityisyyshuolia hieman erilaisista lähtökohdista. Ne ovat selvästi oman aikansa tuotoksia, vaikka edelleen hyvin päteviä. Smith ym. (1996) CFIP-malli rakensi hyvän pohjan tulevalle kuluttajien yksityisyystutkimukselle. Malli koostui kuluttajalle tietojen keruun ilmoittamisesta, käyttäjän myöntymisestä, tietojen asiallisesta käytöstä, tietojen virheiden minimoinnista ja sen suojaamisesta ulkopuolisilta tahoilta.

Malhotra ym. (2004) kehittivät oman mallin, joka pyrki yksityisyyshuolien ja käytön aikomusten tarkasteluun internetin kontekstissa. Koska Smith ym. (1996) julkaisivat mallinsa ennen kuin internet oli suurimman osan arkea ja elämää, ei se pystynyt ennakoimaan täydellisesti yksityisyyshuolia ja tiedonkeruumenetelmiä, joita internet mahdollistaa. Tämän takia IUIPC-mallin luominen oli olennaista. IUIPC-malli perustuu sosiaalisen sopimuksen teoriaan ja yksityisyyshuolia tarkastellaankin oikeudenmukaisuuden näkökulmasta. IUIPC-malli on koostettu kolmesta osasta: tietojen keräämisestä, tietojen hallinnasta ja tietoisuudesta, miten organisaatio käyttää käyttäjän tietoja.

Kolmas esitelty malli on Xun ym. (2012) MUIPC-malli, jonka tarkoituksena oli luoda yksityisyyshuolien tutkimusmalli mobiilisovellusten kontekstiin. Monissa mobiililaitteita ja sovelluksia käsittelevissä tutkimuksissa käytetään edelleen CFIP- tai IUIPC-malleja, vaikka MUIPC-malli on luotu juuri mobiilisovellusten kontekstiin. MUIPC-malli koostuu kolmesta tekijästä, jotka perustuvat yksityisyyden viestinnän hallinnan-teoriaan ja ne ovat: koettu valvonta, koettu tunketuminen ja tietojen toissijainen käyttö. Tämän tutkielman kannalta MUIPC-malli toimii kaikkein parhaiten, kun halutaan tarkastella käytön muutoksia mobiilisovelluksissa, jotka johtuvat yksityisyyshuolista. Vaikka CFIP-mallia on käytetty enemmän aikaisemmissa tutkimuksissa, voidaan todeta MUIPC-mallin olevan sopivampi tähän tutkimukseen, koska se käsittelee mobiilikäyttäjien yksityisyyshuolia eikä esimerkiksi yksityisyyshuolia

organisaatio näkökulmasta kuten CFIP-malli. Kuvio 2 esittää Xu ym. (2012) vertailun yksityisyyshuolien tutkimusmalleista ja niiden keskeisistä eroista.

| | CFIP | IUIPC | MUIPC |
|---|---|---|---|
| Tarkoitus | Reflektoida yksilöiden huolia organisaatioiden tiedonkeruumenetelmistä | Reflektoida internet käyttäjien huolia informaatio-yksityisyydestä | Reflektoida mobiili- käyttäjän huolia informaatio-yksityisyydestä |
| Painopiste | Organisaation vastuu, miten käyttäjän tietoja hallitaan | Yksilön subjektiiviset näkemykset oikeudenmukaisuudesta informaatio-yksityisyyden kontekstissa | Yksilön tunne siitä, että hänellä on oikeus omistaa yksityiset tiedot |
| Dimensiot | • Tietojen kerääminen<br>• Luvaton tietojen toissijainen käyttö<br>• Virheet tiedoissa<br>• Luvaton pääsy tietoihin | • Tietojen kerääminen<br>• Tietojen hallinta<br>• Tietoisuus yksityisyys- käytännöistä | • Koettu valvonta<br>• Koettu tunkeutuminen<br>• Tietojen toissijainen käyttö |

TAULUKKO 1 Tutkimusmallien vertailu (Xu ym., 2014)

## 3.6 Yksityisyyden hallinta

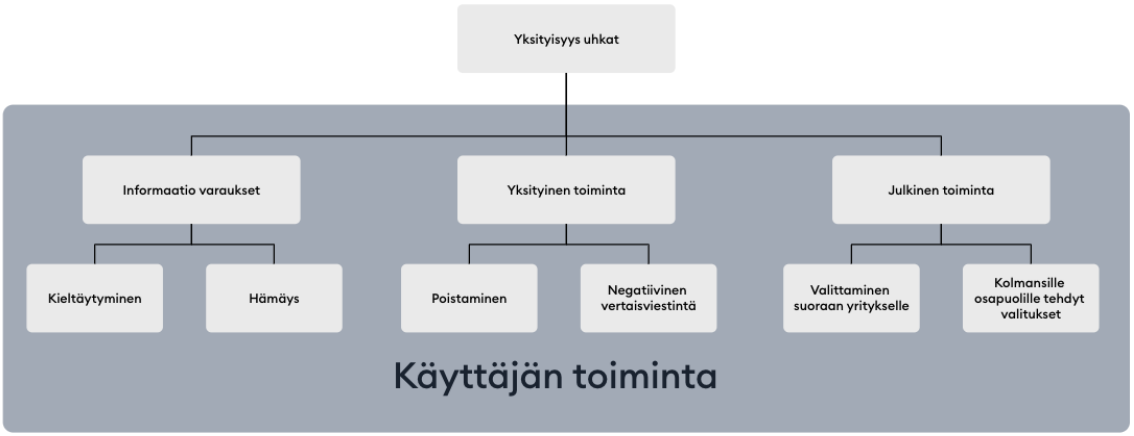
Son ja Kim (2008) esittelevät tutkimuksessaan käsitteen informaatioyksityisyyden suojaamisreaktiot (IPPR: Information privacy-protective responses). Tällä tarkoitetaan käyttäjän käyttäytymisessä havaittavia reaktioita heidän kokemiaan yksityisyysuhkia kohtaan, jotka johtuvat jonkun organisaation datan keruu toiminnoista. IPPR keskittyy kolmeen kategoriaan, jotka sisältävät erilaisia tapoja reagoida yksityisyysuhkiin verkossa. Ne ovat informaatiovaraus (information provision), yksityinen toiminta (private action) ja julkinen toiminta (public action) (Son & Kim, 2008).

Informaatiovarauksella tarkoitetaan tilannetta, jossa esimerkiksi käyttäjä on rekisteröitymässä johonkin palveluun ja palvelun kysyessä käyttäjän henkilötietoja voi käyttäjä kieltäytyä antamasta tietoja palveluun. Tällaista toimintaa Son ja Kim kutsuvat kieltäytymiseksi (refusal). Kieltäytymisellä voidaan myös Sonin ja Kimin mukaan tarkoittaa esimerkiksi evästeiden keruun kieltämistä. Kieltäytyminen voi kuitenkin olla käyttäjälle haastavaa, koska usein monet palvelut vaativat henkilötietojen antamista, jotta palvelua voi käyttää. Yksityisyyttä suojatakseen Son ja Kim esittävät, että käyttäjät voivat suojata yksityisyyttään antamalla vääriä tietoja palveluun. Tätä Son ja Kim kutsuvat hämäykseksi (misrepresentation). Aiempaan esimerkkiin viitaten tällaisessa tilanteessa käyttäjä pääsee käyttämään haluttua palvelua ilman, että

käyttäjä joutuu antamaan omia henkilötietojaan palvelun käyttöön. Son ja Kim pitävät näitä kahta keinoa tehokkaimpina, jotka suojaavat käyttäjän yksityisyyttä. Myös muut tutkimukset ovat tutkineet paljon sitä, miten käyttäjät kieltäytyvät antamasta organisaatioille tietoja ja miten kieltäytyminen vaikuttaa yksityisyyshuoliin (Smith ym., 1996; Malhotra ym., 2004).

Toinen kategoria Son ja Kimin (2008) mallissa on yksityinen toiminta (private action). Tällä viitataan toimintaan, joka johtuu esimerkiksi tyytymättömyyteen jotain organisaatiota kohtaan. Käyttäjä ollessa tyytymätön voi hän esimerkiksi boikotoida palvelua ja jakaa huonoja kokemuksia lähipiirin kanssa. Boikotointiin liittyen Son ja Kim kertovat poistamisen (removal) olevan konkreettinen tapa suojata käyttäjän yksityisyyttä. Tällöin käyttäjä pystyy pyytämään tietojen poistoa organisaation tietokannoista tai poistaa tietoja itse, jos se on mahdollista. Son ja Kim antavat esimerkin, jossa käyttäjä kieltäytyy personoiduista sähköposti viesteistä suojatakseen omaa yksityisyyttään. Tämän tutkimuksen kontekstissa poistamisella voidaan myös tarkoittaa sitä, että käyttäjä poistaa sovelluksessa olevan tilinsä tai poistaa sovelluksen puhelimestaan. Tällä tavoin sovellus ei pysty enää keräämään käyttäjästä tietoja. Son ja Kim esittävät toisen tavan yksityisessä toiminnassa. Negatiivinen vertaisviestintä (negative word-of-mouth) on käyttäjän yksityistä toimintaa, jossa käyttäjä viestii omalle lähipiirilleen tyytymättömyyttä palvelun yksityisyystoimia kohtaan. Resnick ym. (2000) kertovat, että negatiivisella vertaisviestinnällä voi olla negatiivinen vaikutus yritysten maineeseen ja se voi vaikuttaa yrityksen myyntiin tulevaisuudessa. Negatiivista vertaisviestintää voidaan pitää yhtenä merkittävänä tapana, miten tieto yrityksen huonoista yksityisyyskäytännöistä leviää käyttäjien keskuudessa.

Son ja Kim esittävät kolmannen kategorian, joka on julkinen toiminta. Julkinen toiminta voidaan Son:n ja Kim:n mukaan jakaa kahteen osaan: suorat valitukset yritykselle ja kolmansille osapuolille tehdyt valitukset. Singh (1989) mukaan tyytymättömät kuluttajat valittavat ensin suoraan yritykselle, mutta sen ollessa tehotonta voidaan valitus tehdä jollekin kolmannelle osapuolelle. On kuitenkin tärkeää huomata tilanne, jossa kohdattavalle yritykselle on hyvin haastavaa antaa palautetta, jolloin voidaan ensin kääntyä kolmannen osapuolen puoleen (Brown & Swartz, 1984). Kolmansilla osapuolilla tarkoitetaan tässä tilanteessa jotakin yksityisyysasioihin erikoistunutta yhdistystä tai yritystä, joka voi auttaa yksityisyysuhkiin liittyvissä haasteissa. Son ja Kim kertovat, että tällainen toiminta voi hyödyttää käyttäjää itseään ja kaikkia muita palvelun käyttäjiä, jos julkinen toiminta johtaa joihinkin muutoksiin esimerkiksi palvelun käyttöehdoissa.




KUVIO 1 IPPR-malli (Son & Kim, 2008)

Sonin ja Kimin (2008) lisäksi myös muut tutkimukset ovat pyrkineet selvittämään käyttäjien mahdollisuuksia ja keinoja suojautua yksityisyysuhkilta. Wirtz ym. (2007) esittelee kolme kategoriaa siihen, miten käyttäjät saattavat hallita omaa yksityisyyttään. Ne ovat tiedon väärentäminen (fabricate), jolla tarkoitetaan oman identiteetin suojaamista antamalla esimerkiksi väärä sähköpostiosoite. Suojaaminen (protect) tarkoittaa erilaisten teknologioiden käyttöä, jotka suojaavat käyttäjää erilaisilta uhkilta. Esimerkki suojaavasta toiminnasta on evästeiden kieltäminen tai suojaavan palvelun käyttöönotto. Tiedon panttaaminen (withold) tarkoittaa sitä, että käyttäjä ei suostu antamaan itsestään tietoja kyseiselle palveluntarjoajalle (Wirtz ym., 2007). Wirtz:n toiminnoissa nähdään paljon samankaltaisuuksia Sonin ja Kimin (2008) mallin kanssa, mutta Sonin ja Kimin malli on kattavampi käyden läpi myös toimia, jotka eivät suoraan vaikuta käyttäjän yksityisyyteen, mutta voivat yleisesti parantaa tilannetta yksityisyyden näkökulmasta esimerkiksi erilaisten boikottien tai palautteen kautta. Myös Yang & Wang (2009) tutkimuksessaan esittävät suojaustoimenpiteitä, joita käyttäjä voi ottaa suojatakseen omaa yksityisyyttään. Yang & Wang (2009) antavat esimerkit väärien tietojen antamisesta: vaatimukset poistaa tietoja palveluntarjoajan palvelimilta ja kieltäytyä luovuttamasta tietoja. Euroopassa tämän tyyppinen henkilötietojen suojaaminen on tehty helpommaksi, koska yleinen tietosuojalauseke (GDPR) antaa käyttäjille mahdollisuuden yksityisyyttä suojaaviin toimiin kuten pyytää tietojensa poistamista, pyytää mitä tietoja yrityksellä on käyttäjästä, pyytää yritystä lopettamaan omien tietojen prosessoinnin ja pyytää saada kopiota kaikesta datasta, joita yrityksellä on käyttäjästä (Euroopan Unioni, 2022)

Käyttäjillä on mahdollista myös käyttää yksityisyyttä suojaavia teknologioita, joiden tarkoituksena on suojella käyttäjän yksityisyyttä sovelluksissa. Käyttäjä voi esimerkiksi rajoittaa sovelluksen pääsyä sensoreihin tai muuhun laitteessa olevaan dataan. Tällöin sovelluksella ei ole mahdollista käyttää näitä tietoja seurantaan tai profilointiin. Konkreettisia esimerkkejä toiminnoista, joita käyttäjät voivat tehdä suojellakseen yksityisyyttä voidaan löytää esimerkiksi Applen ja Googlen verkkosivuilta. Esimerkki tietojen väärentämisestä on Applen tarjoama “piilota sähköpostini” ominaisuus, jonka

avulla sovellukseen voidaan luoda yksittäinen sähköpostiosoite, joka uudelleenohjaa sovelluksen lähettämät sähköpostit käyttäjän oikeaan osoitteeseen. Tällöin, jos käyttäjä haluaa lopettaa viestien saamisen tai lopettaa palvelun käytön ei hänen sähköpostinsa jää palveluntarjoajan tietokantoihin (Apple, 2022). Toinen konkreettinen esimerkki Applen tarjoamista yksityisyyspalveluista on sovelluksen kysyessä pääsyä puhelimen kuvagalleriaan voi käyttäjä valita pääsyn vain tiettyihin kuviin eikä koko galleriaan. Tällä tavoin käyttäjän valokuvat pysyvät piilossa sovellukselta, jos käyttäjällä on huoli yksityisyydestä. Android tarjoaa käyttäjilleen myös erilaisia yksityisyyttä parantavia toimintoja kuten toiminnon, joka automaattisesti evää sovellukselta pääsyn joihinkin tietoihin ja sensoreihin, jos sovellus ei ole ollut käytössä muutamaan kuukauteen. Tällä tavalla voidaan välttää tilanne, jossa käyttäjä on ladannut sovelluksen, mutta unohtanut sen puhelimeensa ja ominaisuuden takia sovellus ei pysty keräämään käyttäjästä tietoja (Google, 2022). Molemmille älypuhelimien alustoille on myös saatavilla sovelluksia, jotka skannaavat käytössä olevia sosiaalisen median sovelluksia ja kertovat käyttäjälle, jos yksityisyysasetuksissa on puutteita ja miten paremmin suojata omaa yksityisyyttä. Tällaiset toiminnot ovat esimerkkejä siitä, miten haluttuja palveluita pystyy edelleen käyttämään täysin normaalisti, mutta samalla huolehtien hyvästä yksityisyydestä. Ne osoittavat, että yksityisyys ei välttämättä ole kaikki tai ei mitään kysymys, vaan on mahdollista luoda ratkaisuja, jotka ovat sekä toimivia, että turvallisia käyttäjälle.

# 4 EMPIIRINEN TUTKIMUS

Tämän tutkimuksen empiirinen osuus pyrkii selvittämään, miten käyttäjän kokemat yksityisyyshuolet vaikuttavat käyttäjän mobiilisovelluksen käyttöön. Tarkoituksena on siis selvittää, millä tavoilla käyttäjä muuttaa mobiilisovelluksen käyttöä, jos hän kokee yksityisyyshuolia kyseistä sovellusta käyttäessään. Ensimmäisenä selvitetään millaista tutkimusmenetelmää käyttäen tutkimus on toteutettu. Toisena selvitetään, miten tutkimus toteutettiin ja mistä saatu aineisto kerättiin ja kolmantena selvitetään, miten luotettava tutkimus oli ja oliko tutkimuksen toteutuksessa jonkinlaisia rajoitteita tai haasteita. Viimeisenä käsitellään aineiston analyysiä.

## 4.1 Tutkimuskysymys ja sen rajaus

Tutkielmaan yritettiin löytää kaikkein relevantein tutkimuskysymys, jonka avulla valittua ilmiötä halutaan tutkia. Tutkielman tutkimuskysymyksenä on "Miten kuluttajien yksityisyyshuolet vaikuttavat mobiilisovellusten käytön muutoksiin?" Tutkielmaa haluttiin rajata koskemaan pelkästään kuluttajia, koska usein organisaatioiden käytössä oleviin sovelluksiin yksittäiset työntekijät eivät pysty vaikuttamaan kovinkaan paljoa ja heillä ei ole valinnanvaraa toisin kuin tavallisella kuluttajalla, joka pystyy tekemään itsenäisiä päätöksiä siitä, millaisia mobiilisovelluksia hän käyttää. Tutkielmassa haluttiin käsitellä mobiilisovelluksia hieman laajemmin, koska käyttäjillä voi olla hyvin suuri määrä erilaisia sovelluksia käytössä ja yksityisyyshuolet vaikuttavat eri sovelluksiin eri tavoilla. Täten tutkielmasta ei haluttu rajata pois sovelluksia, joissa käyttäjillä saattaisi nousta yksityisyyshuolia. Sovellusten käyttöä haluttiin myös tutkia melko korkealla tasolla, jotta voidaan saada selville pieniä eroja erilaisten muutos toimintojen välillä.

## 4.2 Tutkimusmenetelmän valinta

Tutkielman teoriaosuus toteutettiin kirjallisuuskatsauksena tutkien aikaisempaa kirjallisuutta liittyen tutkielman aiheeseen. Edellisessä alaluvussa mainittujen rajauksien pohjalta päädyttiin tässä tutkimuksessa käyttämään kvalitatiivista eli laadullista tutkimusmenetelmää tutkielman empiirisessä osuudessa. Laadulliseen tutkimusmenetelmään päädyttiin, koska tutkielmassa halutaan ymmärtää, millä tavalla käyttäjän mobiilisovelluksen käyttö muuttuu yksityisyyshuolien johdosta. Laadullisessa tutkimuksessa pyritään tulkintaan ja toimijoiden näkökulman ymmärtämiseen, kun taas määrällinen tutkimus pyrkii asioiden ennustettavuuteen ja yleistettävyyteen (Hirsjärvi & Hurme, 2001, s. 22). Tämän jaottelun perusteella on valittu laadullinen tutkimusmenetelmä, koska halutaan ymmärtää toimijoiden näkökulmaa siitä, miksi he muuttavat käytöstään ja miten yksityisyyshuolet vaikuttavat tähän muutokseen.

Tutkielman empiirisessä osuudessa tiedonkeruumenetelmänä on käytetty puolistrukturoitua teemahaastattelua. Hirsjärven ja Hurmeen (2001) mukaan haastattelua voidaan pitää yhtenä yleisimmin käytetyistä tiedonkeruumenetelmistä. Haastattelu on joustava menetelmä, jota voidaan käyttää monissa eri tutkimus tarkoituksissa. Haastattelussa ollaan suorassa kielellisessä vuorovaikutuksessa haastateltavan henkilön kanssa, joten tutkimuksen kannalta hyödyllistä tietoa on mahdollista kerätä tutkimustilanteessa. Haastattelun aikana on mahdollista syventää haastateltavalta saatua tietoa kysymällä lisäkysymyksiä tai pyytää lisää perusteluja tai ajatuksia haastateltavalta (Hirsjärvi & Hurme, 2001, s. 34). Haastattelututkimuksessa on useita hyötyjä, mutta myös tämän tutkielman kannalta olennaisia haittoja, joita on otettu huomioon tiedonkeruumenetelmää valittaessa. Hirsjärvi ja Hurme (2001) esittävät keskeisinä etuina sen, että ihminen nähdään tutkimustilanteessa subjektina, jolloin voidaan tuoda esille haastateltavaa koskevia asioita mahdollisimman vapaasti. Toinen heidän mainitsema etu on se, että jo etukäteen tiedetään tutkimuksen aiheen tuottavan monenlaisia vastauksia, joita on etukäteen mahdollisesti vaikea kartoittaa ja tarkasti määritellä. Kolmas etu on se, että haastattelussa on laajemmat mahdollisuudet syventää vastauksia, joka on tämän tutkielman kannalta olennaista. Näin voidaan syvemmin ymmärtää, miksi käyttäjä muuttaa mobiilisovelluksen käyttöä tietyllä tavalla. Hirsjärvi ja Hurme (2001) esittävät myös monenlaisia haittoja, joita haastattelututkimuksen tekemisessä on. Ensimmäisenä haittana he mainitsevat sen, että haastattelijalta vaaditaan kokemusta haastattelututkimuksesta ja myös taitoa haastatella. He ehdottavat myös sitä, että haastattelijan rooliin pitäisi olla erikseen koulutettu henkilö, jota tämän tutkielman resurssien pohjalta ei ole mahdollista saavuttaa. Haastattelussa onkin huomioitu erilaisia seikkoja, jotta kokematon haastattelija pystyisi saamaan mahdollisimman hyviä tuloksia. Hirsjärvi ja Hurme (2001)

mainitsevat, että myös tutkijan ilmeillä, eleillä ja puhetyylillä on vaikutus haastateltavien halukkuuteen vastata kysymyksiin. Haastattelijan pitäisi välttää vaikuttamasta tutkimustuloksiin ilmeillä tai reaktioilla vaan pysyä mahdollisimman neutraalina. Kolmantena haasteena Hirsjärvi ja Hurme (2001) mainitsevat haastattelujen vievän paljon aikaa, niin haastateltavien löytämiseen, aikojen sopimiseen kuin aineiston litterointiin voi tutkijalta kulua merkittävä määrä aikaa ja vaivaa. Haastatteluissa on myös monia virhelähteitä esimerkiksi se, että haastateltava antaa vain sosiaalisesti hyväksyttäviä vastauksia tai pimittää tietoja haastattelijalta. Kaikki hyödyt ja haitat huomioon ottaen sekä verraten haastattelua esimerkiksi kyselylomaketyyliseen tutkimukseen on päädytty kuitenkin siihen, että tutkielmalle hyödyllisintä on kerätä aineisto haastattelujen avulla, jolla voidaan saavuttaa mahdollisimman hyviä tuloksia.

Haastattelu päätettiin toteuttaa puolistrukturoituna teemahaastatteluna. Olennaista puolistrukturoidussa haastattelussa on se, että kysymykset on laadittu etukäteen valmiiksi. Kysymykset voidaan esittää haastattelijan haluamassa järjestyksessä ja niihin on myös mahdollista vastata avoimesti ilman ennalta määriteltyä skaalaa tai vastaustyyliä. Kysymykset ovat kaikkien haastateltavien kesken samat, mutta esimerkiksi haastateltavan esittämät jatkokysymykset voivat erota haastateltavien välillä (Hirsjärvi & Hurme, 2001, s. 47)

## 4.3 Tutkimuksen toteutus

Haastatteluiden haastattelurunko löytyy tämän tutkielman liitteistä (Liite 1). Tutkielman haastattelukysymykset on johdettu olennaisista lähteistä esimerkiksi Xu ym. (2012) MUIPC-mallin mittaristosta, jossa selvitetään käyttäjän yksityisyyshuolia ja käytön aikomuksia tulevaisuudessa. MUIPC-mallin kysymysten lisäksi tutkimuksessa kysyttiin käyttäjän perustietoja kuten ikää, sukupuolta, ammattia (työssä käyvä, opiskelija, työtön vai eläkkeellä), millaisia sovelluksia he käyttävät, onko käytössä oma vai työnantajan puhelin, lataako haastateltava puhelimeensa mobiilisovelluksia, kuinka haastateltava käyttää mobiilisovelluksia ja millaiset mobiilisovellukset käyttäjä kokee itselleen tärkeäksi. Sen jälkeen pyrittiin selvittämään käyttäjän yksityisyysasenteita hyödyntäen MUIPC-mallin kysymyksiä ja muutamia muita kysymyksiä, jotka koettiin relevantiksi tämän tutkimuksen kannalta. MUIPC-mallista otetut kysymykset koskettavat kaikkia mittariston osa-alueita kuten koettua valvontaa, koettua tunkeutumista, tietojen toissijaista käyttöä, aikaisempia yksityisyys kokemuksia ja käytön aikomuksia. Tämän jälkeen siirryttiin kysymään haastateltavalta, onko hän kokenut yksityisyyshuolia jossain tietyssä sovelluksessa ja pyrittiin kartoittamaan paremmin, miten käyttäjän mobiilisovellusten käyttö on muuttunut näiden yksityisyyshuolien seurauksena. Käytön muutoksien mittaamiseen ei löydetty suoraan valmiita kysymyksiä aikaisemmasta tutkimuksesta joten tätä varten kehitettiin omat

kysymykset. Haastateltavalle annetaan lopuksi myös vapaa sana, jotta voidaan käydä läpi mahdollisia lisäkysymyksiä tai haastateltavan ajatuksia sellaisesta aiheesta, jotka eivät tulleet ilmi haastattelukysymyksissä.

Tämän tutkielman haastattelut tehtiin vuoden 2022 keväällä päivämäärillä 30.3.2022-8.4.2022. Vallitseva koronapandemia aiheutti tämän tutkielman kannalta tilanteen, jossa haastateltaville tarjottiin mahdollisuutta fyysiseen haastatteluun tai videon välityksellä tapahtuvaan haastatteluun Zoom-palvelun välityksellä. Vaikka kasvokkainen haastattelu olisi monessa tilanteessa suotuisaa, olosuhteille ei tässä tilanteessa voitu mitään ja sen takia osa haastatteluista on toteutettu etätoteutuksena. Tutkimukseen osallistuvat haastateltavat valittiin tutkijan omista kontakteista pyrkien siihen, että jokaisella haastatteluun osallistuvalla olisi aiheeseen sanottavaa. Osa haastatteluun osallistuneista henkilöistä oli tutkijalle tuttuja henkilöitä. Mukana oli myös useampi tutkijalle ennestään tuntematon haastateltava. Tällä pyrittiin parantamaan tutkielman reliabiliteettia. Haastateltaville kerrottiin etukäteen tutkimuksen tarkoitus, mitä aiotaan tutkia ja kerrottiin myös kuinka kauan haastattelu suurinpiirtein kestää. Todettiin, että jokainen haastattelu kestää vastauksista ja lisäkysymyksistä riippuen 30-60 minuuttia. Tutkimuksessa pyrittiin siihen, että haastattelu kestää maksimissaan tunnin verran. Ennen haastatteluita haastateltaville annetiin täytettäväksi myös ennakkolomake, jolla pyrittiin selvittämään aikaisemmin mainittuja ennakkotietoja ja selvittämään tutkimuskysymyksen kannalta sopivuutta tutkimukseen. Ennen varsinaisia haastatteluja toteutettiin myös muutama testihaastattelu, jolla pyrittiin selvittämään kysymysten sopivuutta ja valmistautua oikeisiin haastattelu tilanteisiin paremmin. Testihaastattelujen pohjalta todettiin, että haastattelurunkoa piti korjata hieman selkeämmäksi ja siihen piti lisätä muutama kysymys, jotta haastateltava ymmärtää aihealueen paremmin. Varsinaisissa haastatteluissa haastateltaville kerrottiin vielä, miten haastattelu tulee etenemään ja kerrottiin, että tutkimus on luottamuksellinen sekä täysin anonyymi. Haastateltaville kerrottiin myös siitä, että haastattelut tullaan äänittämään, jotta tutkimuksen tuloksia kasatessa on helpompi palata kuuntelemaan, mitä haastateltavat olivat vastanneet kysymyksiin. Haastateltaville painotettiin, että äänitteitä ei jaeta muille henkilöille. Viimeiseksi haluttiin korostaa, että haastattelussa ei ole tarkoitus miellyttää haastateltavaa ja olemassa ei ole oikeita tai vääriä vastauksia, oikeat vastaukset ovat niitä, mitä henkilö ajattelee.

Haastattelut kestivät keskimäärin 42 minuuttia. Haastatteluista lyhin oli kestoltaan 34 minuuttia ja pisin haastattelu kesti 47 minuuttia. Haastattelut kestivät yhteensä 332 minuuttia. Haastattelut tallennettiin tutkijan tietokoneelle ja älypuhelimeen. Tietokoneella käytettiin, joko Jyväskylän Yliopiston Zoom alustaa nauhoitukseen tai Applen Voice Memo -sovellusta. Kahdella laitteella äänittäessä oli hyötyä, koska puhelimen mikrofoni oli useasti lähempänä haastateltavaa, jolloin pystyttiin kuulemaan selkeämmin, mitä haastateltava sanoi. Haastattelujen litteraattia syntyi 110 sivua ja litteroinnin jälkeen äänitallenteet poistettiin tutkijan laitteilta.

## 4.4 Tutkimuksen toteutuksen arviointi

Kaikelle tutkimukselle on olennaista, että pyritään luomaan mahdollisimman toistettavia ja luotettavia tuloksia. Tämän vuoksi on tärkeää arvioida tutkimuksen validiteettia ja reliabiliteettia. Hirsjärvi, Remes ja Sajavaara (2009) määrittelevät reliaabeliuden mittaustulosten toistettavuutena. Tällä tarkoitetaan sitä, että tutkimus antaa johdonmukaisia eikä sattumanvaraisia tuloksia. Samoilla tutkimusmenetelmillä ja kysymyksillä pitäisi siis päästä samanlaisiin tuloksiin. Reliabiliteetti voidaan saavuttaa esimerkiksi sillä, että kaksi tutkijaa päätyvät samaan tulokseen. Toinen olennainen käsite Hirsjärven, Remeksen ja Sajavaaran (2009) mukaan on validius. Se tarkoittaa heidän mukaansa "tutkimusmenetelmän kykyä mitata juuri sitä, mitä on tarkoituskin mitata". He antavat esimerkin esimerkiksi siitä, että kyselylomakkeeseen saadaan vastauksia, mutta vastaajat ovat ymmärtäneet kysymykset väärin ja ovat täten vastanneet aiheen vierestä, jolloin kyselyn vastauksista ei ole tutkijalle hyötyä. Laadullisessa tutkimuksessa jossain määrin voidaan ajatella, että koska tutkimuksessa tutkitaan yksilöitä ja heidän uniikkeja ajatuksia aiheesta, ei ole välttämättä mahdollista tuottaa täysin samanlaisia tuloksia, koska jokaisella ihmisellä voi olla täysin erilaiset näkemykset asiasta, joten tuloksetkaan eivät olisi vastaavia. Heidän mukaansa laadullisen tutkimuksen luotettavuutta voidaan parantaa kertomalla tarkasti, miten tutkimus on toteutettu. He mainitsevat tarkkuuden koskevan kaikkia vaiheita tiedonkeruusta tulosten analysointiin asti. Kun analysoidaan laadullista aineistoa, olisi tärkeä kertoa, miten tulokset luokiteltiin ja perustelut luokittelujen taustalla. Jos tutkimus on toteutettu haastattelututkimuksena, tutkimuksen luotettavuutta lisää se, että tekstiin lisätään haastateltavien lainauksia.

Tämän tutkimuksen reliabiliteettia ja validiteettia on pyritty kasvattamaan Hirsjärven, Remeksen ja Sajavaaran (2009) ohjeiden mukaan esimerkiksi pyrkimällä selittämään tutkielman tutkimusmenetelmää mahdollisimman seikkaperäisesti ja kuvailemaan muitakin tutkimusvaiheita, jotta lukijalle tulee mahdollisimman selkeä kuva, mitä on tehty ja mitä metodeja käyttäen. Tutkimuksen tuloksissa on hyödynnetty suoria lainauksia haastateltavilta, jolloin saadaan peilattua ihmisten ajatuksiin tutkielman aiheesta. Mahdollisia ongelmia tämän tutkielman reliabiliteettia ja validiteettia kohtaan on esimerkiksi se, että tutkimukseen osallistui henkilöitä, jotka olivat tutkijalle ennestään tuttuja. Tämä on voinut aiheuttaa sitä, että tutkijalle pyritään antamaan hyväksyttäviä vastauksia tai antamaan vastauksia, jotka haastateltava olettaa haastattelijan haluavan kuulla. Myös se, että kaikki tutkimukseen osallistujat olivat suomalaisia, voidaan tietynlaisena uhkana tutkimuksen reliabiliteetille. Saman tutkimuksen toteuttaminen jossain toisessa maassa voisi saada hyvin erilaisia tuloksia, jotka johtuvat esimerkiksi kulttuurisista tekijöistä. Haastatteluissa reliabiliteettia parannettiin esittämällä

kaikille haastateltaville samat kysymykset ja muotoilemalla kysymykset siten, että ne eivät johdattele tietynlaisiin vastauksiin. Haastattelut litteroitiin huolellisesti haastattelujen jälkeen, jotta tutkielmassa käytetyt lainaukset kuvaavat tarkasti sitä, miten haastateltavat vastasivat haastattelussa.

## 4.5 Aineiston analyysi

Haastattelujen toteutuksen jälkeen ne litteroitiin luettavaan muotoon erilliseen Google Docs-tiedostoon. Litterointia tehdessä alettiin aineistoa jo alustavasti analysoimaan ja alleviivaamaan tiettyjä kohtia, joissa haastateltavat antavat tutkimukselle olennaisia vastauksia. Tämän huomattiin nopeuttavan analyysiä melko paljon, koska litteroinnin jälkeen aineistoon oli huomattavasti helpompi palata tarkempaa analyysiä varten. Aineistoa suositellaan käytäväksi läpi jo litterointi vaiheessa, koska asiat ovat tuoreena mielessä (Hirsjärvi & Hurme, 2001). Hirsjärven ja Hurmeen (2001) mukaan litteroinnin tarkkuudelle ei ole olemassa täysin yksiselitteistä ohjetta. He suosittelevat valitsemaan tarkkuuden tutkimustehtävän mukaan. Tämän tutkielman kannalta ei ollut tarpeellista tehdä erittäin tarkkaa litterointia, jossa tallennetaan haastateltavien jokaiset täytesanat ja äänet, koska ne eivät tällaisessa tutkimuksessa tuota lisäarvoa. Haastattelut pyrittiin siis kirjoittamaan kuten ne oli sanottu, mutta ilman ylimääräisiä täytesanoja ja ääniä. Tällä tavalla pystyttiin tarkasti säilyttämään haastateltavan kertomat asiat ilman, että se vaikeuttaa analyysia ja lainauksien lukemista.

Tämän tyyppisessä tutkimuksessa on olennaista tietää milloin tutkimusaineistoa on kerätty riittävästi, jotta voidaan vastata tutkimuskysymykseen (Eskola & Suoranta, 1996). Tässä tutkimuksessa toteutettiin kahdeksan haastattelua, jonka jälkeen aineiston todettiin olevan tarpeeksi saturoitunut. Saturaatiolla tarkoitetaan tässä yhteydessä tilannetta, jossa aineistosta alkaa toistamaan itseään ja samat teemat alkavat nousta esiin uudelleen ja uudelleen. Tällöin voidaan todeta, että lisähaastattelujen avulla ei välttämättä löydetä enää uutta informaatiota vaan voidaan siirtyä aineiston analyysiin.

Tämän tutkielman aineisto analysoitiin teemoittelun avulla. Hirsjärvi ja Hurme (2001) mainitsevat teemoittelun olevan yksi useista keinoista, jolla teemahaastattelu voidaan analysoida. He kertovat teemoittelun tarkoittavan tapaa, jossa aineistosta usean haastateltavan kohdalla nousee esille samoja piirteitä. Aineistosta tunnistettiin erilaisia käytön muutoksia, joita esiteltiin myös kirjallisuuskatsauksessa. Teemoittelun koettiin olevan luontaisin tapa analysoida aineistoa, koska haastateltavilta tunnistetut käytön muutokset muodostivat valmiita teemoja, joista voitiin johtaa tutkimuksen tuloksia.

# 5 TULOKSET

Haastatteluissa pyrittiin selvittämään henkilöiden ajatuksia ja kokemuksia siitä, miten yksityisyyshuolet olivat saattaneet vaikuttaa heidän mobiilisovellusten käyttöön. Tässä kappaleessa käydään läpi ensin, millaisia yksityisyyshuolia haastateltavat ovat kokeneet ja mistä nämä huolet ovat mahdollisesti voineet johtua. Sen jälkeen siirrytään siihen, miten mobiilisovellusten käyttö muuttui. Tässä hyödynnetään teoriaosuudessa esiteltyjä käytön muutoksia ja yksityisyyden teorioita.

## 5.1 Haastateltavien kokemat yksityisyyshuolet ja niiden syyt

Haastateltavilta pyrittiin ensin selvittämään, millaisia yksityisyyshuolia tai uhkia he kokevat tai ovat kokeneet käyttäessään mobiilisovelluksia. Tämän selvittämiseen käytettiin Xu ym. (2012) MUIPC-tutkimusmallia. Tutkimusmallin valintaan päädyttiin siksi, koska kolmesta tässä tutkielmassa esitellyistä yksityisyyshuolien tutkimusmalleista ainoastaan MUIPC on suunniteltu mobiilipalveluiden kontekstiin. Kaikkein eniten käytetystä CFIP-mallista tunnistettiin myös yksi mallin osa-alue, joka on ristiriidassa käyttäjien toiminnan ja koettujen yksityisyyshuolien kanssa. Smith ym. (1996) mainitsevat virheet käyttäjien tiedoissa yhtenä yksityisyyshuolten tekijänä, mutta kuten Son ja Kim (2008) esittävät käyttäjät saattavat tarkoituksen mukaisesti syöttää vääristeltyjä tietoja sovellukselle suojatakseen yksityisyyttään. Tällaisten havaintojen johdosta päädyttiin käyttämään MUIPC-mallia. Siinä käyttäjien kokemia yksityisyyshuolia selvitetään kysymällä aikaisemmista yksityisyyskokemuksesta, koetusta seurannasta ja tietojen toissijaisesta käytöstä. Kaikkia MUIPC-mallin kysymyksiä ei käytetty, koska esimerkiksi käytön aikomuksiin liittyvät kysymykset olivat vanhentuneita. Kysymykset olivat: aion jakaa tietojani sovelluksille seuraavan vuoden aikana, aion käyttää sovelluksia seuraavan vuoden aikana ja uskon

käyttäväni sovelluksia seuraavan vuoden aikana. Kaikkiin kysymyksiin voitiin haastattelujen perusteella vastata, että haastateltavat käyttävät mobiilisovelluksia ja aikovat jakaa niiden kanssa tietoa, jonka takia voidaan nähdä, että nämä kyseiset kysymykset olivat tämän tutkimuksen osalta vanhentuneita.

Ennen MUIPC-mallin kysymyksiä pyrittiin lyhyesti selvittämään, millaisia yksityisyyshuolia tai uhkia haastateltavat kokevat. Kaikki haastatteluun osallistuneet henkilöt pitivät yksityisyyden suojaamista jollain tasolla tärkeänä. Yksityisyyden suojaamisen tärkeys vaihteli haastateltavien välillä jonkin verran.

> ”Erittäin tärkeäksi” (H6)

> ”No kyllä mä väitän, että se on mulle tärkeää ja mä teen silleen jotain” (H1)

> ”Sanotaan näin, että yritän vaikuttaa siihen niissä tilanteissa. Siis lähes kaikissa tilanteissa missä voin” (H4)

> ”Tärkeäksi” (H5)

H7 kertoi ensin, että ykstyisyyden suojaamisella ei ole merkitystä, mutta myöhemmin oli kuitenkin sitä mieltä, että se on erittäin tärkeää.

> ”No mä oon sitä mieltä, että jos joku haluaa mun tietoja käyttää, käyttäköön, että minulla ei ole niin tärkeitä tietoja minun elämässäni.” (H7)

> ”Ei mulla oo elämässä niin paljon salattavaa, jos joku haluaa käyttää minun tietojani, antaa palaa, kunhan ei vie mun identiteettiä” (H7)

> ”Ei ulkopuolisten ihmisten tarvitse tietää musta yhtään enempää kuin on pakko näyttää.” (H7)

> ”Sit jos se on ihan tahansa joku muu ku se voi olla kuka vaan, niin kyllä se voi käyttää mun tietoja väärin. Käyttää mun kuvia tai käyttää mun muita tietoja, mitä multa löytyy niin johonkin omiin juttuihinsa.” (H7)

Tässä voidaan havaita, että yksityisyys on hyvin yksilöllistä ja kaikki suhtautuvat siihen eri tavoilla. Yksityisyyden suojaamisessa voidaan nähdä olevan eri tasoja, koska H7 ei ollut kovinkaan huolissaan siitä, jos esimerkiksi yritykset tai organisaatiot seuraavat hänen toimintaansa, mutta oli huolissaan siitä, että muut ihmiset voisivat käyttää hänen tietojaan väärin. Tästä yksityisyyshuolesta johtuen H7 mainitsi, että oli esimerkiksi laittanut sosiaalisen median profiilejaan yksityiseksi, eikä esimerkiksi jaa sijaintiaan Snapchat -ystävilleen.

Kysyttäessä siitä, millaisia yksityisyysuhkia haastateltavat kokevat huomattiin, että haastateltavat eivät välttämättä halunneet kutsua tällaisia asioita uhkiksi, vaan pitivät niitä joko epäilyttävänä, arveluttavana tai ärsyttävänä.

> ”No en mä ehkä laskisi yksityisyyden uhkiksi, vaan enemmän sitten mennään mun mielestä toiseen kategoriaan sitten ongelmana.” (H4)

> ”Esimerkiksi jos miettii jotain Facebookia tai näitä, niin musta tuntuu, että jos esimerkiksi puhuu jostain riisikakuista tyyppisesti, niin sitten jonkun 2 tunnin päästä tulee riisikakku mainoksia facebookissa, niin se on vähän ärsyttävää ja niin no ehkä se ei sinänsä ole pelko. Se vaan on silleen turhauttavaa, koska sit tietää tavallaan et kuunnellaan.” (H8)

> ”En mä koe uhkia, mutta tuota täytyy katsoa mihin jakaa ja mitä jakaa ja mihin nimensä laittaa.” (H6)

### 5.1.1 Aikaisemmat yksityisyyskokemukset

Kysyttäessä siitä ovatko haastateltavat kokeneet henkilökohtaisesti, että heidän tietojaan olisi käytetty jollain tavalla väärin tai ilman lupaa ei yhdelläkään haastateltavalla löydetty omakohtaisia kokemuksia tällaisesta tilanteesta. Muutama haastateltava mainitsi vain sellaisia tilanteita, missä heidän sähköpostiin tulee esimerkiksi paljon mainoksia tai roskapostia, joka oli saanut ajattelemaan, että heidän sähköposti oli joutunut vääriin käsiin, mutta näissä tilanteissa haastateltava ei ollut tietoinen mitä kautta ja kenelle sähköposti oli päätynyt.

> ”Tietysti aina aina usein tulee semmoisia tilanteita, että avaa sähköpostin ja sinne on tullut joku roskaposti ja miettii, että mistäköhän tämä sähköpostiosoite nyt on tällä kertaa kiskottu, että niissä tietysti mietityttää vähän se, että onko itse vahingossa laittanut sen sähköpostin johonkin” (H3)

Kun kysyttiin, että ovatko he viimeisen vuoden aikana kuulleet tai lukeneet, että jokin yritys tai organisaatio käyttäisi tietoja väärin, joita ovat keränneet verkosta kertoivat useat haastateltavat, että Facebookin yksityisyyteen liittyvästä uutisoinnista. Yksi haastateltava mainitsi myös Zoomin.

> ”Mä kuulin sen, että oliko sitten yritys nimeltä Cambridge Analytica oli siis tuota tämmöinen data mining yritys tai tämmöinen datan keruu jossa enimmäkseen just Facebookin käyttäytymismalleja ja oliko jopa myös niistä Messenger viesteistä niin oli sitten päätelty niin kuin tehty

> kohdennettua poliittista kampanjaa tai poliittisia mainoksia, joita oli kohdennettu yksilöitä kohden ja siitä tuli silleen skandaali" (H2)

> "Facebookin sun muiden kohdalla onkin selvinnyt, ettei ehkä ihan oikein ole niitten tietoja käytetty." (H5)

> "Itse asiassa kun nyt, kun aloin miettii niin kyllähän jollain niitä tulee välillä jossain WhatsAppissa ja Facebookissa pitää vaihtaa jotkut salasanat, että niistä on vuotanut tietoja." (H8)

> "En mä tiiä vuoden sisällä, mutta eikö noista Facebookin ja noiden WhatsAppin tietosuojasta ollut jotain kohuja olemassa?" (H7)

> "Just nää kaikki Facebookin tai nykyisen Metan silleen epäilyt ja Zuckerbergin oikeudenkäynnit ja muut ja ne isot kohut, mutta siitä kyllä on varmasti yli vuosi että se on nyt silleen aina päällimmäinen mielessä" (H3)

> "Niillä (Zoomilla) oli se silloin korona-aikana, siitä on ehkä vähän yli vuosi sitten, mutta kuitenkin niin oli se, että ne väitti että ne on end to end encrypted ne puhelut mut ei ollutkaan, kusettivat" (H5)

Vaikka tunnistettiin yrityksiä sellaisina toimijoina, jotka olisi mahdollisesti käyttänyt väärin käyttäjiensä tietoja, oli kuitenkin kaikilla asiasta mainitsevilla haastateltavilla käytössä yrityksien sovelluksia puhelimessaan. Haastateltavat kertoivat, että heille yrityksen maineella on vaikutus koettuihin yksityisyyshuoliin ja maineella nähtiin myös olevan vaikutus siihen, miten paljon yksityisyyshuolia koetaan.

> "Lähtökohtaisesti kenellä on huono maine yksityisyyden kohdalla just Meta ja Google niin tottakai se on niitten business, mutta tottakai se vaikuttaa siihen että ei preferoi näitä palveluja versus sitten Apple, joka taas toisella puolella spektrumia et se on tehnyt tai panostanut siihen yksityisyyteen, jolloin myöskin luottaa siihen kunnes toisin käy niin luottaa siihen, mitä he puolestaan sanoo, että miten he tekevät bisnestä, niin tuota kyllä maineella on merkitystä." (H5)

> "Kyllä se luottamus on siinä mielessä mennyt, että kun esim. snapchat tekee niin ei siinä hirveästi luottoa siihen, että sieltä ei tapahdu mitään katastrofaalista, niin sillä ehkä yrittää myös suojella muita eikä pelkästään itseään." (H8)

> "Kyllähän se vähän semmoinen, että nyt kun tuntuu, että Metalla on ollut aika paljon noita tollaisia sekoiluja tuon ihmisten yksityisyyden ja muiden esimerkiksi salasanojen hallinnan kanssa sun muuta, niin kyllä

> siitä tulee semmoinen olo, että ei kyllä hirveästi tee mieli niiden sovelluksia ladata tai käyttää aktiivisesti että.” (H8)

### 5.1.2 Koettu valvonta

Kaikki haastateltavat kokivat kysyttäessä, että sovellukset keräävät käyttäjistä liikaa tietoja, mutta sille ymmärrettiin myös syitä, että sen avulla sovellukset pystyvät tarjoamaan ilmaisia palveluja. Sitä pidettiin kuitenkin häiritsevänä.

> ”No yleisesti ottaen vaan maailmassa tuota kerätään liikaa tietoa, mutta se on se on pelin henki tällä hetkellä.” (H6)

> ”No kyllä siis sanoisin, että monet sovellukset kerää ehdottomasti liikaa kyllä joo semmoisia jotka ne niin kun ottaa vaan kaupan päälle.” (H4)

> ”No joo, koska kyllä suurin osa ainakin tulee semmoinen olo kun niitä kaivataan että, miksi nää edes tarvitsee tätä hommaa? ” (H8)

> ”No joo ja sitten myöskin se että kun sitä tietoa ylipäätään kerätään ei kerrota enää mihin sitä käytetään eikä sitä kerrota silleen selkeästi, että tottakai mä voin käyttää vuosikausia lukea niitä pikku pränttejä, mutta sekin vie aikaa.” (H8)

Välttämättä tiedonkeruu itsessään ei aiheuttanut haastateltavilla yksityisyyshuolia, koska tiedonkeruu koettiin usein olevan massakeruuta. Haastateltavat uskoivat, että yritykset eivät varsinaisesti ole kiinnostuneita yksittäisistä henkilöistä vaan, että he ovat yksi pisara suuremmassa lammessa.

> ”Mun mielestä semmonen niin kuin anonyymi massadata ei ole niin paha, että jos esimerkiksi vaikka silleen. Kaupat vaikka keräisi dataa siitä, että kuinka paljon nyt suomalaiset kuluttaa mitä kahvimerkkejä ja sitten mainostaisi niitä kahvimerkkejä bussipysäkillä, niin se nyt ei mun mielestä ole yhtään niin vakavaa kuin se, että mun kännykkä vieressä kuuntelee ja poimii musta jotain avainsanoja ja sitten yhtäkkiä ilta sanomien sivussa on juuri sopivia mainoksia niin mä en jotenkin koe sitä ehkä ihan niin isona tietoturvauhkana, mutta silti vähän silleen arveluttavana.” (H3)

> “Ei nyt todennäköisesti on, vaan ehkä silleen dataa ison datan joukossa, että ei välttämättä silleen henkilötasolla.” (H2)

On kuitenkin huomioitavaa, että liiallinen kustomointi aiheutti jonkinlaisia yksityisyyshuolia muutamalla haastateltavalla. Koettiin, että jos palvelu on liian

kustomoitu omiin käyttötarpeisiin varsinkin mainonnan osalta, niin sitä pidettiin enemmän huolestuttavana.

> "No sellaisia, että niin kuin se Instagram selkeästi tietää, että kuka minä olen ja mistä minä pidän ja sellaisia huolia niin se on ehkä semmoinen, mistä olen ollut vähän huolestunut, että se tietää niin tarkasti ja ajankohtaisesti esimerkiksi mitä tulee ensimmäisenä siihen näytölle, niin tietää tosi tarkasti, että missä elämänvaiheessa ja tilanteessa olen ja mistä olen juuri silloin kiinnostunut." (H1)

> "Minua alkoi myös silleen jotenkin ahdistamaan se, että kun mä swaippailen Tiktokkia yhtäkkiä sieltä tulee mulle parempia ja kivempiä videoita niin rupesi silleen arveluttamaan tosi paljon, että no mihinköhän tätä käytetään niin sitten tuota poistin sen kokonaan." (H3)

> "No esimerkiksi Googlella voi valita sen, että haluaako personalisoidut ja mainoksia liikkeelle Facebookin semmoinen, niin siinä nyt nousee heti red flagi, että eihän tässä nyt pointtina se, että mä sain sen muka parempia mainoksia vaan että he saa mulle myytyä enemmän tavaraa sitä kautta periaatteessa siinä vaan se todellinen tarkoitus on peitelty silleen mukavasti, että mä saisin siitä enemmän irti." (H5)

### 5.1.3 Tietojen toissijainen käyttö

Tietojen toissijainen käyttö osoittautui haastattelujen perusteella yhdeksi isoksi tekijäksi, joka aiheutti kyseisillä haastateltavilla yksityisyyshuolia. Monet haastateltavat pitivät sitä hyvin ongelmallisena ja huolettavana, mutta osa oli myös ottanut sellaisen asenteen, että jos antaa tietojaan jonnekkin voi niiden olettaa päätyvän tuntemattomien tahojen haltuun.

> "Mietityttää, että mihinköhän sähköposti sitten menee, koska huolestuttaa just nimenomaan se, että jos mä annan sen nyt niin kuin tällä random nettisivulle, niin mihin se sieltä nyt sitten päätyy" (H3)

> "Se, että onko ne varsinaisia uhkia niin sitä en tiedä, mutta ehkä se se tota et tavallaan se, että et tuntematon taho, jolle en ole jakanut tietoja niin tulee tulee tai siis lähestyy tiedoilla jotka on niin kuin hyvinkin spesifisiä." (H4)

> "No siis yleinen käsitys on, että nehän on bisnestä osittain, että ne myydään eteenpäin" (H5)

> “Eiköhän se mene silloin taustalla ilman mun tietoa jonnekin, jossa ne tekee sille datalle jotain, joka sitten taas ei ole mun mielestä hyvä juttu. Ei vaikka se menisi positiiviseen käyttöön.” (H8)

> “Jotenkin musta tuntuu että mä oon ehkä vähän just silleen kyynistynyt ja ottanut enemmän semmosen kannan, että no että kaikki mitä mä laitan someen on kaikkialla ja sitä käytetään kaikilla mahdollisilla tavoilla väärin, että minä en oikein voi sille mitään, mutta lopulta enhän mä tiedä tekeekö se sitä oikeasti.” (H3)

> “Jos on ollut jossain yhteydessä tekemisissä ulkopuolisen yrityksen kanssa ja jakanut sinne tietoja, on se sitten yrityksen tietoja tai niitä omia tietojani ja sitten joku muu lähestyy niillä tiedoilla ja tuota sitä kautta sitten syntyy epäilys, että miksi, miksi näin?” (H4)

## 5.2 Haastateltavien käytön muutokset

Tämän tutkielman tutkimuskysymyksen perusteella kaikkein olennaisin asia oli selvittää, miten haastateltavien yksityisyyshuolet olivat vaikuttaneet heidän mobiilisovellustensa käyttöön. Vastaukset on jaoteltu kirjallisuuskatsauksen kappalejaon mukaan käsitellen käytön muutosten eri tyyppejä.

### 5.2.1 Käytön muokkaaminen

Käytön muokkaamista tapahtui selvästi eniten ja sen koettiin olevan ensisijainen tapa, jolla voidaan vaikuttaa omaan yksityisyyteen ja vähentää yksityisyyshuolia. Ensimmäinen käytön muokkaamisen tapa, joka tuli esille oli väärien tietojen antaminen sovelluksille. Useat haastateltavat mainitsivat antaneensa vääristeltyjä tietoja suojatakseen yksityisyyttään. Tietoja kuten nimi, ikä ja sähköposti pidettiin sellaisina, jotka voitiin helposti väärentää, jos sovellus ei toiminnaltaan vaatinut niiden olevan oikeita.

> “Temporary emails periaatteessa kaikissa tai on nyt ruvennut sanotaanko viimeisen vuoden 2 aikana radikaalisti vähentämään ton pääsähköpostin käyttöä eri palveluissa tai sit mä käytän sitä Apple tarjoamaan, missä voi piilottaa sen.” (H5)

> “Apple Login silloin kun se mahdollistaa anonyymin sisäänkirjautumisen.” (H6)

> “Jos ei se liity mihinkään, enhän mä nyt omaani anna siihen.” (H6)

> "Joo mulla on 2 eri sähköpostiosoitetta. Mulla on semmoinen sähköpostiosoite, minkä mä annan vaan kaikkiin verkkokauppaostoksiin ja sitten mulla on henkilökohtainen sähköpostiosoite, minkä mä annan esimerkiksi sukulaisille tai ihan oikeille persoonille. " (H1)

Tietojen vääristämistä helpottavat myös käyttöjärjestelmien omat yksityisyyttä suojaavat ominaisuudet, joita haastateltavat olivat käyttäneet. Näihin voidaan nähdä esimerkiksi edellisissä lainauksissa mainittu Applen anonyymi sisäänkirjautuminen, asetusten ja oikeuksien muokkaaminen.

> "Säätämällä, vaikka puhelimeen tai selaimen tai muuten yksityisyysasetuksia, että itse ainakin poistanut kai mahdollisimman monesta niin kuin apeissa kaikki käyttöoikeudet mitä ne ei saa kuten esille mitä ei tarvitse." (H2)

> "Ihan WhatsAppissa nimenomaan silleen tosiaan aikaisemmin minulla oli siellä kaikki mahdolliset käyttöluvat, jotka on sittemmin poistanut" (H3)

> "Mutta ulkopuolisista sovelluksista niin taitaa telegram, snapchat ja Instagram olla ainoat, että muilta pyrin kiertämään aina. " (H3)

> "Toinen tapa on se, että kyllä mä katson niitä, siis erityisesti siviilikännykän puolella tulee ehkä kokeellisemmin asennettua sovelluksia niin muokkaan niitä oikeuksia, että kiellän tuota ohjelmistojen pääsy ja kiellän automaatti startteja ja niin edelleen. " (H4)

Jos sovellus tarvitsee toimiakseen esimerkiksi pääsyä kuviin kertoi yksi haastateltava erikseen kopioivansa kuvia ja sen jälkeen lähettävänsä kuvan ilman, että sovelluksella on suoraa pääsyä kuvakirjastoon.

> "Eli esimerkiksi nykyään siis WhatsAppissa, jos haluan jollekin lähettää kuvan niin, kun mulla ei WhatsAppilla ole ollenkaan, sitä kuvien käyttölupaa vaan mä erikseen käyn kameralla sitä kopioimassa kuvaa ja sit mä liitän sen sinne." (H3)

Muut haastateltavat kertoivat muokkaavansa muuten yksityisyysasetuksia esimerkiksi H1 kertoi, ettei Snapchatilla ole ollenkaan pääsyä hänen kuvakirjastoonsa. H2 ja H4 kertoivat, että Android-puhelimella he estävät, että sovellukset eivät voi käynnistyä automaattisesti ja pitävänsä sijaintitiedot pois sovellusten saatavilla. H2 ja H5 kertoivat, että he olivat myös muokanneet asetuksia ja vaihtaneet oletusselaimen turvallisempaan vaihtoehtoon.

Muutama haastateltava kertoi myös, että he olivat piilottaneet omia sosiaalisen median profiilejaan suojatakseen yksityisyyttään.

> "No just silleen, että mulla ei ole julkinen profiili esim instagramissa. Eli mä pystyn tavallaan säätelee sillä, kuka näkee, mitä näkee. Sitten mä en

> koskaan laita tavallaan kotia tavallaan paikaksi sille, että mä yritän tehdä tavallaan sen, missä me asutaan niin mahdollisimman tunnistamattomaksi niille ketkä ei niinkun tarvitse sitä tietoa. ” (H8)

> “Plus mun mielestä oon suojannut, jos et sä ole mun kaveri Facebookissa niin sä et pysty näkemään mun tiedoista kaikkea.” (H8)

> “Sisältöjä ja instagramissakin on just silleen yksityinen käyttötili joka kerta kun saan uuden seuraaminen niin katson, että kuka ihminen se on ja tunnen kun en tunne. No en päästä, että tavallaan yritän pitää silleen niin kuin aika pienellä piirillä” (H3)

Sovelluksien käyttöä oltiin myös monessa tilanteessa pyritty vähentämään ja olemaan enemmän katsojan roolissa sen sijaan, että tuotettaisiin sisältöä sosiaaliseen mediaan.

> “No kyllä sitä varmaan päivittäin tulee käytettyä, mutta silleen, että katsoo vaan muita, että en mä lähde tässä kuvia oikeastaan lähettänyt varmaan vikaan vuoteen tai puoleentoista kenellekään.” (H8)

Sovellusten käytössä ja sosiaalisen median käytössä muutama haastateltava oli myös varovainen siinä, miten muiden ihmisten tietoja voisi päätyä heidän kautta vääriin käsiin ja sitä kautta haluttiin suojata esimerkiksi yhteystietojen antamista.

> “Esimerkiksi tai muita kuvia tai muita yhteystietoja mulla ei taida olla mihinkään jaettuna silleen, että niitä saisi käyttää vapaasti.” (H7)

> “Koen ehkä sen, että mä en halua ottaa vastuuta siitä, jos mun tiedoista päätyy väärien ihmisten käsiin jonkun mun ystävän tietoja tai muuta vastaavaa.” (H7)

> “Kun esim Snapchat tekee, niin ei siinä hirveästi luottoa siihen, että siellä ei tapahdu mitään katastrofaalista, niin sillä ehkä yrittää myös suojella muita eikä pelkästään itseään” (H8)

Haastateltavat mainitsivat myös pitävänsä joitain tällaisia asioita hyvin arkisina, joita ei edes ajattele varsinaisesti yksityisyyden suojaamisena. Tämän perusteella voidaan uskoa, että tässä tutkimuksessa nähtiin ainoastaan jäävuoren huippu siitä, millaisia käytön muutoksia käyttäjät ovat todellisuudessa tehneet.

### 5.2.2 Tauon pitäminen käytöstä

Kaksi haastateltavaa kertoi, että olivat poistaneet Facebookin yksityisyyshuolien takia aikaisemmin, mutta olivat ottaneet sen kuitenkin myöhemmin käyttöön, koska Facebookissa oli sellaisia ryhmiä tai toimintoja, joihin haastateltavat halusivat olla yhteydessä ja joita haastateltavat halusivat käyttää.

> "Halusi poistaa vanhoja julkaisuja ja sen sijaan, että olisi poistanut ne yksi kerrallaa, jota selitti sosiaalisen paineen takia, hän poisti koko Facebookin. Otti sen käyttöön kuitenkin myöhemmin, koska opiskelijaelämää varten sitä tarvitsee paljon." (H1)

> "Poistin Facebookin yhessä vaiheessa, mutta sitten jouduin tekemään sen uudestaan armeijassa, koska kaikki informaatio tuli Facebookin kautta ja sen jälkeen opiskelijan elämässä, mutta vaikka siellä on ollut nyt sen jälkeen, niin voi sanoa, että käyttö on niin pientä, että voisi sanoa sama asia olisi, että ei olisi siis Facebook tiliä enää." (H1)

Molemmat haastateltavat olivat siis halunneet poistaa Facebookin, mutta erilaiset sosiaaliset kontaktit saivat heidät luomaan tilin uudelleen. Käyttöä kuitenkin pyritään minimoimaan ja sitä käytetään vain informaation saantiin eikä sinne varsinaisesti luoda mitään sisältöä.

### 5.2.3 Vaihtaminen

Sovelluksien vaihtamiseen löytyi myös useita esimerkkejä haastateltavilta ja se vaikutti vastausten perusteella olevan toiseksi eniten tehty toiminto käytön muokkaamisen jälkeen. Vaihtaminen ei tarkoittanut kaikille haastateltaville sitä, että jokin sovellus korvataan kokonaan jollain toisella. Vaihtamisella tarkoitettiin myös vanhan sovelluksen jäämistä edelleen käyttöön, mutta pääasiassa uutta sovellusta käytetään toiminnon suorittamiseen. Tällaiset tilanteet tapahtuivat viestintäsovelluksissa. H3 mainitsi myös pyrkineensä vaihtamaan sovellusta, jossa käy keskustelua oman äitinsä kanssa, koska koki yksityisyyshuolia alkuperäisessä sovelluksessa.

> "Itsellä on just Whatsappi siirtynyt telegramiin just sillä niin kuin ajatuksella myös että kokee että se on turvallisempi sitten tai siinä on enemmän turvallisuus ominaisuuksia." (H3)

> "Jos tulee joku uusi tuttavuus, niin yrittää ohjata sitä keskustelua sellaiseen kanavaan, jonka itse kokee turvalliseksi ja just pois vaikka

> sieltä Whatsappin puolelta ja Telegram on semmoinen, että sinne mä oon keskittänyt aika lailla mun silleen kaiken yhteydenpidon.” (H3)

> “Kyllä nyt yrittää silleen Whatsappin käytön siirtää iMessageen, mutta toki sekin aika mahdotonta niiden kanssa, joilla ei ole iPhonea eli sen takia se ei sataprosenttisesti sinne kääntynyt esimerkiksi Whatsapissa, vaikka siitä voisi olla sinänsä hyvä päästä eroon, niin siellä on taas tosi moni ihminen työpaikan Whatsapp- ryhmä ” (H8)

Haastateltavilla esiintyi myös vaihtamiskäytöstä missä jokin sovellus korvataan jollain toisella sovelluksella ja sen jälkeen vanha sovellus poistetaan.

> “Jos sen tarvii vaikka editoida jotain kuvaa, niin sitten jos mun mielestä siihen ei tarvita mun henkilökohtaisia tietoja, sitten usein mä vaan vaihdan sovellusta, että joo jos ei ole mitään painiketta, että sitä voisi ohittaa niin usein vaan poistaa sovelluksen mieluummin kuin annan mitään omia tietoja.” (H2)

> “Mulla on tota sekä tietokoneessa, että kännykässä niin kun en käytä oletusselainta ollenkaan vaan mulla on semmonen Brave browser, joka blokkaa tavallaan kaikki evästeet ja kaikki mainokset ja mahdollisimman laajasti kaiken.” (H3)

Vaihtaessa toiseen palveluun harkittiin sen turvallisuutta, ominaisuuksia ja hintaa. Yksi haastateltava pyrki etsimään avoimen lähdekoodin sovelluksia korvaaviksi sovelluksiksi

> “Yritän etsiä korvaavaa ja silloin se juuri on sitä, että sitten luetaan niitä tietosuojaselostetta ja etsitään vaihtoehtoja. Luetaan mielipiteitä ja kokemuksia siitä, että minkälaista olis tarjolla tähän tarkoitukseen ja sitten aika usein sieltä saattaa löytyä joku semmoinen avoimen tällaisen ohjelmistoprojektin tuote ” (H4)

Toinen haastateltava oli vaihtanut unenseurantasovelluksen korvaavaan maksulliseen palveluun, koska toinen palvelu oli markkinoinut itseään turvallisena vaihtoehtona ja, että maksamalla palvelusta he pystyvät olla keräämättä tietoa.

> “No lähtökohtaisesti semmoiset ilmaiset esimerkiksi uniapit on vähän sketchyjä. Kerää kuitenkin aika paljon dataa ja niistä nyt ei kukaan ota selvää että minne sitten menee. Mutta nyt en oo niitäkään käyttänyt kun esim. oon ostanut tämmöisen maksullisen, joka ei kerää tai lähetä mitään dataa ulospäin.” (H5)

> "No se oli elementti siinä päätöksenteossa, että heillä selkeästi oli tämä heidän mantraansa, että he eivät nimenomaan keräile mitään et se on heidän heidän pointti tässä." (H5)

Myös muut haastateltavat olivat valmiita maksamaan palveluista, jos sitä kautta voitaisiin välttää tietojen keruuta. Oli kuitenkin huomioitava, että haastateltavat tunnistivat tietojen keräämisen olevan täysin mahdollista myös silloin, kun palvelun käytöstä kerätään maksu. Maksullisuus ei siis automaattisesti tarkoita sitä, etteikö käyttäjältä kerättäisi tietoja johonkin tarkoitukseen.

### 5.2.4 Poistaminen

Sovellusten poistaminen on usein paras keino suojata omaa yksityisyyttä, koska poistamisen jälkeen sovelluksella ei ole enää pääsyä käyttäjän tietoihin. H2 ja H6 mainitsivat, että olivat poistaneet omat Facebook-tilinsä kokonaan sen jälkeen, kun he olivat huomanneet sovelluksen keräävän heidän mielestään liikaa dataa. H3 mainitsi poistaneensa Tiktok-sovelluksen sen jälkeen, kun häntä oli alkanut ahdistamaan, miten sovellus kustomoi sisältöä hänen mieltymyksiensä mukaan.

> "Tiktokin poistin vastikään, koska en halunnut kuluttaa siihen paljon aikaa, mutta minua alkoi myös jotenkin ahdistamaan se, että kun mä swaippailen Tiktokkia yhtäkkiä sieltä tulee mulle parempia ja kivempia videoita niin rupesi silleen arveluttamaan tosi paljon, että no mihinköhän tätä käytetään niin sitten tuota poistin sen kokonaan." (H3)

Sovelluksen poistamiseen liittyi usein myös vaihtamiskäyttäytymistä, kuten aiemmassa alaluvussa haastateltavan H5 kohdalla. Hän oli vaihtanut toiseen sovellukseen ja sen jälkeen poistanut vanhan sovelluksen, jota ei enää tarvinnut. H5 oli poistanut myös Snapchat-sovelluksen sen jälkeen, kun hänelle oli noussut yksityisyyshuolia erilaisista ominaisuuksista, joita Snapchat tarjoaa.

> "Eli ensin alkoi yksityisyyshuolet siinä kohtaa, kun siihen lisättiin, missä sä näät missä sun kaverit menee. Mutta sitten yleisesti kuinka paljon dataa he kerää. Myöskin itsellä ei ole käyttöä sille apille, näissä oikeastaan seurasi vaan muutamaa henkilöä silloin tällöin, niin se oli vaan helpompi poistaa sit kokonaan." (H5)

> "Nää muutokset sai sit aikaan, että lopetti miltei käytön kokonaan ja sitten loppujen lopuksi poistin sen apin." (H5)

Tässä tilanteessa on huomattava, että poistamispäätös ei tullut H5:lle yllättäen vaan se oli enemmänkin kasvava huoli, joka johti loppujen lopuksi poistamiseen. H4 kohdalla hän poisti sovelluksia heti, jos ne käyttäytyvät

oudosti tai alkavat kysyä lisää epäsopivia tietoja. H4 poisti sovelluksia myös tilanteessa, jossa sovellus edellytti toimiakseen joitain tietoja, joita H4 ei halunnut antaa.

> "Tosiaan se jos näyttää siltä, että on jotain tietoja, joita en halua sinne antaa ja sovellus sitä edellyttää toimiakseen niin silloin se sovellus saattaa kyllä päästä sovelluskauppaan takaisin." (H4)

> "Se alkaa pyytää esimerkiksi päivityksen jälkeen jotain sellaista tietoa, jota sille ei ole aikaisemmin annettu ja se haluaa siihen luvan niin on mahdollista, että sovellus pääsee poistettavien listalle ja ja poistan sen samantien pyynnön jälkeen." (H4)

> "Jos sovellus toteuttaa jotain yksinkertaista tehtävää, niin en halua sille antaa mitään ylimääräisiä (tietoja)." (H4)

### 5.2.5 Ennaltaehkäisevä toiminta

Haastateltavien vastauksista tunnistettiin myös paljon ennaltaehkäisevää toimintaa, jonka avulla pyrittiin suojaamaan omaa yksityisyyttä. Suurimpana tällaisena oli sovellukseen tutustuminen sovelluskaupassa ennen sen lataamista.

> "On semmoisia sovelluksia, joita en ole asentanut sen takia, että ne pyytää sellaisiin toimintoihin oikeuksia, jota en usko edes niillä selityksillä." (H4)

> "Jos sovelluksen keräämät tiedot on sellaisia, että se ylipäätään paljastaa, että mitä tietoja se kerää, jos se vaikuttaa siltä, että se kerää tietoja, jotka ei kuulu sen sovelluksen toimintaan millään tavalla niin se sovellus jää kyllä asentamatta." (H4)

> "Mä en käytä sovelluksia, mistä mä tiedän, joiden bisnesmalli perustuu siihen (tietojen keräämiseen)." (H5)

> "Mä laitan aika tiukat kriteerit siinä vaiheessa, kun mä lataan sitä sovellusta." (H7)

> "No sillä lailla ennaltaehkäisevästi. Yleensä en edes anna mitään turhia tietoja minnekään, mutta ja pyrin sellaisiin luotettaviin lähteisiin ja käyttämään luotettavien lähteiden palveluja ja sovelluksia, että en ota ihan mitä sattuu. " (H1)

Toinen tapa, jolla pyrittiin toimimaan ennaltaehkäisevästi oli tutustua sovellusten tietosuojaselosteisiin. Kaikki haastateltavat eivät toimineet näin.

Ainoastaan ne tutustuivat sovellusten tietosuojaselosteisiin, jotka kertoivat olevan eniten huolissaan yksityisyydestään.

Ennaltaehkäisevää toimintaa oli myös, että käyttäjät kertovat mahdollisista yksityisyysuhkista omalle lähipiirilleen ja sitä kautta voivat helpottaa yksityisyyden suojaamista. Kysyttäessä, mistä haastateltava oli kuullut yksityisyyshuolia aiheuttavia asioita vastaus oli kaikilla, joko mediasta tai omalta lähipiiriltä.

> "Olisikohan, että poikaystävältä kuulin? Ja kyllä se aika lailla taisi hiipua siihen (Snapchatin käyttö) ja ainakin alkoi miettiä paljon enemmän, että mitä kuvia siellä lähettää. " (H8)

## 5.3 Muutoksia estävät tekijät

Haastateltavien kommenteista tunnistettiin myös esteitä sille, miksi yksityisyyshuolet eivät aina johtaneet muutoksiin. Suurimpana syynä muutoksille nähtiin sovelluksien tarjoamat sosiaaliset verkostot ja sovelluksien tarjoamat hyödyt.

> "Mä en voi vaihtaa Whatsapissa tai jättää Whatsappia kokonaan taakseen, koska niin monet perheestä ja muista tuttavista pelkästään käyttää Whatsappia. Niin en sitten ole kuitenkaan sitä voinut jättää kokonaan pois, mutta ehdottomasti poistanut sen day to day käytöstä." (H2)

> "Whatsapp on sellainen minkä käytön haluaisin lopettaa ihan kokonaan, mutta siellä mun pitää muutama tosi sitkeästi semmoset viestinnän kanavat, joissa on vaan vähän ns. pakko olla mukana." (H2)

> "Poistaminen on käynyt monta kertaa kyllä mielessä, että pitäisikö se koko sovellus (Snapchat) vaan deletoida. Niin sitä ei tarvitsisi miettiä, mutta silleen pikkusiskon kanssa viestiminen pitää minua siellä edelleen tosi hanakasti kyllä, mutta tuota en ole, en ole vielä tehnyt." (H3)

> "Mulla on semmoinen olo, että mä en pysty, koska silloin mä putoaisin tietyistä sosiaalisista ympyröistä kokonaan pois, koska vaikka meillä on työporukalla semmoinen epävirallinen Whatsapp-ryhmä vaan leiristä ja vaihdetaan kuulumisia ja kerrotaan esimerkiksi hauskoja työsattumuksia. Niin siitä yhteydenpidosta putoaisi kokonaan pois ja kokisin, että se olisi mulle siellä työyhteisössä hankalaa." (H3)

> "No ne (viestintäsovellukset) on kuitenkin sellaisia, mitä mä käytän päivittäin ja niissä tapahtuu paljon kommunikaatiota. Niissä olisi vähän

> vaikea sitten yrittää siirtää kaikki muutkin ihmiset niihin muihin palveluihin missä niitä käyttää.” (H7)

> “No en mä välttämättä niin ehkä sanoisin, kun en mä sitä käytä aktiivisesti se (Facebook) on lähinnä sen takia, että siellä on tosi moni esimerkiksi harrastusryhmä sun muu on siellä, jolloin se on vähän pakko käyttää. Mut en mä esim. itsestäni on julkaissut siellä enää mitään pitkiin aikoihin.” (H8)

Muutamilla haastateltavilla oli havaittavissa, myös yksityisyyden paradoksiin viittavaa toimintaa, että kerrottiin olevan huolissaan yksityisyydestä, mutta se ei heijastunut varsinaiseen käyttöön kovinkaan paljon.

> “No joo siis kyllähän täytyy sanoa, että jos sitä sovellusta ei olisi, niin yhteydenpito niin kuin ystäviin olisi haastavampaa ja sillä lailla. Tai heidän kuulumisiaan ei samalla tavalla kuulisi. Niin koen, että se on tässä tapauksessa melkein jopa tärkeämpää, varsinkin koska en koe, että se luo sellaista, niin kuin kyllä mä oon silleen tietoinen, että siinä on omat riskinsä, mutta en koe niitä niin uhkaavina, että vielä siirtyi sinne kun tekemään asialle mitään.” (H1)

Tämän voidaan todeta sillä, että sovellus tuottaa käyttäjälle niin paljon hyötyä, että ei välttämättä välitetä yksityisyydestä niin paljoa tai koettiin myös, että yksityisyyden suojaaminen on tehty käyttäjälle liian vaikeaksi ja jos sovelluksia käyttää paljon voi olla hyvin hankalaa pysyä perässä kaikista muutoksista.

> “No ehkä ajan puutteesta ja siitä, että se on ehkä mun mielestä hyvin haastavaa saada sitä tietoa, että aika monissa paikoissa on sun pitää lukea joku tietosuojaseloste, mistä saat kuulla että mitä sun pitää tehdä, että joo, se on turvallisempaa.” (H7)

Privacy Calculus -teorian mukainen ajattelu oli myös muutamalla haastateltavalla tunnistettavissa. Jos sovelluksen tarjoama hyöty koettiin suuremmaksi, kuin tiedon antamisesta aiheutuvat haitat jaettiin sovelluksille tietoa.

> “Jos joku yksityisyyshuoli on, niin sitten sovellus menee boikottiin. Mikä todennäköisesti on aika mahdotonta nykymaailmassa, jos haluaa olla internetin käyttäjä, niin mun mielestä on siinä aina pakko tehdä trade off vastine.” (H2)

> “Esimerkiksi, jos näytille ottaisi ne oikeudet, että ei anna oikeutta kameran rullaan, eikä anna oikeutta kameraan, eikä mikrofoniin. Niin jos tekisi sitä, että kävisi jumppaamassa niitä oikeuksia päälle ja pois niin sen sovelluksen käyttäminen olisi ihan mahdotonta.” (H1)

Yhtenä esteenä toiminnan muutoksille oli myös se, että jotkin sovellukset, jotka ovat saavuttaneet todella suuren suosion, ei nähty niin pahana. Esimerkiksi yksi haastateltava totesi, että jos niin moni muu ihminen on käyttöehdot hyväksynyt, on niiden hyväksyminen helpompaa itsellekin.

> "Jotain Whatsappin käyttöehtoja tai tällaisia julkisia laajasti käytettyjä, niin ei niitä tule luettua siinä mielessä, että jos kerran kohderyhmä, jonka kanssa haluaa viestiä niillä ja noin 2 miljardia muuta ihmistä on sitä mieltä, että ne on ok niin sitten ne on ok. " (H4)

Muutamassa haastattelussa kävi ilmi myös ajattelua, jossa tietojen koetaan olevan jo menetettyjä, jolloin niiden suojaamiseen eteen ei nähdä enää niin paljoa vaivaa.

# 6 POHDINTA

Tässä luvussa käydään läpi vastaukset tutkimuksen tutkimuskysymykseen, johon pyrittiin vastaamaan niin tutkielman teoriaosuudessa, kuin myös empiirisessä osuudessa. Lisäksi tässä luvussa vertaillaan tutkimuksen tuloksia aiempaan kirjallisuuteen ja arvioidaan niitä kriittisesti sekä käydään läpi, millaisia käytännön vaikutuksia tuloksilla voi olla. Kappaleen lopussa tuodaan esille myös rajoitteet, joita tutkimuksessa oli ja myös mahdolliset jatkotutkimusaiheet. Tutkielma pyrki vastaamaan yhteen tutkimuskysymykseen, joka oli "Miten käyttäjän yksityisyyshuolet vaikuttavat mobiilisovellusten käytön muutoksiin?" Tähän kysymykseen pyrittiin vastaamaan sekä teoria että empiirisessä osuudessa. Tutkimuskysymykseen vastattiin kahdessa osassa. Ensin pyrittiin aikaisemman kirjallisuuden perusteella selvittämään, millaisia yksityisyyshuolia käyttäjät kokevat ja onko niillä jonkinlaista vaikutusta sovellusten käyttöön. Empiirisessä osuudessa pyrittiin saamaan selville, millaisia yksityisyyshuolia haastateltavat ovat kokeneet ja miten nämä huolet olivat vaikuttaneet sovellusten käyttöön.

## 6.1 Johtopäätökset teorian ja tutkimuksen kannalta

Kirjallisuuskatsauksessa saatiin selville, että käyttäjien yksityisyyshuolet voidaan selittää Liun ym. (2014) mukaan seitsemällä tekijällä, jotka ovat:

1. Käyttäjän henkilökohtaisia tietoja kerätään hyvin paljon
2. Käyttäjältä kerätyt tiedot saattavat olla epätarkkoja tai ne voivat sisältää virheitä
3. Organisaatiot, jotka keräävät käyttäjän tietoja eivät välttämättä pysty suojelemaan tietoja, jolloin ulkopuolisille saattaa avautua pääsy tarkastelemaan tietoja
4. Organisaatiot, jotka keräävät käyttäjän tietoja saattavat käyttää niitä tarkoituksiin, jotka ovat käyttäjältä salassa tai jotka ovat epäsopivia. Tällaista toimintaa kutsutaan tietojen toissijaiseksi käytöksi.

5. Organisaatiot, joiden lain mukaiset sopimukset ja selosteet eivät ole kunnossa aiheuttavat käyttäjille yksityisyyshuolia
6. Organisaation ominaisuudet ja maine vaikuttavat käyttäjien yksityisyyshuolten syntymisen
7. Organisaatiot saattavat muuttaa käyttöehtojaan usein ja muutokset voivat jäädä yksilöiltä huomaamatta, joka kasvattaa käyttäjien yksityisyyshuolia

Liun ym. (2014) ensimmäiseen kohtaan löydettiin yhteneväisyyksiä haastatteluista. Haastateltavat kokivat, että heistä kerätään liikaa tietoja ja tämän tiedonkeruu aiheutti heillä yksityisyyshuolia. Liialliselta tiedonkeruulta haastateltavat pyrkivät suojautumaan esimerkiksi muuttamalla sovelluksen yksityisyysasetuksia sellaisiksi, että sovellus ei pystyisi seuraamaan heitä niin tarkasti. Tähän liittyy olennaisesti teoriaosuudessa käsitelty kontekstuaalinen integriteetti. Kontekstuaalisen integriteetin mukaan tietojen keruu liittyy jonkinlaisiin sosiaalisiin normeihin siitä, mitä tietoa on sopivaa kerätä missäkin tilanteessa. H4 kohdalla kontekstuaalista integriteettiä oli rikottu joidenkin sovellusten toimesta, joka oli saanut hänet poistamaan sovelluksia, koska ei halunnut jakaa tietoja näiden kanssa. Myös H6 mainitsi, että oli poistanut sovelluksia siitä syystä, että ne olivat pyytäneet kerätä epäsopivia tietoja häneltä. Liun ym. (2014) toiseen kohtaan ei löydetty yhtäläisyyksiä tämän tutkimuksen tuloksista. Kolmanteen kohtaan haastateltavilla nousi yksityisyyshuolia siitä, että kaikki sovellukset eivät välttämättä pysty suojaamaan tietojaan esimerkiksi tietomurroilta ja sen takia arkaluontoisempien tietojen syöttämistä haluttiin välttää mahdollisimman paljon. Liun ym. neljäs selitys yksityisyyshuolille tuli kaikkein selvimmin ilmi tutkimuksen tuloksissa. Tietojen toissijainen käyttäminen aiheutti paljon yksityisyyshuolia haastateltavilla, koska tiedot koettiin menetetyiksi sattuessaan päätymään kolmansien osapuolien käsiin, jolloin käyttäjällä ei ole enää vaikutusta, miten ja mihin niitä tietoja käytetään. Kaikki haastateltavat tiedostivat, että tietojen toissijaista käyttöä ilmenee sovelluksissa, joita he käyttävät, mutta totesivat ettei asialle voi tehdä mitään. Smith ym. (1996) esitti toissijaisen käytön muodostuvan sisäisestä ja ulkoisesta toissijaisesta käytöstä. Sisäinen toissijainen käyttö ei ollut haastateltavien mielestä yhtä huolestuttavaa, kuin ulkoinen toissijainen käyttö. Vastauksien pohjalta voidaan todeta, että ulkoinen toissijainen käyttö nostaa käyttäjien ykstiyisyyshuolia. Myös aikaisemmassa tutkimuksessa on todettu, että tietojen toissijainen käyttö vaikuttaa positiivisesti käyttäjien kokemiin yksityisyyshuoliin (Xu ym; 2012). Tästä johtuen yksityisyyshuolien tutkimusmalleista CFIP -ja MUIPC-malleissa esitellään tietojen toissijainen käyttö yhtenä merkittävistä yksityisyyshuolien luojista ja se oli selkeästi havaittavissa vastauksissa. Xu ym. (2014) esittämässä MUIPC-tutkimusmallissa mallin painopisteenä on yksilön tunne siitä, että hänellä on oikeus omistaa yksityiset tiedot, mutta ulkoisen tietojen toissijaisen käytön yhteydessä voidaan nähdä tämän oikeuden menetys, koska käyttäjä ei ole tiedon haltija ja ei pysty enää vaikuttamaan sen jakeluun tai käyttöön. Myös liiallinen kustomointi nähtiin tietyissä tilanteissa yksityisyyshuolia

kasvattavana tekijänä. Tämän voidaan nähdä liittyvän tietojen toissijaiseen käyttöön, koska tietoja saatetaan myydä mainostajille, jotka näyttävät käyttäjän mieltymyksien mukaan räätälöityjä mainoksia. Xu ym. (2011) esittää, että kustomointi vaikuttaa positiivisesti koettuun riskiin tiedon jakamisessa. Vaikka palvelua voidaan tehdä hyödyllisemmäksi kustomoimalla sitä kuluttajan aikaisemman datan perusteella, se voi kuitenkin aiheuttaa käyttäjällä yksityisyyshuolia käyttäjän välittäessä paljon yksityisyydestään. Liun ym. viidennelle selittävälle tekijälle ei tämän tutkimuksen yhteydessä löydetty yhteneväisyyksiä. Kuudes tekijä eli organisaation maine tunnistettiin hyvin vahvasti vaikuttavaksi tekijäksi käyttäjien kokemissa yksityisyyshuolissa. Suuret yritykset kuten Meta, Snap, Zoom ja Google nousivat kaikki esille sellaisina toimijoina, jotka aiheuttivat haastateltaville jonkinlaisia yksityisyyshuolia. Mainehaittaan oli kaikkein selvimmin vaikuttanut erilainen negatiivinen uutisointi ja osittain myös se, miten haastateltavien lähipiiri oli puhunut yrityksestä. Negatiivisesti yksityisyyshuoliin maine vaikutti Applen kohdalla, jossa useat haastateltavat kertoivat luottavansa Appleen enemmän kuin aiemmin mainittuihin yrityksiin. Osa kuitenkin nosti esille, että vaikka he käyttävät Applen palveluita ja laitteita eivät he silti halua siihenkään luottaa sokeasti. Jos Applen kohdalla nousisi samantyyppisiä yksityisyyshuolia, kuin muiden toimijoiden kohdalla, olisi reaktio hyvin samanlainen. Liun ym. seitsemäs selitys tunnistettiin myös tutkimuksen tuloksista. Haastateltavat kokivat, että organisaatiot muuttavat käyttöehtojaan usein ja muutosten perässä pysyminen on hyvin vaivalloista. Koettiin myös, että käyttöehdot ovat tehty tavalliselle kuluttajalle liian monimutkaisiksi ja niihin voidaan helposti piilottaa käyttäjälle haitallisia kohtia. Tutkimuksen perusteella ja teoriaan nojaten käyttäjien yksityisyyshuoliin vaikuttaa myös konteksti, jossa käyttäjältä kerätään tietoja. Nissenbaumin (2011) teoria kontekstuaalisesta integriteetistä nähtiin vaikuttavan olennaisesti käyttäjien yksityisyyshuoliin ja varsinkin siitä johtuviin käytön muutoksiin. Jos sovellus keräsi tietoja, jotka eivät oleellisesti liittyneet sen toimintaan, herätti se haastateltavissa yksityisyyshuolia ja motivoi myös käytön muutoksia. Yhteenvetona käyttäjien yksityisyyshuolien syntyyn vaikuttivat siis tiedonkeruun määrä, mitä tietoja käyttäjiltä kerättiin ja missä kontekstissa, organisaation maine ja liiallinen kustomointi.

Käyttäjän yksityisyyshuolia ja sen vaikutuksia mobiilisovellusten käytön muutoksiin voidaan myös tarkastella Sonin ja Kimin (2008) IPPR-mallia hyödyntäen, missä he esittelivät erilaisia tapoja, joilla käyttäjät voivat suojata omaa yksityisyyttään. Tähän malliin peilaten voidaan löytää myös erilaisia tapoja, joilla sovellusten käyttö muuttuu. IPPR-mallin kolme reaktioiden kategoriaa ovat informaatio varaus, yksityinen toiminta ja julkinen toiminta. Informaatiovaraukseen kuuluu kieltäytyminen ja hämäys. Kieltäytymisessä käyttäjä ei suostu antamaan tietojaan sovelluksen käyttöön tai kieltäytyy sen käyttämisestä. Kieltäytymisen esimerkkejä, joita tuloksissa tuli ilmi oli esimerkiksi sovelluksen poistaminen, käyttöehdoista kieltäytyminen ja asetusten muuttaminen siten, että sovellukselle ei anneta pääsyä joihinkin tietoihin. Haastateltavat tunnistivat, että informaatiovaraus voi olla joskus

haastavaa, koska sovellukset yleensä vaativat tietojen jakamista toimiakseen. Son ja Kim (2008) esittävät tähän yhtä ratkaisua, joka on sovelluksen tai palvelun hämääminen. Hämäyksellä tarkoitetaan tilannetta, jossa käyttäjä antaa tietoisesti vääriä tietoja sovelluksen käyttöön. Tutkimuksen tuloksissa tunnistettiin hämäys toimintaa haastateltavilla. Käyttäjät esimerkiksi antoivat anonymisoituja sähköpostiosoitteita sovellusten käyttöön. Sonin ja Kimin (2008) toinen kategoria oli yksityinen toiminta. Tässä kategoriassa he antoivat esimerkkeinä palveluiden boikotointia tai huonojen kokemusten jakamista muiden ihmisten kanssa, koska he ovat tyytymättömiä sovelluksen taustalla olevan organisaation toimintaan. Tutkimuksen tuloksissa tunnistettiin samanlaista toimintaa, missä omalta lähipiiriltä oli kuultu jotain yksityisyyshuolia herättävää, mikä oli vaikuttanut sovelluksen käyttöön. Palvelujen boikotointia esiintyi myös juurikin suurimpien yritysten sovelluksien kohdalla. Boikotointi näkyi eniten siinä, että käyttäjät poistivat boikotoidun sovelluksen puhelimestaan. Kukaan haastateltava ei suoraan maininnut boikotoivansa mitään sovellusta, mutta osan vastauksista voitiin tunnistaa siihen hyvin lähelle viittavaa. Esimerkiksi H5 koki tulleensa huijatuksi Zoomin tietosuojaperiaatteiden johdosta, jonka takia ei halunnut käyttää Zoomia muuta kuin pakon edessä. Henkilökohtaisessa käytössä oli havaittavissa siis boikotti. Kolmantena kategoriana Son ja Kim (2008) esittävät julkista toimintaa. Tällä tarkoitetaan valittamista suoraan yritykselle esimerkiksi tiedonkeruukäytännöistä tai valituksia, jotka on tehty esimerkiksi valvontaviranomaisille. Tämän tutkimuksen tuloksissa ei tunnistettu tällaista toimintaa.

Siirrytään tarkastelemaan käytön muutoksia tarkemmin. Tutkimuksessa todettiin, että yksityisyyshuolilla on vaikutusta sovellusten käytön muutoksiin ja tutkimuksen tuloksissa tunnistettiin useita muutoksen tyyppejä, joilla käyttäjät reagoivat sovelluksen aiheuttamiin yksityisyyshuoliin. Käytön muutoksiin vaikuttaa olennaisesti se, miten tärkeä sovellus on kyseessä ja miten käyttäjä arvioi tiedon jakamisen hyötyjen ja haittojen välisen riskin. Wottrich ym. (2018) esittää, että sovelluksen koettu arvo vaikuttaa positiivisesti aikomukseen hyväksyä tiedonkeruun lupapyyntöjä. Heidän mukaansa jopa kaikkein varovaisimmilla käyttäjillä saatava hyöty voi hetkellisesti ylittää mahdolliset riskit. Tuloksissa tunnistettiin samanlaista toimintaa, jos sovellus koettiin oman elämän kannalta hyvinkin tärkeäksi. Vähemmän tärkeät sovellukset, jotka tuovat lähinnä hedonistista arvoa käyttäjälle, joutuivat herkemmin muutoksien kohteeksi. Kaikki paitsi yksi haastateltava tunnistivat, että sovelluksen tuottama arvo saattaa joskus ylittää ehdottoman yksityisyyden tavoittelun. Tämä ei kuitenkaa tarkoita sitä, että käyttäjät olisivat täysin välinpitämättömiä vaan he silti suojaavat yksityisyyttään useilla eri keinoilla.

Yksi näistä käytön muutoksista, joilla käyttäjät suojasivat yksityisyyttään oli käytön muokkaaminen. Salon ym. (2022) mukaan käytön muokkaamista on esimerkiksi yksityisyysasetusten muokkaaminen, jolloin käyttäjä muokkaa sovelluksen käyttöä esimerkiksi poistamalla seuraamiaan ihmisiä ja sivuja tai vähentää sovelluksen käyttöä. Myös Yang ja Wang (2009) mainitsevat käytön

muokkaamisena esimerkiksi väärien tietojen antamisen. Tutkimuksen tuloksissa tunnistettiin kaikkia näitä käytön muokkaamisen tapoja. Tuloksista kävi myös ilmi, että palveluista oltaisiin myös valmiita maksamaan ja muutama haastateltava oli myös itse käyttänyt rahaa parempaa yksityisyyttä tarjoavaan palveluun. Aiemmassa tutkimuksessa nostetaan esille samanlaisia löydöksiä kuluttajien halukkuudestaa maksaa tiedonkeruun sijasta, jos palvelu on hyödyllinen ja luotettava (Schreiner & Hess, 2015a).

Jos koettiin, ettei käytön muokkaamisella päästy toivottuihin tuloksiin yksityisyyden suojaamisen suhteen saattoi käyttäjä harkita sovelluksen poistamista tai sen vaihtamista johonkin toiseen sovellukseen. Tutkimuksessa huomattiin, että poistamiseen ja vaihtamiseen vaikuttivat usein samantyyppiset lainalaisuudet ja ne saattoivat monessa tilanteessa kulkea käsi kädessä. Tästä esimerkkinä oli haastatteluissa moneen kertaan esille tullut tilanne, jossa sovelluksesta oli vaihdettu toiseen ja sen jälkeen vanha sovellus oli poistettu. Vaihtamisen taustasyitä voidaan mallintaa Bansalin (2005) push-pull-mooring mallilla. Malli koostuu kolmesta muuttujasta. Push-tekijät työntävät käyttäjiä pois nykyisestä sovelluksesta, pull-tekijät vetävät käyttäjiä johonkin toiseen sovellukseen ja mooring-tekijät ovat käyttäjän tilanteeseen ja kontekstiin liittyviä muuttujia, jotka voivat viedä päätöstä suuntaan tai toiseen. Haastatteluissa tuli useasti ilmi esimerkki Whatsappin käyttämisestä ja haastateltavien toiveista saada vaihdettua siitä pois. Whatsappin tapauksessa haastateltavilla push-tekijäksi muodostui Whatsappiin kohdistuvat yksityisyyshuolet, sovelluksen maine ja negatiivinen uutisointi, jotka työnsivät haastateltavia pois sen käytöstä. Pull-tekijöinä toimi korvaavien sovellusten yksityisyysominaisuudet ja parempi maine. Vahvana mooring-tekijänä tässä esimerkissä toimii sosiaalinen verkosto, joka jokaisella haastateltavalla oli hieman erilainen. Joidenkin haastateltavien lähipiiri oli kokonaan Whatsappin ulkopuolella, jolloin Whatsappin vaihtaminen oli helpompaa, mutta muut kokivat, että he eivät pysty kokonaan vaihtamaan pois Whatsappista, koska heidän sosiaaliset verkostot pitävät heidät sen käyttäjinä. Tällainen on hyvä esimerkki mooring-tekijästä, joka estää käyttäjän vaihtoaikeet. Tätä on aiemmassa tutkimuksessa kutsuttu myös vaihtamisen esteeksi, joka johtuu esimerkiksi sosiaalisesta kustannuksesta käyttäjälle (H.-T. Tsai & Huang, 2007) Sovelluksen poistamisen osalta nähtiin hyvin samanlaisia lainalaisuuksia eli yksityisyyshuoli sai käyttäjälle ajatuksen siitä, että sovellukselle pitäisi tehdä jotain ja jos käytön muokkaamisella ei saatu haluttuja tuloksia eikä sovellusta voida korvata jollain toisella, täytyy tehdä päätös käytön lopettamisesta ja sovelluksen poistamiseta. Poistamiseen liittyy samanlaisia tekijöitä, kuin vaihtamiseen, mutta pull-tekijä muuttuu poistamisen toiminnoksi. Push-tekijät edelleen työntävät käyttäjää pois sovelluksesta ja mooring-tekijät yhdessä erilaisten esteiden kanssa vaikuttavat päätökseen poistaa sovellus. Wottrich (2018) nostaa esille, että käyttäjän yksityisyyden suojaamisen motivaatio voi laskea tällaisessa tilanteessa, koska jos sovellus poistetaan ei käyttäjällä ole pääsyä sovelluksessa oleviin tietoihin tai kontakteihin. Tässä palataan jälleen kysymykseen siitä, miten tärkeä sovellus on käyttäjälle ja millaista arvoa se

tuottaa. Jos käyttäjä pitää sovellusta tärkeänä ja se tuottaa käyttäjälle sen verran arvoa, että hyödyt nähdään suurempana kuin haitat sovellusta ei luultavasti poisteta. Jos taas yksityisyyshuolet kasvavat suuremmaksi, kuin sovelluksesta saatava hyöty, on tuloksena käytön loppuminen. Tämä nähtiin tuloksissa esimerkiksi H5 Snapchatin käytön kohdalla. Hänelle oli noussut jo käytön aikana yksityisyyshuolia uusien päivitysten myötä, mutta sovellus oli tuottanut hänelle enemmän arvoa, kuin haittoja, joten sovellus pysyi edelleen käytössä. Kun ajan myötä sovelluksen käyttö väheni ja yksityisyyshuolet kasvoivat voitiin todeta, että vaaka oli kääntynyt sovellusta vastaan ja lopputulos oli sovelluksen poistaminen kokonaan. Poistamiseen liittyi myös tauon pitämistä muutaman haastateltavan kohdalla. Tuloksissa tunnistettiin melkein identtinen tapahtumaketju, minkä York ja Turcotte (2015) kuvailevat tutkimuksessaan taukokäyttäytymisenä Facebookin käyttäjillä. Tämän tutkimuksen tuloksissa kaksi haastateltavaa oli, jossain vaiheessa poistanut Facebookin johtuen yksityisyyshuolista. H1 halusi poistaa vanhan profiilinsa, jossa oli sisältöä, jonka ei halunnut muiden näkevän ja H5 poisti Facebookin yleisien yksityisyyshuolien seurauksena. Molemmat pitivät taukoa Facebookin käytöstä, mutta palasivat käyttämään sitä myöhemmin, koska heidän elämäntilanteensa vaati sen käyttämistä, koska siellä jaettiin heille tärkeää informaatiota. On kuitenkin huomioitavaa, että tässä tilanteessa vaikutti siltä, että kumpikaan ei välttämättä olisi halunnut ottaa palvelua takaisin käyttöön vaan sen arvo heille nousi suuremmaksi, kuin koetut yksityisyyshuolet, jolloin käyttö alkoi uudestaan.

Kuten tässä luvussa on käynyt ilmi, käytön muutoksia esti pääasiassa sovelluksien tarjoamat hyödyt. Hyödyt näkyivät tämän tutkimuksen tuloksissa lähinnä sosiaalisen verkoston muodossa. Haastateltavat kokivat, että sosiaalisten verkostojen takia monet sovellukset tarjosivat niin paljon arvoa, että niiden käyttäminen oli perusteltua, vaikka samaan aikaan he saattoivat kokea samaa sovellusta kohtaan yksityisyyshuolia. Sosiaalisten verkostojen takia käyttäjät kokivat, että sovelluksesta irtautuminen on vaikeampaa, koska heidän lähipiirinsä ei välttämättä löydy vaihtoehtoisista palveluista. Tästä johtuen muutama haastateltava oli esimerkiksi hyväksynyt yksityisyyshuolia herättäneen sovelluksen käyttöehdot, koska niin monet muutkin ovat sen tehneet. Muutoksia esti osalla haastateltavista, myös se, että ei tiedetty millaisia yksityisyysuhkia sovelluksiin liittyy ja mitä kaikkea tulisi edes varoa. Tähän voidaan lisätä, että on huomattava, että kaikilla haastateltavilla ja läheskään kaikilla sovellusten käyttäjillä käyttö ei muutu yksityisyyshuolien seurauksena mitenkään. Vaikka kaikki tähän tutkimukseen osallistuneet pitivät yksityisyyden suojaamista tärkeänä, on mahdollista, että suurin osa kuluttajista ei koe sitä yhtä tärkeänä. Tästä johtuen tämän tutkielman tuloksia kannattaakin tulkita yksityisyystietoisen kuluttajan näkökulmasta ja tuloksia ei voida yleistää koskemaan kaikkia kuluttajia, joiden yksityisyysajattelu voi olla täysin päinvastaista.

## 6.2 Johtopäätökset käytännön kannalta

On huomioitavaa, että nämä tulokset pätevät vain osalle sellaisista käyttäjistä, jotka pitävät yksityisyyden suojaamista tärkeänä edes jollain tavalla ja tietävät erilaisia tapoja suojata yksityisyyttään mobiilisovelluksissa. Haastatteluihin ei tässä tutkimuksessa osallistunut henkilöitä, jotka eivät ole ollenkaan kiinnostuneita suojaamaan yksityisyyttään, joten sellaisten henkilöiden kohdalla tulokset ja käytännön vaikutukset voisivat olla hyvin erilaisia. Voidaan kuitenkin nähdä, että jos olisi tutkittu henkilöitä, jotka eivät ole kiinnostuneita yksityisyyden suojaamisesta ei välttämättä nähtäisi sovelluksen käytössä minkäänlaisia muutoksia tai päinvastaisia, joita tässä tutkimuksessa nähtiin. Jotkut henkilöt saattavat nähdä suurtakin arvoa siinä, että he vaihtavat dataansa parempaan kustomointiin ja parempiin ilmaisiin palveluihin. Tämän perusteella voidaan todeta, että riippuen millaisille käyttäjille sovellus on tarkoitettu, täytyy sovelluksen tiedonkeruun strategian olla sen mukainen. Jos sovelluksen toiminta vaatii kaikkien käyttäjien jakavan tietojaan sovellukseen, on se suunniteltava siten, että jopa kriittisimmät käyttäjät pystyisivät sitä käyttämään esimerkiksi pitämällä tietoja vain laitteella ja myös analysoida pelkästään laitteella. Sovelluksen liiketoiminnan perustuessa vahvasti datan keruuseen, sen myyntiin tai muuhun prosessointiin voidaan tämän tutkimuksen perusteella olettaa sen herättävän yksityisyyshuolia, jotka saattavat aiheuttaa joko datan rajoittamista, palvelun vaihtamisen tai sen poistamisen kokonaan. Sovelluskehittäjille siis tästä tutkimuksesta voidaan kertoa, että jos kerätään paljon käyttäjien tietoja, tulisi tiedon keruulle olla jokin selkeä syy ja siitä tulisi olla hyvin läpinäkyvä käyttäjälle. Näiden toimien avulla voidaan nostaa luottamusta käyttäjän välillä ja heiltä voidaan mahdollisesti kerätä jatkossa enemmän tietoa. Pitkällä aikavälillä ei ole yrityksen edun mukaista, jos suuri osa käyttäjistä haluaa jossain vaiheessa päästä sovelluksesta eroon jos sille löytyy vain jokin korvaaja.

## 6.3 Tutkimuksen rajoitteet

Tutkimuksen selvänä rajoitteena voidaan pitää sitä, että tutkimukseen osallistui suhteellisen pieni määrä henkilöitä, joten kovinkaan yleistettäviä johtopäätöksiä ei voida tehdä tulosten perusteella. Tutkimuksen toteutuksesta tulee myös huomioida, että kaikki haastatteluihin osallistuneet olivat suomalaisia, joka voi vaikuttaa siihen, miten yksityisyyskysymyksiin suhtaudutaan yleisesti ja millaiset asiat pidetään merkityksellisenä. Kaikki tutkimukseen osallistuneet henkilöt kokivat jollain tasolla yksityisyyden suojaamisen tärkeäksi, joten tuloksia täytyy tarkastella näkökulmasta, jossa korostuu käyttäjän tietämys ja

viitseliäisyys omaa yksityisyyttä kohtaan. Tätä ei kuitenkaan pidetty varsinaisesti ongelmana, koska tutkielman tarkoituksena oli tarkastella, miten käyttö muuttuu, jos käyttäjälle nousee yksityisyyshuolia jostain sovelluksesta. Yhtenä vastauksena voitaisiin pitää sitä, että käyttö ei muutu mitenkään, mutta silloin kyse ei olisi varsinaisesti käytön muutoksista. Rajoitteena tutkimuksessa nähtiin myös haastateltavien tausta. Puolet haastateltavista olivat suomalaisia korkeakouluopiskelijoita ja toinen puoli työssäkäyviä, joten tutkimuksen tulokset edustavat vain näitä ihmisiä.

## 6.4 Jatkotutkimusaiheet

Tämän tutkielman perusteella voidaan tarjota muutama jatkotutkimusaihe. Tämän tutkimuksen pohjalta voitaisiin lähteä rakentamaan vieläkin tarkempaa näkemystä siitä, miten käyttö muuttuu yksityisyyshuolien seurauksena. Jatkotutkimus voitaisiin toteuttaa määrällisenä tutkimuksena, johon voitaisiin ottaa osallistujaksi huomattavasti suurempi määrä osallistuja. Tämän avulla voitaisiin laajemmin selvittää, mitkä tekijät selittävät muutoksia ja olisiko käytön muutoksia mahdollista ennustaa tai välttää jollain tavalla. Tulevassa tutkimuksessa kannattaisi hyödyntää mahdollisimman laajaa otantaa erilaisia ihmisiä, jotta saataisiin laajemmin tuloksia. Jatkotutkimukseen voitaisiin liittää myös tarkastelua siitä, miten sovelluksen koettu arvo tai tärkeys vaikuttaa yksityisyyshuolien syntymiseen. Tämä tutkimus osoitti, että sovelluksien tärkeydellä on vaikutusta käyttäjien kokemiin yksityisyyshuoliin. Sen pohjalta voitaisiin kehittää mallia, joka pystyisi kertomaan, miten todennäköisesti käyttäjä kokee yksityisyyshuolia, jos hän kokee sovelluksen olevan hyvin tärkeä. Toinen jatkotutkimusaihe liittyy sovelluksiin kohdistuvien käytön muutoksien luokitteluun. Tämän tutkimuksen alussa esiteltiin erilaisia IT:n käytön muutoksia, jotka oli tunnistettu aikaisemmasta tutkimuksesta. Käytön muutokset, jotka kohdistuvat nimenomaan mobiilisovelluksiin, löytyivät usein toisista konteksteista kuten teknostressin tutkimuksesta. Uskon, että olisi hyödyllistä tehdä lisää tutkimusta siitä, millaisia erilaisia käytön muutoksia käyttäjät tekevät ja kategorisoida niitä systemaattisesti entistä tarkemmin. Kolmantena jatkotutkimusaiheena tarjoan kulttuurien ja alustojen välisten erojen tarkastelua. Koen, että kulttuuri vaikuttaa vahvasti siihen, miten yksityisyyteen suhtaudutaan. Tämän kaltaisten tutkimusten tulokset voisivat erota hyvin paljon toisistaan, jos se toteutettaisiin eri maissa. Myös älypuhelinalustojen vertailu voisi olla mielenkiintoista, jos haluttaisiin selvittää, miten iOS-käyttäjät muuttavat toimintaansa eri tavalla, kuin Android-käyttäjät ja onko näiden muutoksien välillä jotain eroa. Molemmat alustat vetävät puoleensa eri tyyppisiä käyttäjiä ja alustojen tarjoamat yksityisyysominaisuudet ovat toisistaan hyvin erilaisia.

# 7 YHTEENVETO

Sovellusten ja älypuhelinten tultua erottamattomaksi osaksi melkein kaikkien arkea ja tiedonkeruun yleistyttyä valtavasti, sen mukana on oletettavaa, että sovellusten käyttäjille nousee yksityisyyshuolia tietoa kerääviä sovelluksia kohtaan. IT:n käytön muutokset ovat olleet olennainen osa tietojärjestelmätieteen tutkimusta, joten tässä tutkielmassa haluttiin yhdistää yksityisyyden tutkimus ja IT:n käytön tutkimus. Tässä tutkielmassa tutkittiin sitä, miten yksityisyyshuolet vaikuttavat käyttäjien sovellusten käyttöön. Tutkimuksen tutkimuskysymykseksi muodostui: Miten käyttäjän yksityisyyshuolet vaikuttavat mobiilisovellusten käytön muutoksiin?

Tutkielmassa haluttiin ensin tutustua aiheesta tehtyyn aikaisempaan tutkimukseen ja tunnistaa millaisia tutkimusmalleja ja teorioita IT:n käytöstä ja yksityisyyshuolista on luotu aiemmin. Kirjallisuudesta tunnistettiin erilaisia käytön muutoksia, joita pyrittiin sovittamaan yksitysiyyshuolten kontekstiin. Näitä muutoksia olivat esimerkiksi käytön muokkaaminen, sovelluksen vaihtaminen, tauon pitäminen ja sovelluksen käytön lopettaminen kokonaan. Kirjallisuuskatsauksessa määriteltiin myös mitä ovat yksityisyys ja yksityisyyshuolet sekä tutustuttiin yksityisyyshuolien tutkimusmalleihin. Tähän tutkielmaan valikoitui Xu ym. (2014) MUIPC-malli, joka tarkastelee käyttäjien kokemia yksityisyyshuolia mobiilisovelluksissa. Malli koostuu kolmesta vaikuttavasta tekijästä, jotka olivat koettu valvonta, koettu tunkeutuminen ja tietojen toissijainen käyttö. Sen jälkeen esiteltiin Sonin ja Kimin IPPR-malli, joka mallintaa erilaisia reaktioita, joita käyttäjillä saattaa syntyä yksityisyyshuolien johdosta. IPPR-mallin reaktiot olivat informaatio varaukset, yksityinen toiminta ja julkinen toiminta. IPPR-mallin pohjalta oli mahdollista tunnistaa käytön muutoksia tutkielman tuloksissa.

Tutkimuksen empiirinen osuus toteutettiin laadullisena tutkimuksena käyttäen puolistrukturoituja haastatteluja. Tutkimukseen osallistui kahdeksan henkilöä, joista osa oli tutkijalle ennestään tunnettuja, mutta osa oli myös tuntemattomia. Haastatteluihin haluttiin valita tavallisia älypuhelimien käyttäjiä, jotka ovat jollain tapaa kiinnostuneita yksityisyydestään.

Haastatteluista osa suoritettiin etänä ja osa paikan päällä. Haastattelut litteroitiin tulosten analyysia varten.

Tutkimuksessa saatiin selville, että haastatteluun osallistuneille yksityisyyskysymykset olivat jollain tapaa tärkeitä. Haastateltavat eivät kokeneet varsinaista pelkoa tai uhkia yksityisyyttä kohtaan, mutta pitivät monia yksityisyyteen liittyviä kysymyksiä arveluttavana. Haastateltavat eivät olleet henkilökohtaisesti kokeneet yksityisyyden loukkauksia, mutta olivat kuitenkin kaikki kuulleet jonkinlaisesta yksityisyyttä loukkaavasta toiminnasta. Kävikin ilmi, että haastateltavat kokevat epäluottamusta huonomaineisia yrityksiä kohtaan ja näiden yritysten palveluiden käyttö on eniten arveluttavaa, mutta samaan aikaan ristiriitaista. Osa haastateltavista kokivat, että he joutuvat käyttämään joitakin sovelluksia esimerkiksi sosiaalisten verkostojen takia ja tästä syystä he ovat valmiimpia joustamaan myös yksityisyydestään. Tästä voitiin päätellä, että sovelluksen tärkeydellä on olennainen vaikutus siihen, millaisia yksityisyysuhkia käyttäjät kokevat. Sosiaaliset verkostot sovelluksien sisällä olivat tässä tutkimuksessa kaikkein vaikuttavimpia keinoja pitää käyttäjät sovelluksessa yksityisyyshuolista huolimatta. Haastateltaville nousi ykstiysyyshuolia kontekstuaalisen integriteetin rikkomisesta. Jos sovellus keräsi sen kontekstiin sopimattomia tietoja, herätti se haastateltavissa huolia siitä, miksi tietoja kerätään. Aiheutuneet yksityisyyshuolet aiheuttivat haastateltavissa seuraavanlaisia käytön muutoksia. Käytön muokkaaminen oli haastateltaville yleisimpiä tapoja, miten sovelluksen käyttö muuttui yksityisyyshuolten seurauksena. Haastateltavat olivat tarjonneet vääriä tietoja sovelluksille, muokanneet omia yksityisyysasetuksia ja muuttaneet omaa käyttöään sisällöntuottamisesta pelkkään katseluun. Haastateltavat olivat myös pitäneet taukoa sovellusten käytöstä esimerkiksi poistamalla käyttäjätilin ja jonkun ajan päästä palanneet takaisin käyttämään sovellusta. Vaihtaminen nousi myös yhdeksi keskeiseksi tavaksi, jolla haastateltavat pyrkivät suojaamaan yksityisyyttään. Vaihdettaessa uuteen sovellukseen tarkasteltiin yleensä toisen sovelluksen tarjoamaa yksityisyyttä ja ominaisuuksia. Jos toinen sovellus tarjosi parempaa yksityisyyttä ja parempia ominaisuuksia todettiin vaihdon olevan todennäköinen. Osa haastateltavista olivat myös maksaneet korvaavasta tuotteesta, joka tarjoaa parempaa yksityisyyttä. Vaihtamisen suurimpana esteenä pidettiin sosiaalisia verkostoja, koska esimerkiksi viestipalvelua on vaikea vaihtaa, jos uudessa palvelussa ei ole samanlaista verkostoa. Sovellusten poistaminen nähtiin myös ratkaisuna. Monet haastateltavat olivat poistaneet sovelluksia, joita eivät enää kokeneet tarpeelliseksi tai jolle ei tarvittu löytää korvaavaa vaihtoehtoa.

Tutkielman tutkimuskysymykseen löydettiin useita vastauksia yksityisyyshuolien vaikutuksista sovellusten käyttöön, jolloin seurauksena voi olla käytön muokkaamista, tauon pitämistä käytöstä, sovelluksen vaihtaminen tai sovelluksen poistaminen.

# LÄHTEET

Apple. (2022). *Privacy – Features*. Apple. https://www.apple.com/privacy/features/

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological Antecedents and Implications. *MIS Quarterly*, *35*(4), 831–858. https://doi.org/10.2307/41409963

Bansal, H. S. (2005). "Migrating" to New Service Providers: Toward a Unifying Framework of Consumers' Switching Behaviors. *Journal of the Academy of Marketing Science*, *33*(1), 96–115. https://doi.org/10.1177/0092070304267928

Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*, 55–69. https://doi.org/10.1016/j.tele.2019.03.003

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017–1041. https://doi.org/10.2307/41409971

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3), 245–270. https://doi.org/10.1016/S0963-8687(02)00018-5

Bhattacherjee, A., & Park, S. C. (2014). Why end-users move to the cloud: A migration-theoretic analysis. *European Journal of Information Systems*, *23*(3), 357–372. https://doi.org/10.1057/ejis.2013.1

Brown, S. W., & Swartz, T. A. (1984). Consumer Medical Complaint Behavior: Determinants of and Alternatives to Malpractice Litigation. *Journal of Public Policy & Marketing*, *3*, 85–98.

Chandon, P., Wansink, B., & Laurent, G. (2000). A Benefit Congruency

Framework of Sales Promotion Effectiveness. *Journal of Marketing*, *64*(4), 65–81. https://doi.org/10.1509/jmkg.64.4.65.18071

Cho, H., Li, P., & Goh, Z. H. (2020). Privacy Risks, Emotions, and Social Media: A Coping Model of Online Privacy. *ACM Transactions on Computer-Human Interaction*, *27*(6), 1–28. https://doi.org/10.1145/3412367

Clarke, R. (1999). *Roger Clarke's "What's Privacy?"* http://www.rogerclarke.com/DV/Privacy.html

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents—Measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413–422. https://doi.org/10.1080/01449290410001715723

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Ding, Y., & Chai, K. H. (2015). Emotions and continued usage of mobile applications. *Industrial Management & Data Systems*, *115*(5), 833–852. https://doi.org/10.1108/IMDS-11-2014-0338

Doub, A. E., Levin, A., Heath, C. E., & LeVangie, K. (2015). Mobile app-etite: Consumer attitudes towards and use of mobile technology in the context of eating behaviour. *Journal of Direct, Data and Digital Marketing Practice*, *17*(2), 114–129. https://doi.org/10.1057/dddmp.2015.44

Eskola, J., & Suoranta, J. (1996). *Johdatus laadulliseen tutkimukseen*. Lapin yliopisto.

Euroopan Unioni. (2022). *GDPR compliance checklist*. GDPR.Eu. https://gdpr.eu/checklist/

Fodor, M., & Brem, A. (2015). Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany. *Computers in Human Behavior*, *53*, 344–353. https://doi.org/10.1016/j.chb.2015.06.048

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A

systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Google. (2022). *Android Safety Center – Mobile Security & Privacy*. Android. https://www.android.com/safety/

Heinonen, K., & Pura, M. (2008). *Classifying Mobile Services*. 19.

Hirsjärvi, S., & Hurme, H. (2001). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö*. Yliopistopaino.

Keith, M., Thompson, S., Hale, J., & Greer, C. (2012). *Examining the rationality of information disclosure through mobile devices*. *3*.

Kim, G., Shin, B., & Lee, H. G. (2006). A study of factors that affect user intentions toward email service switching. *Information & Management*, *43*(7), 884–893. https://doi.org/10.1016/j.im.2006.08.004

Kohvakka, R. (2018). *Tilastokeskus – Väestön tieto- ja viestintätekniikan käyttö 2018*. Tilastokeskus. https://tilastokeskus.fi/til/sutivi/2018/sutivi_2018_2018-12-04_tie_001_fi.html?ad=notify

Lanier, C. D., & Saini, A. (2008). *Understanding Consumer Privacy: A Review and Future Directions*. 48.

Liu, Z., Shan, J., Bonazzi, R., & Pigneur, Y. (2014). Privacy as a Tradeoff: Introducing the Notion of Privacy Calculus for Context-Aware Mobile Applications. *2014 47th Hawaii International Conference on System Sciences*, 1063–1072. https://doi.org/10.1109/HICSS.2014.138

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Martin, K., & Shilton, K. (2016). Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society*, *32*(3), 200–216. https://doi.org/10.1080/01972243.2016.1153012

Nissenbaum, H. (2004). PRIVACY AS CONTEXTUAL INTEGRITY. *Washington Law Review*, *79*, 39.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus*, *140*(4), 32–48. https://doi.org/10.1162/DAED_a_00113

Pearson, S., & Benameur, A. (2010). Privacy, Security and Trust Issues Arising from Cloud Computing. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, 693–702. https://doi.org/10.1109/CloudCom.2010.66

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, *65*, 409–419. https://doi.org/10.1016/j.chb.2016.09.005

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, *19*(1), 27–41. https://doi.org/10.1509/jppm.19.1.27.16941

Resnick, P., Ko, K., Zeckhauser, R., & Friedman, E. (2000). *Reputation systems | Communications of the ACM*. https://dl.acm.org/doi/abs/10.1145/355112.355122

Salo, M., Pirkkalainen, H., Chua, C., & Koskelainen, T. (2022). Formation and Mitigation of Technostress in the Personal Use of IT. *MIS Quarterly*, *46*. https://doi.org/10.25300/MISQ/2022/14950

Schreiner, M., & Hess, T. (2015a). *Why Are Consumers Willing to Pay for Privacy? An Application of the Privacy-freemium Model to Media Companies*. 17.

Schreiner, M., & Hess, T. (2015b). *Examining the Role of Privacy in Virtual Migration: The Case of WhatsApp and Threema*. 12.

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2347–2356. https://doi.org/10.1145/2556288.2557421

Singh, J. (1989). Determinants of Consumers' Decisions to Seek Third Party Redress: An Empirical Study of Dissatisfied Patients. *The Journal of*

*Consumer Affairs*, *23*(2), 329–363.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, *20*(2), 167–196. https://doi.org/10.2307/249477

Son & Kim. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS Quarterly*, *32*(3), 503. https://doi.org/10.2307/25148854

Stewart, K. A., & Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*, *13*(1), 36–49.

Toch, E., Wang, Y., & Cranor, L. F. (2012). Personalization and privacy: A survey of privacy risks and remedies in personalization-based systems. *User Modeling and User-Adapted Interaction*, *22*(1–2), 203–220. https://doi.org/10.1007/s11257-011-9110-z

Tsai, H.-T., & Huang, H.-C. (2007). Determinants of e-repurchase intentions: An integrative model of quadruple retention drivers. *Information & Management*, *44*(3), 231–239. https://doi.org/10.1016/j.im.2006.11.006

Tsai, J. Y., Kelley, P. G., Cranor, L. Fa., & Sadeh, N. (2010). Location-Sharing Technologies: Privacy Risks and Controls. *I/S: A Journal of Law and Policy for the Information Society*, *6*, 119.

Wang, H., Li, H., & Guo, Y. (2019). Understanding the Evolution of Mobile App Ecosystems: A Longitudinal Measurement Study of Google Play. *The World Wide Web Conference on - WWW '19*, 1988–1999. https://doi.org/10.1145/3308558.3313611

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management*, *18*(4), 326–348. https://doi.org/10.1108/09564230710778128

Woodall, T. (2003). *Conceptualising "Value for the Customer": An Attributional, Structural and Dispositional Analysis*.

Wottrich, V. M., Reijmersdal, E. A., & Smit, E. G. (2019). App Users Unwittingly in the Spotlight: A Model of Privacy Protection in Mobile Apps. *Journal of*

*Consumer Affairs*, *53*(3), 1056–1083. https://doi.org/10.1111/joca.12218

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, *106*, 44–52. https://doi.org/10.1016/j.dss.2017.12.003

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring Mobile Users' Concerns for Information Privacy. *in Proceedings of the 33rd International Conference on Information Systems*.

Yang, H. C. (2013). Bon Appétit for Apps: Young American Consumers' Acceptance of Mobile Applications. *Journal of Computer Information Systems*, *53*(3), 85–96. https://doi.org/10.1080/08874417.2013.11645635

Yang, S., & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *40*(1), 38–51. https://doi.org/10.1145/1496930.1496937

York, C., & Turcotte, J. (2015). Vacationing from Facebook: Adoption, Temporary Discontinuance, and Readoption of an Innovation. *Communication Research Reports*, *32*(1), 54–62. https://doi.org/10.1080/08824096.2014.989975

# LIITE 1 HAASTATTELURUNKO

## Yksityisyys

Ikä?

Sukupuoli?

Työssäkäyvä, opiskelija, eläkkeellä, työtön?

Onko käytössäsi oma vai työnantajan tarjoama puhelin?

Mikä käyttöjärjestelmä puhelimessasi on?

Millaiset tai mitkä sovellukset koet itsellesi tärkeäksi?

## Yksityisyys

Oletko aikaisemmin kokenut tilanteen, jossa jokin organisaatio tai yksilö oli käyttänyt tietojasi väärin tai ilman suostumustasi?

Oletko viimeisen vuoden aikana lukenut tai kuullu, että jokin yritys tai organisaatio käyttäisi väärin tietoja, jotka he ovat keränneet verkosta?

Miten tärkeäksi määrittelisit yksityisyyden suojaamisen itsellesi?

Millaisia yksityisyysuhkia koet?

Koetko suojaavasi yksityisyyttäsi jollain tavalla tällä hetkellä?

Oletko huolissasi siitä, että sovellukset saattavat seurata aktiivisesti toimintaasi?

Koetko, että sovellukset keräävät sinusta liikaa tietoja?

Oletko tietoinen minne sovellukselle antamasi tiedot päätyvät ja mihin niitä käytetään?

Oletko huolissasi siitä, että sovellukset käyttävät tietojasi muihin tarkoituksiin kuin mihin ne oli alunperin kerätty?

Oletko kokenut yksityisyyshuolia, kun olet käyttänyt mobiilisovelluksia?

Muuttuiko käyttösi jotenkin?

Miten sait kuulla tähän sovellukseen kohdistuvasta mahdollisesta uhasta, joka herätti sinussa yksityisyyshuolia?

Koetko, että saatat joskus olla välittämättä yksityisyydestä, jos sovellus tarjoaa sinulle arvoa ja on hyödyllinen?

### Vapaa sana

Tuleeko mieleesi jotain, joka ei käynyt ilmi aikaisemmista kysymyksistä? Tai haluaisitko lisätä vielä jotain?