Uppsala universitet
Inst. för informatik och media

# Vem vet var du är?

## En kvalitativ studie om användares medvetenhet om säkerhetsrisker med platsdelning

*Kajsa Johansson och Rebecka Wenkler*


UPPSALA
UNIVERSITET

Kurs: Examensarbete
Nivå: C
Handledare: Fredrik Bengtsson
Termin: HT-18
Datum: 2019-01-16

# Sammanfattning

Platsdelning finns i många olika sociala medier idag och har blivit en populär funktion. Platsdelning kan vara väldigt användbart i olika situationer när det kommer till att lokalisera personer, men många är omedvetna om de säkerhetsrisker som kan komma till följd av platsdelning. Syftet med studien är att uppmärksamma de säkerhetsrisker som finns i samband med platsdelning och undersöka hur medvetna användare är om dessa. Fokus ligger på de tre mest använda sociala medierna i Sverige; Facebook, Instagram och Snapchat. Studien bygger på ett antal semistrukturerade intervjuer där frågor om användandet av sociala medier, platsdelning och kunskap om säkerhetsrisker resulterar i möjligheten att svara på studiens forskningsfråga. Analysen gjordes utifrån ett teoretiskt ramverk sammansatt av flera grenar inom informationssäkerhet, bland annat C.I.A-triangeln. Informanterna diskuterade problem såsom förföljelse och möjlighet till inbrott när det syntes att man inte var hemma. Slutsatser som kan dras av studien är att flera av informanterna inte såg platsdelning som en säkerhetsrisk, en del för att de inte ansåg sig själva tillräckligt viktiga för att det skulle bli ett hot och andra för att de inte hade kunskapen om vilka säkerhetsrisker som kunde uppstå.

**Nyckelord**

*Informationssäkerhet, säkerhetsrisk, C.I.A-triangel, sociala medier, platsdelning*

# Innehållsförteckning

# 1 Inledning

Hur många i din vänskapskrets har du på sociala medier? Enligt internetstiftelsen i Sverige (2017) har fyra av fem personer ett konto vilket innebär att du med enkelhet kan umgås genom din smartphone. Användningsområdet för smartphones och sociala medier blir bredare i och med att världen blir allt mer digitaliserad (Davidsson & Thoresson, 2017). Många av dessa medier gör det enkelt för användaren att dela med sig av sitt privatliv till vänner och bekanta. Idag är användningen av sociala medier störst bland 16-25-åringar, som dagligen använder sig av dessa för direktkommunikation eller kunskapsutbyte (Davidsson & Thoresson, 2017). De vanligaste sociala medierna bland smartphone-användare är Instagram, Snapchat och Facebook (Internetstiftelsen i Sverige, 2017).

Utbredningen av sociala medier leder till att privat information kan delas snabbt med många olika nätverk på kort tid. En allt mer populär funktion är platsdelning, ett lättanvändligt användargränssnitt i mediet som gör att användaren snabbt och enkelt kan dela sin plats utan längre betänketid (Furini & Tamanini, 2014). Genom att användaren i realtid kan uppdatera sin platsinformation delas platsinformation mellan dem och applikationer så som Instagram, Snapchat och Facebook. Det ger oss möjligheten till bland annat individanpassade restaurangförslag eller kartfunktioner som visar ditt nätverk vilken park du lägger upp en bild ifrån.

Trots att många använder platsdelning dagligen har få kunskap om hur platsinformationen lagras, hanteras och vilka risker delning av personlig information kan utgöra (Vicente et al., 2011). Platsinformation i fel händer kan användas för att utsätta användaren för fara, avslöja känslig information eller identitet (ibid.). De negativa konsekvenser som kan uppstå kan undvikas genom säker hantering av informationen, vilket står i fokus inom informationssäkerhet. Vem är det användaren delar sin platsinformation med egentligen? Vem ser bilden man lägger upp? Och vem äger rättigheterna för platsinformationen?

I och med detta har det uppkommit frågor kring om ägarna bakom applikationen använder platsinformationen i egen vinning uppstått (Mendel et al., 2012). Likaså borde användarna ifrågasätta sitt nätverk, de personer man valt att ha kontakt med i det sociala mediet, och om information kan komma att avslöja något känsligt för dessa, vilket i sin tur utgör en säkerhetsrisk för användaren.

## 1.2 Problemformulering

Platsdelning sociala medier kan komma att utgöra en säkerhetsrisk för användaren. Den brittiska dagstidningen The Guardian publicerade redan år 2012 en artikel om stalkning på

sociala medier och hur det blivit allt vanligare med åren. Artikeln handlar om hur smartphones och sociala medier gör det väldigt mycket lättare för människor att stalka andra, både stalkning som bara handlar om att följa varenda sak en annan person gör online men även att kunna leta upp vart den personen befinner sig. I artikeln nämns flertalet funktioner på sociala medier som gör det möjligt att fysiskt spåra andra och det anses vara en säkerhetsrisk. Det påvisas att detta är ett problem och det vill den här studien uppmärksamma. När man kan lokalisera var en person är kan man även lokalisera var den inte befinner sig eller vilka de befinner sig med vilket också kan ses som en säkerhetsrisk, läs mer om detta under det teoretiska ramverket i 2.2. Det är inte alltid tydligt att platsdelning på statusar och uppladdningar i applikationer sker, vilket lämnar användaren ovetandes om att andra användare kan se vart denne är (Gan & Jenkins, 2015). Användarens integritet kan ifrågasättas när de delar med sig av sitt privatliv, hur kan användaren upprätthålla sin personliga integritet samtidigt som de delar med sig av personlig information om sig själv till både vänner och okända? Och hur stor kunskap har användarna om hur det sociala mediet hanterar den informationen de själva delar med sig när de använder sig av tjänsten?

Användare av social media tycker att det är kul att visa upp sina liv och sina åsikter men är inte alltid medvetna om vilka säkerhetsrisker detta medför (Hallikainen, 2015). Vare sig det är en familjemedlem eller avlägsen bekant som man accepterade för ett flertal år sedan kan båda se ens position om man inte har gjort mer säkrade inställningar som kan säkra ens konfidentialitet. Problemet med informationsdelning på internet har blivit så stort att det utvecklats en modell som kallas C.I.A-triangeln som kan användas för att analysera hur säkert ett informationssystem är (Whitman & Mattord 2016). Det är inte många som har frågat sig själv om de verkligen vill att den där personen de endast träffade en gång för fyra år sedan alltid ska kunna se deras position på diverse olika sociala medier. Med det så kommer även syftet med denna studien.

## 1.3 Syfte och forskningsfrågor

*Syftet med denna studie är att bidra med kunskap om medvetenhet bland systemvetenskapsstudenter i egenskap av användare om säkerhetsrisker med platsdelning i sociala medier.*

För att besvara syftet kommer studien att undersöka vilka säkerhetsrisker som finns med att dela sin position på tre utvalda sociala medier och vilka konsekvenser detta kan få för användaren själv. De potentiella säkerhetsriskerna kopplas ihop med C.I.A-triangeln som är en metod för att mäta informationssäkerhet. Denna metod kollar framför allt på konfidentialitet, integritet och tillgänglighet men även några andra aspekter som har med informationsdelning att göra. För att kunna göra en generalisering bland användarna kommer vi fokusera på Snapchat, Instagram och Facebook då dessa tre sociala medier är bland de mest använda bland svenskar och framförallt bland ungdomar (Internetstiftelsen i

Sverige, 2017).Vidare kommer användaren i den valda målgruppen att stå i fokus genom att undersöka hur dessa personer förhåller sig till de risker som är kopplade till funktioner som möjliggör geolokalisering. Studien ska undersöka varför användare har ett visst beteende på sociala medier och om de aktivt gör något för att motverka säkerhetsrisker sammankopplade med platsdelning.

### 1.3.1 Forskningsfråga

Den frågeställning som ligger till grund för denna studie är:

- *Vilka säkerhetsrisker är användarna inom studiens tänkta målgrupp medvetna om när det kommer till platsdelning?*

## 1.4 Avgränsningar

Denna studie fokuserar på de tre av de mest använda sociala medierna i Sverige; Snapchat, Instagram och Facebook. Studien fokuserar på personer i åldern 20 - 25 då dessa tillhör den målgrupp som använder sociala medier mest (Internetstiftelsen i Sverige, 2017). Informanter ligger inom rätt åldersspann för den tänkta målgruppen och är studenter på Uppsala universitet. Intervjugruppen avgränsades till studenter på Uppsala universitet, vi ansåg att det var viktigt för den korta tidsramen att finna informanter enkelt. I och med att vi själva befann oss i Uppsala kunde vi vara flexibla och då relativt snabbt boka in intervjuer. I Uppsala valde vi att avgränsa oss till att undersöka studenter inom systemvetenskap. Vi fann det intressant att undersöka studenter inom denna utbildning då vi trodde att de hade en större förkunskap och medvetenhet kring säkerhetstänk och datainsamling genom teknik än andra. Tidigare studier har inte fokuserat på utbildningsområde kopplat till säkerhetsmedvetenhet, det gör att denna avgränsning känns extra spännande för att bidra med nytt forskningsområde för vidare studier.

Genom vår egna förkunskap ansåg vi att detta urval skulle göra det enkelt för oss att hitta informanter inom målgruppen, som hade viss förkunskap om platsdelning och förhoppningsvis själva reflekterat över varför eller varför inte de aktiverat denna funktion. Vi anser att ett mindre antal intervjuer var viktigt för att få så uttömmande svar som möjligt under den tid som utgjordes av studiens tidsram. Vi ville få en en så omfattande förståelse för informanternas användande av platsdelning och deras medvetenhet om dess säkerhetsrisker.

## 1.5 Disposition

I *kapitel två* presenteras den teori och tidigare forskning som ligger till grund för hela uppsatsen. Vi förklarar sociala medier, platsdelning och informationssäkerhet utifrån de sociala medier som kommer undersökas. Sist presenteras ett ramverk som kommer användas på intervjuerna för analys.

I *kapitel tre* presenteras tillvägagångssättet för studien. Vi presenterar metoden för studien och redogör för hur urval av informanter har gått till och hur intervjuerna har byggts upp med olika typer av frågor.

I *kapitel fyra* presenteras informanterna som deltagit i studien med den viktigaste bakgrunden som behövs för att förstå deras förhållningssätt. Sedan följer en redogörelse för hur informanterna har svarat på frågor inom fem olika kategorier som ska ligga till grund för analysen.

I *kapitel fem* analyseras det material som kommit av intervjuerna och presenterades i det föregående kapitlet. Det teoretiska ramverket från kapitel två appliceras på materialet för att slutligen leda till svaret på våra forskningsfrågor.

I *kapitel sex* sammanfattas studien och slutsatser dras. Vi reflekterar över hur studien har gått och tar ställning till forskningsfrågan. Vi diskuterar utveckling av studien och fortsatt forskning.

I *kapitel sju* presenteras alla de källor som uppsatsen bygger på i alfabetisk ordning och vart e-källorna kan nås.

I *kapitel åtta* presenteras de bilagor som har varit aktuella under uppbyggnaden av studien.

# 2. Teori och tidigare forskning

*Detta avsnitt avser att förklara väsentliga begrepp och områden för den här studien. I de tre underavsnitten sociala medier, platsdelning och informationssäkerhet presenteras tidigare forskning och teori som är nödvändig för bakgrundsinformation och problematisering av området. Avsnitten följs av diskussion om säkerhetsrisker kopplat till platsdelning, vilket är fokus i denna studie. Sista avsnittet beskriver vårt teoretiska ramverk som kommer användas i analysen. I ramverket sammankopplas risker till följd av platsdelning med fyra egenskaper i en teorimodell inom informationssäkerhet.*

---

## 2.1 Teoretisk bakgrund

### 2.1.1 Sociala medier

När användandet av sociala medier ökar forskas det mer om hur användandet påverkar oss människor. Det har kommit flertalet rapporter om hur det påverkar den psykiska hälsan och hur det har förändrat individens levnadssätt. Den yngre generationen lever sitt sociala liv med hjälp av teknologi i dagens samhälle (Alt, 2017). De använder sig av sociala medier för att hålla kontakten med vänner och familj och knyta kontakter med nya bekantskaper. Det har blivit en självklarhet för dessa att använda sig av sociala medier och för många har det blivit ett till ett beroende. Till följd av det har ett uttryck formats, FoMO - Fear of Missing Out, vilket sammanfattar den rädslan många har för att missa saker i sitt sociala umgänge om de inte ständigt har koll på vad som händer i mobilen (Alt, 2017).

Genom tjänster och funktioner i applikationerna kan användare dela personlig data till sociala medier (Hallikainen, 2015). Organisationer och företag använder sig av sociala medier för att nå ut till till en stor mängd människor. Yrkesmänniskor kan idag sitta under arbetstid och använda sig av sociala medier för att locka nya kunder och marknadsföra sitt företag som en del av sin yrkesroll (Hallikainen, 2015). Då de populäraste sociala medierna är gratis att gå med i, förstår man att det måste finnas något bakomliggande sätt för ägarna av mediet att tjäna pengar. Sociala medier kan utvecklas utan tanke på att tjäna pengar men efter en tid som populärt nätverk tillkommer kostnader för underhåll och utveckling vilket måste betalas (Falch et. al., 2009). Mendels forskargrupp beskriver utbytet mellan sociala medier och dess användare i en rapport om internetfrihet för UNESCO, de förklarar att användarna lämnar ifrån sig privat data "*in return for a 'monetarily free' service"* (Mendel et al., 2012, s. 33).

Det brukar inte förekomma ett ekonomiskt utbyte mellan användare och medie, istället är det mellan medie och partners det sker ett ekonomiskt utbyte (Mendel et al., 2012). Partners syftar på de företag som står för finansieringen av medierna, där reklamannonser utgör den vanligaste intäktsformen (Mendel et al., 2012). I sin tur leder det att nätverken

utnyttjar användaruppgifter i syfte att bättre kunna rikta reklam till rätt målgrupp. Vidare i rapporten från Unesco skriver Mendel et al. att persondata utgör ”the key currency” för att nätverken ska upprätthålla lönsamhet.

Fox och Royne (2018) skriver om hur användarnas medvetenhet påverkas av att de delar privata uppgifter på sociala medier. Det finns en växande rädsla bland användare när det kommer till hur och i vilken utsträckning de sociala medierna samlar in data. Användare blir sårbara när de delar information om sig själva då många användare inte vet vad tjänsterna gör med den (Fox & Royne, 2018). Det finns många föreskrifter om vilken typ av data olika sociala medier samlar in och användarna måste informeras om detta innan de får tillgång till det sociala mediets funktioner. Ändå skriver Fox och Royne (2018) *“Indeed, it is unclear whether consumers truly understand how their personal information such as name, contact information, and birthdate is used by these social networking sites.”*

### 2.1.2 Platsdelning

Det huvudsakliga syftet med platsdelning är att dela en användares position med andra och att sedan ha möjligheten att associera platser i omgivningen till dennes position (Ionescu, 2010). Detta gör att platsdelning i applikationer på mobila enheter vanligen ger mer relevant information än platsinformation från en dator då den kan uppdatera realtid när användaren använder sig av mobilenheten. I användarens smartphone finns ett GPS chip som använder sig av data från satelliter för att beräkna användarens position (Ionescu, 2010).

GPS-teknologi har länge varit en användbar funktion för flera delar av den vanliga internetanvändningen. GPS är ett positioneringssystem som använder sig av satelliter för att lokalisera mottagare (McNeff, 2002). Systemet kan lokalisera en GPS-mottagare vart som helst på jorden. Det syftar till att kunna lokalisera användares position med hög precision för att kunna använda sig av den informationen (Mendel et al., 2012). Samtidigt som användningen av internet ökar så ökar också informationen om användarna vilket har lett till större precision hos tjänster med platsdelning. Funktioner som kombinerar sociala medier och en fysisk plats kallas geosociala nätverk (eng. Geosocial Network) (Europol, 2018). I internet-applikationer som använder sig av platsdelning har användare möjlighet att dela eller tagga bilder, upptäcka vänner eller att checka-in, alltså tillfällen då man markerar vart befinner sig genom en funktion på det sociala mediet (Haynes & Robinson,2015; Vicente et al., 2011). Användargenererat innehåll som associeras med en plats kallas geotagging. Applikationen kan tillåta användaren att specificera en mer generell plats eller sin exakta position. I denna studie kommer ordet platsdelning användas som då inkludera alla de funktioner som visar var en användare befinner sig.

#### *Platsdelning på Snapchat*

År 2011 lanserades applikationen Picaboo som 2012 kom att döpas om till Snapchat (Bernazzani, 2017). Snapchats platsdelningsfunktion heter Snap-kartan, där kan man se

vart ens snap-vänner befinner sig. Man kan publicera offentliga snappar på platsen man befinner sig på så att resten av snapchat-världen kan se dem (Snapchat-support, 2018a). När man installerar appen får man möjlighet att välja om ens plats ska visas eller inte och vilka man vill visa den för. Dessa alternativ går även att ändra under inställningar om man ångrar sitt beslut. Bara de vänner som man själv har valt kan se ens plats, man kan välja att visa den för alla, bara en utvald grupp eller slå på spökläge vilket innebär att ingen kan se vart man är. Ens plats på snap-kartan uppdateras endast när man har appen öppen, och platsen på kartan slutar visas efter ett visst antal timmar.

Snapchat-supporten (2018b) ger några tips för att skydda integriteten medan man använder snap-kartan:

- Välj bara att dela din plats med personer du känner.
- Kontrollera dina sekretessinställningar ofta för att se till att du delar din plats som du vill.
- Skicka bara saker till Vår Story om du inte har något emot att andra människor ser var du är, inklusive gatuskyltar eller andra landmärken

### *Platsedelning på Instagram*

Instagram lanserades 2010, applikationen är utformad för att se och publicera bilder, vilka kan taggas med den plats de är tagna på (Instagram, 2018). Användaren har möjlighet att söka efter platser, då bilder från offentliga konton eller vänners konton med samma GPS-position komma upp. Det går att välja mellan två typer av konton, privat eller offentligt. Om man väljer ett privat konto kan endast de man väljer att acceptera som vänner se de inlägg man gör och då dess geotaggar. Instagrams geotaggar anses som passiva då de kan uppdateras i efterhand, bilden måste inte publiceras på plats.

Tidigare har det funnits en kart-funktion kallad "Photo map", där bilder som taggats visades upp på en världskarta så att man kunde se vilka platser man besökt och dela det med sina vänner och även se deras äventyr. Funktionen togs bort år 2016 efter att ha blivit mycket omtalad i media (Hinchliffe, 2016). Det har spekulerats över om denna förändring kom på grund av av att många kändisars position och annan oönskad information avslöjades i appen (Hill, 2015). Denna funktion delade väldigt många egenskaper med Snapchats nuvarande funktion Snap-kartan. På samma sätt som man i Photo map delade sin plats gör man i Snap-kartan, dock går det inte att hitta någon diskussion om att Snap-kartan också är integritetskränkande.

### *Platsdelning på Facebook*

Facebook har flertalet plats delningsfunktioner, ännu fler om man räknar in funktioner som hör till Messenger. Facebook är det sociala mediet som funnits längst i Sverige, sedan 2006, av de tre vi undersöker och är även det med flest användare (Svenskarna och Internet, 2017). Eftersom Facebook funnits så länge med en stor användargrupp ändras

dess utformning hela tiden efter de funktioner som efterfrågas för tillfället. Precis som på instagram kan man tagga platser när man lägger upp statusar och det finns en funktion som heter "Checka in" där man markerar att man befinner sig på en viss plats (Facebook hjälpcenter, 2018a).

En annan funktion är "Vänner i närheten", den påminner om Snap-kartan och har ändrats en del under åren (Facebook hjälpcenter, 2018b). När funktionen lanserades år 2014 kunde man se exakt var ens vänner befann sig på en karta. Det blev diskussion om att funktionen kunde ses som integritetskränkande vilket gjorde att Facebook gjorde om hur platsdelningen visades. Nu kan man bara se ungefär hur långt avstånd det är mellan en själv och ens vänner, inte exakt var de befinner sig (Karlsson, 2016). En av de nyare platsdelningsmöjligheterna är messengers funktion att dela sin position live på en karta genom ett messenger-meddelande till utvalda vänner under en begränsad tid som man själv väljer (Karlsson, 2017).

Facebooks senaste platsdelningsfunktion kallas Katastrofsvar och ska hjälpa användare att visa sina nära och kära att man mår bra om man befinner sig i närheten av ett terrordåd eller miljökatastrof (Facebook hjälpcenter, 2018c). I funktionen analyserar Facebook ens inställda ort i profilen, aktuell plats om man har gps igång eller om det finns annan aktivitet som kan visa på var man befinner sig. Det är är frivilligt att kryssa i "i säkerhet", ens nätverk kan inte se att man befinner sig på platsen om man inte aktivt väljer att trycka i det.

### 2.1.3 Informationssäkerhet

Med alla nätverksbaserade plattformar som finns idag och alla dess användare blir det en gigantisk mängd information som cirkulerar omkring. Informationssäkerhet fokuserar på hur man bör skydda data från att hamna i fel händer (Whitman & Mattord, 2016). Termen nämns ofta i samband med IT-säkerhet och datasäkerhet då man fokuserar på hela IT-miljön och hur man bäst gör för att skydda den. Information är det som skickas mellan två parter när de kommunicerar med varandra (Whitman & Mattord, 2016). Den är värdefull för om information hamnar i fel händer kan det få negativa följder och därför är det väldigt viktigt att skydda den information som skulle kunna skada individen.

När man talar om informationssäkerhet brukar det vara i samband med företag och organisationer men det är minst lika viktigt att man som privatperson hanterar privat information på ett säkert sätt (informationssäkerhet.se). Säker hantering beror på användarens förhållningssätt till säkerhet och de risker som kan uppstå genom användning. Att ha ett förhållningssätt är enligt Nationalencyklopedin (Nationalencyklopedin, 2018a) när man uttrycker en viss inställning till något. När personen har en attityd gentemot en specifik företeelse.

Vicente och medarbetare (2011) diskuterar att användare saknar kunskap och därför inte är medvetna om vilka risker de utsätter sig för i och med sin användning av platsdelning. *Medvetenhet* syftar till en individs varseblivning och insikter om fysiska samt icke fysiska objekt (Pötzsch, 2009). Tillståndet att vara medveten finns så länge som stimuli är närvarande, stimuli är information från omgivning eller människor. Vidare har modellen CIA-triangeln utvecklats för att öka säkerhetstänket för många (Se fig 1).

### *CIA-triangeln*

C.I.A triangeln är en modell för att analysera säkerheten av ett system för att minimera hot och risker. Ett säkert IT-system bör följa dessa egenskaper för att räknas som säkert. C.I.A står för konfidentialitet (Confidentiality), integritet (Integrity) och tillgänglighet (Availability) (Whitman & Mattord 2016).

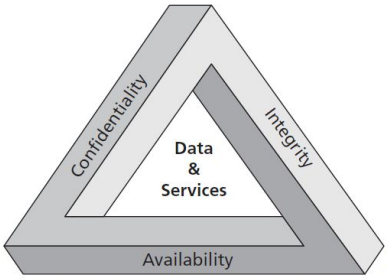


Fig 1. C.I.A-triangeln (Källa: Whitman & Mattord, 2016, s.11)

Informationen som lagras i ett system ska bara nås av rätt personer, den ska vara skyddad mot manipulering och den ska alltid finnas tillgänglig vid behov. Samtidigt som användningen av sociala medier ökar har även hoten ökat och därför har C.I.A triangel utökats med fyra andra egenskaper; riktighet (accuracy), äkthet (authenticity), ägande (possession) och användbarhet (utility).

Nedan följer en förklaring av de sju aspekterna för informationssäkerhet som Whitman och Mattord (2016) formulerat. Den här studien fokusera på de fyra aspekter som har starkast koppling till syftet och markeras i fet stil. I avsnitt 2.2 presenterar vi vår avgränsning av modellen.

***Konfidentialitet*:** Information får inte avslöjas eller vara tillgänglig för fel person.

***Integritet*:** Man ska kunna förlita sig på att informationen är fullständig och oförstörd.

***Riktighet*:** Information ska inte kunna ändras av misstag eller av obehöriga.

***Ägande*:** Det ska vara tydligt vem som äger informationen och vilka som kontrollerar den.

*Tillgänglighet*: Informationen måste finnas tillgänglig och i sin rätta form under alla omständigheter men endast för de som ska ha tillgång till den. Det måste finnas backuplösningar om en olycka sker.

*Användbarhet*: Informationen ska vara användbar i sammanhanget, den ska ha ett värde och inte samlas in i onödan.

*Äkthet*: Informationen ska vara äkta, inte tillverkad eller reproducerad.

### 2.1.4 Platsdelning och säkerhetsrisker

***Vad är en säkerhetsrisk?***

I en studie om terminologi inom området informationssäkerhet som gjorts på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB) defineras termen risk av experter inom olika yrkeskategorier (Andersson, Hedström & Karlsson, 2016). De två beskrivningarna som experterna ansåg bäst definiera termen risk var:

> "En sammanvägning av sannolikheten för att en händelse ska inträffa och de konsekvenser händelsen kan leda till"
>
> "Risk är kombination av sannolikheten för att ett givet hot realiseras och den därmed uppkommande skadekostnaden"
>
> (Andersson, Hedström & Karlsson, 2016, s. 31).

Liknande definition används i en brittisk studie om risker kopplat till sociala medier. Författarna Haynes och Robinson (2015) beskriver att begreppet risk i många fall förklarar sannolikheten för att en ogynnsam händelse ska uppstå. Vidare utgår de ifrån att risker inom sociala medier har en negativ påverkan på individen då personlig information avslöjas. Att ha ett riskbeteende och medvetenhet ställs ofta i relation till individens säkerhet och integritet i sociala medier. (He, 2013; Mendel et al., 2012 ).

Vi har valt att i denna studie använda oss av ordet säkerhetsrisk för att visa på risker som uppkommer i och med användning av platsdelning i sociala medier. Vi ämnar att undersöka säkerhetsrisker som utsätter användare för negativa konsekvenser i och med användning av platsdelning samt medvetenheten om dessa hos användarna.

***Vad finns det för säkerhetsrisker med platsdelning?***

I och med att allt fler sociala medier används på internetuppkopplade enheter uppkommer frågor relaterat till samtycke och kontroll över användarens data från platsdelningstjänster (Mendel et al., 2012). När platsinformation kan associeras till en användares identitet eller kopplas till information denne anser vara privat uppkommer integritetshot (Vicente et al., 2011; Mendel et al., 2012). Vicente och medarbetare delar upp säkerhetsrisker i två kategorier:

*(1) Avslöjandet av känslig platsinformation:* Gäller inte anonyma användare. Den omfattar kategorin sådan information som är kopplat till plats, vilket användaren inte vill att en motståndare ska få tillgång till.

*(2) Identifiering genom platsinformation:* Användarens identitet är inte känd, men genom platsdelning kan motståndare koppla information till andra användare, platser, situationer i syfte att avslöja användarens identitet. Användarnas anonymitet sätts på spel.

Likaså uttrycks orolighet över att individens rörelsemönster kan spåras med en så stor precision, vilket kan komma att användas på fel sätt och hota en individs integritet, och utgöra en säkerhetsrisk. Dessa integritetshot är *Lokalisering av en person*, *Frånvaro av en person*, *Lokalisering för flera personer,* dessa beskrivs närmare nedan med egen översättning Vicente et al. (2011).

1. Lokalisering av en person:
Denna risk innebär att känslig information genom platsdelning som avser användaren avslöjas, t.ex. vanemönster eller hälsoproblem.

2. Frånvaro av en person:
Användarens platsdelning kan antyda om personen inte är på en viss plats vid ett visst tillfälle. I sin tur kan denna information innebära att användare kan göra antaganden om hur långt ifrån en användaren är från en plats eller ej. Detta kan till exempel leda till inbrott när man ser att en bostad står tom.

3. Lokalisering för flera personer:
Geolokalisering kan avslöjas känslig information om flera personer befinner sig vid samma plats vid samma tidpunkt. Här kan frekvens av gånger man besöker en plats tillsammans med andra eller andra användares närvaro vid platsen vara oroväckande. Det kan bli till ett problem om man inte befinner sig med de personerna man sagt att man skulle vara med.

## 2.2 Teoretiskt ramverk

För att kunna analysera materialet från intervjuerna kommer den presenterade teorin användas som ett teoretiskt ramverk. Grunden ligger i säkerhetsriskerna enligt Vicente et al. (2011) och C.I.A-triangeln av Whitman och Mattord (2016). I Studien har vi valt att utgå från de två kategorier av säkerhetsrisker som Vicente et al. (2011) presenterar; avslöjandet av känslig platsinformation och identifiering genom platsinformation. Dessa två kommer båda att sammankopplas med grad av upplevd egenskaper från C.I.A-triangeln.

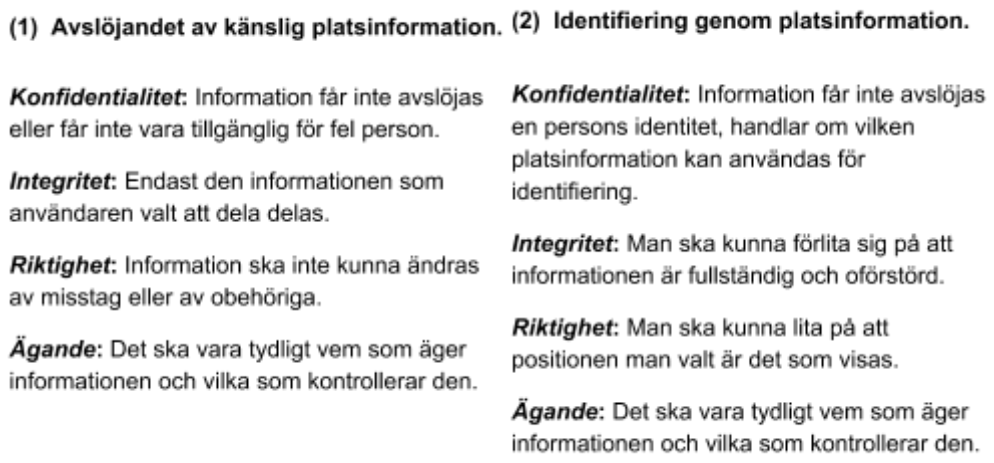


Fig 2. Två kategorier av säkerhetsrisker, kopplat till fyra aspekter i C.I.A-triangeln och platsdelning.

*Konfidentialitet* innebär att information som anses konfidentiell inte får avslöjas eller kan användas för identifiering av användaren (Whitman & Mattord, 2016). I teoriavsnittet belyser vi att användaren själv kan reglera detta genom applikationens säkerhetsinställningar. På Snap-kartan kan användaren undvika den säkerhetsrisken genom att aktivera spökläget (snapchat-support, om Snap-kartan, 2018). Den här egenskapen inom C.I.A kommer att mäta huruvida användare anpassar sitt förhållningssätt, beroende på plats. Detta för att vissa platser eller situationer kan avslöja mer känslig information än andra platser. Konfidentiell information kopplat till plats kan vara sjukhusbesök och tyda på hälsoproblem eller vanemönster hos (Vicente et al., 2011). Det integritetshot som har tydlig koppling till konfidentialiteten är *lokalisering av en person*.

*Integritet* innebär att informationen ska vara fullständig och oförstörd (Whitman & Mattord, 2016). För att inte avslöja känslig platsinformation och kunna hålla sig anonym om så önskas ska användaren vara säker på att informationen lagras säkert och säkerhetsinställningarna är korrekta. Alla de tre tidigare nämnda integritetshoten; lokalisering av en person, avsaknad av en person och lokalisering av flera personer kan uppkomma i och med om integritet upprätthålls eller ej. I en användares fall skulle detta innebära upplevelsen att platsinformationen inte lagras felaktigt, att man litar på att avtal för applikationen är korrekt.

*Riktighet* är nära kopplat till integritet, att informationen inte ändras av misstag eller av någon med onda avsikter (Whitman & Mattord, 2016). Kopplingen till informationssäkerhet innebär hur användaren upplever att denne har kontroll över platsinformationen som den styr över. Användaren ska förlita sig på att exempelvis ägarna av Snapchat inte ändrar inställningar. En sådan ändring skulle kunna leda till att känslig platsinformation avslöjas eller att en användare oönskat delar information i mediet. I teoriavsnittet har det tagits upp hur platsdelning fungerar tekniskt, GPS teknik på mobilen används är att uppdatera platsinformationen i realtid. För att systemet ska uppfattas ha hög

riktighet ska användaren att kunna förlita sig på att sin egna och andra personers platsdelning är fullständig och uppdateras som den ska.

*Ägandet* och kontroll av informationen är sista egenskapen för ett säkert IT-system (Whitman & Mattord, 2016). Användarens förhållningssätt kan bero på upplevelsen av ägande, om man är säker på att data som samlas in inte utnyttjas på fel sätt. Forskning om ekonomiskt utbyte och reklamannonsering inom sociala medier och om en person ser en risk med att bli identifierad kan detta vara en av följderna man upplever oro kring. Utbytet är något som kan påverka upplevelsen av ägande vilket i sin tur utgör en säkerhetsrisk för användaren (Falch et. al., 2009; Mendel et al., 2012). Det är av vikt att tydliggöra för användaren, för att skapa en medvetenhet om vem som äger en applikation samt vad som ägaren kan kontrollera. I sin tur skapas en förståelse för vilken känslig platsinformation som kan komma att avslöjas eller inte.

# 3. Metod

*I detta kapitel förklaras hur studien har gått till. Kapitlet inleds med en sammanfattning av denna kvalitativa studie. Sedan redogörs det för hur datan som ligger till grund för studien samlades in. Kapitlet återger hur våra intervjuer gått till, hur urvalet bestämdes och hur den insamlade datan ska analyseras.*

---

## 3.1 Kvalitativ metod

En kvalitativ studie utfördes för att besvara den tidigare nämnda forskningsfrågan och studiens syfte. Bryman (2012) anser att kvalitativ forskning fokuserar på förståelse av bland annat beteenden eller tankar hos forskningsobjektet. Denna studie bygger på intervjuer för att kunna ge en förståelse för hur människor tänker när det gäller säkerhetsrisker med platsdelning. Vi ville skapa en djupare helhetsförståelse, vilket helst görs med en kvalitativ metod och analys enligt Hjerm et al. (2014), vilket hade stor betydelse för vår urvalsmetod. Vi ville ha en bred intervjugrupp med olika åsikter men som ändå hamnade inom våra urvalskriterier.

Kvalitativ metod möjliggjorde att klargöra begrepp och frågor med informanterna (Kvale & Brinkmann, 2014). Intervjutekniken byggde på en semistrukturerad metod där det fanns flera öppna frågor som lät informanten spekulera själv men att samtalet kunde ledas och ställa följdfrågor. Tekniken ansågs fördelaktigt för att undvika missförstånd eftersom studien bygger på många breda begrepp, begrepp som vi också ville veta hur informanterna tolkar. Detaljerade beskrivningar uppmuntrades och reflektion, därför trodde vi att ett nära deltagande med våra informanter var en fördel. Intervjumallen var uppdelad i tre olika ämnen, från ganska breda frågor till mer ämnesspecifika för att det skulle ge informanten tid och möjlighet att reflektera över sina tankar och beteende.

Subjektiva tolkningar och felaktig kodning av det empiriska materialet kan göra att resultatet påverkas negativt. För att undvika detta gick vi båda igenom det transkriberade materialet och arbetade tillsammans med tematisering samt förde en diskussion när materialet tolkades olika. Validitet mäter hur väl våra intervjufrågor och studie har utformats för att mäta användarnas förhållningssätt och medvetenhet om platsdelning och dess säkerhetsrisker (Kvale & Brinkmann, 2014). Som Bryman (2012) föreslår har vi genomgående haft teori och tidigare forskning i åtanke, vid utformning av intervjufrågor och analys för att uppnå hög validitet. Det transkriberade materialet analyserades till sist i förhållande till det teoretiska ramverket som beskrevs under teoriavsnittet.

## 3.2 Insamling av data

Informationen som ligger till underlag för denna studie kommer från sex intervjuer med personer som passade in i studiens bestämda målgrupp som presenterades under avsnitt

1.4. För att kunna besvara studiens forskningsfråga behövdes informanternas svar om hur de använder sig av platsdelning i sociala medier. Nedan följer en beskrivning av hur insamlingen av data gick till.

### 3.2.1 Förberedande datainsamling

Att inleda med en litteraturstudie var för att skapa en bild av det ämnesområde som vi skulle undersöka. Som Bryman (2012) uttrycker används en litteraturstudie till att skapa förståelse för koncept och teorier inom området samt se vad och hur vår tänkta område har studerats av andra forskare. Genom att inledningsvis skapa en förförståelse inom området kunde teorier och tidigare forskning användas för utformningen av studien. Målet var att hitta forskning från 2010 och framåt då detta ämnesområde är brett och utvecklingen sker i en rasande fart. De artiklar som användes är till största del sådana som har blivit publicerade i tidskrifter om internetanvändning och informationssäkerhet. Fler källor kommer från skrifter beordrade av diverse myndigheter såsom Myndigheten för samhällsskydd och beredskap.

### 3.2.2 Urval

Urvalsmetoden för att få fram för informanter till denna studie var kvoturval. Kvoturval innebär att ett/flera kriterier ställs innan urvalet för informanter utförs (Goldkuhl, 2011). Kritiken som riktas mot kvoturval menar att det inte är helt slumpmässigt och då kan uttalanden och slutsatser inte anses lika tillförlitliga (Oates, 2006). Oates påvisar däremot att om fallstudien har kriterium som också kan gälla andra fall, så kan generaliseringar göras.

Vi inledde datainsamlingen med en förstudie där vi bestämde oss för fyra kriterier att gå efter när vi sökte informanter:

(1) informanterna ska vara mellan 20-25 år.

(2) studerar systemvetenskap, fristående eller program vid Uppsala universitet.

(3) de använder smartphone.

(4) informanterna använder sig av applikationer som tillhandahåller platsdelning.

Inledningsvis sökte vi personer i vår omgivning som föll inom studiens tänkta målgrupp och uppfyllde de tre första kraven för urvalet. Vi ansåg denna metod vara praktisk för få deltagare och enkelt planera in intervjutillfälle. Efter det första kvoturvalet frågade vi om de använde sig utav platsdelning i sociala medier. Utifrån deras svar valdes sex deltagare ut, baserat på vilka som kunde ha intervju med under den tiden vi planerat att hålla dessa. Vi försökte att välja informanter med spridda åsikter angående användning av platsdelning efter den korta förundersökningen för att fånga upp så många tankar som möjligt med den begränsade mängden intervjuer.

### 3.2.3 Etiska överväganden

Genomgående i studien har vi haft i åtanke Vetenskapsrådets (2017) fyra huvudprinciper för intervjuer, dessa är informationskravet, samtyckeskravet, konfidentialitetskravet och nyttjandekravet. Forskningsprinciperna har legat till grund för hur vi arbetat fram vår intervjumall och genomförandet av dessa, för att upprätthålla hög kvalitet.

Vi inledde med hänsyn till informationskravet varje intervju med att deltagarna blev informerade om studiens syfte, att deras medverkan var frivillig och att medverkan kunde avbrytas under intervjuns gång. När personen tackade ja till att delta i intervjun ansåg vi att de samtyckt att medverka i undersökningen. I enlighet med konfidentialitetskravet har vi valt att alla intervjupersoner ska förbli anonyma när vi presenterar resultat och analys i denna studie. Deltagarna fick också godkänna att inspelning av intervjun genomfördes. Fjärde principen, nyttjandekravet, innebär att insamlad data ska användas till det avsedda ändamålet för studien. Därför beskrev vi hur de inspelade intervjutillfällena skulle komma att hanteras och vara till användning för undersökningen samt att dessa enbart är avsedda för den aktuella studien.

### 3.2.4 Intervjumall

Intervjumallen delades in i följande tre områden: (1) Fem bakgrundsfrågor om intervjupersonen, (2) sex allmänna frågor om kunskap och användande, (3) sju frågor som specifikt behandlade säkerhetsrisker med platsdelning och om intervjupersonens egna reflektioner. Vi använde samma intervjumall men vinklade följdfrågorna baserat på om personen använde sig utav platsdelning eller ej.

Dessa områden skulle fånga in studiens syfte och forskningsfrågor så bra som möjligt. Frågorna baserades på tidigare teorier och forskning samt det teoretiska ramverket.

### 3.2.5 Semistrukturerade intervjuer

En semistrukturerad intervjuform tillåter forskarna att anpassa ordningsföljden på huvudfrågor och följdfrågor beroende på informanternas svar och intervjuns riktning (Oates, 2006). Detta passade denna studie bra då både personer som använder platsdelning och de som inte gör det. Vi använde oss av 17 förbestämda huvudfrågor, och dessa frågor var indelade i tre kategorier som skulle fånga in olika områden, se bilaga 1. En inledande del med grundläggande frågor om informanten, sedan en del om användandet av sociala medier och platsdelning och till sist en avslutande del om hur de såg på säkerhetsriskerna med deras användande på svaren i den föreliggande delen. För vissa huvudfrågor hade vi specificerat följdfrågor som vi ställde ut ifall intervjupersonen inte själv tog upp det under samtalets gång.

Eftersom intervjuerna kunde behandla information, som för intervjupersonerna ansågs privat eller känslig, ville vi ha en avslappnad miljö för intervjutillfällena. Eftersom semistrukturerade intervjuer tillåter intervjupersonerna att vara mer delaktiga i strukturen

på intervjun och upplevs mer fri (Hjerm et. al., 2014) ansåg vi att intervjumetoden var en bra insamlingsmetod.

### 3.2.6 Genomförande av intervjuer

Intervjuerna tog plats i Uppsala, de utfördes i grupprum tillhörande universitetsbyggnaden Ekonomikum eller hemma hos informanten. Tillsammans med intervjupersonerna valdes plats för intervjun, för att göra det bekvämt för intervjupersonen. Platsen för intervju behövde uppfylla kriteriet att samtalet skulle kunna hållas så ostört som möjligt, utan onödigt bakgrundsljud eller omgivning som kunde åhöra samtalet.

Intervjun inleddes med en presentation av syftet med uppsatsen, vår definition av platsdelning samt intervjuns tidsupplägg och etiska principer. De semistrukturerade intervjuer blev cirka 30 minuter vardera och utan den föreliggande informationen. Intervjumallen användes för att upprätthålla samma struktur och ordning på frågor under varje intervjutillfälle. Samtalet fördes till större delen av informanterna, de redogjorde för intervjufrågor medan vi stack in med nya frågor eller följdfrågor när informanten hade slut på tankar.

## 3.3 Analys av data

Under intervjuerna samlades väldigt mycket data in som sedan behövde sållas och struktureras upp. De inspelade intervjuerna transkriberades för att sedan kunna tematiseras utifrån olika områden. Sedan analyserades det tematiserade materialet utifrån det teoretiska ramverket vilket förklaras tydligare i 3.3.2.

### 3.3.1 Transkribering och tematisering

Första steget för analys var att transkribera intervjuerna. Detta arbete delade vi upp så att vi tog tre var. Transkriberingarna gjordes så ordagrant som möjligt för att fånga informanternas svar. Under transkriberingen visades sig delar av samtalen vara icke relevant till vår frågeställning och då utelämnades dessa. När transkriberingen var klar påbörjades en tematisk analys på dokumenten för att fånga upp centrala teman i insamlad data. Denna typ av analysmetod passar bra för kvalitativa studier som utgår från insamlad data från intervjuer (Hjerm et al, 2014). I den här studiens utgick vi från det insamlade materialet när vi skapade teman och kategorier för att analysera data. Vi utgick från det transkriberade materialet när vi gemensamt skapade teman och kategorier som sedan skulle analyseras för att besvara vår forskningsfråga.

Först färgkodade vi varje informant, i syfte att urskilja vilken person som kopplades till vilket citat. Detta anser vi var bra för att kunna se samband eller skillnader mellan olika studenters förhållningssätt eller medvetenhet. Vi valde att utgå från de tre olika områden som vår intervjumall avsåg att mäta. Dessa var (1) Användning av sociala medier och platsdelning, (2) För- och nackdelar med platsdelning och (3) Säkerhetsrisker med platsdelning.

För segmenteringen av de transkriberade intervjuerna sållade vi informationen efter Oates (2006) tre segmenteringskategorier; icke användbart material, information kopplat till informanten och material relevant för studiens syfte och forskningsfråga. Vi la mest fokus på sistnämnda punkten, då begrepp eller segment kodades utifrån viktiga nyckelbegrepp från teoriavsnittet. Citat som föll in under något av de tre områdena sparades med informantens färg för att sedan kunna visas i redogörelsen under empiriavsnittet. Processen höll på tills vi ansåg att vi funnit de teman med citat som var mest relevanta för studiens frågeställning och syfte.

### 3.3.2 Implementering av teoretiskt ramverk

Utgångspunkten i analysen var att hitta det som kundes ses som en säkerhetsrisk med hjälp vårt teoretiska ramverk baserat på studien från Vicentes forskargrupp och modellen C.I.A-triangeln. I analysen placerades de extraherade riskerna under någon av de två kategorier av säkerhetsrisker som Vicentes forskargrupp (2011) formulerat. Genom att se om våra användare var medvetna eller upplevde att avslöjandet av information och/eller identifiering genom platsdelning var en säkerhetsrisk kunde vi därefter se hur deras förhållningssätt var gentemot respektive kategori. Informanternas svar genomsöktes efter perception, känslor samt beteende som kunde kopplas till medvetenhet eller förhållningssätt och som kunde ge förståelse om hur de relaterade till informationssäkerhet. De olika riskerna analyserades sedan efter vilken aspekt inom C.I.A-triangeln det var ett hot mot och om det kunde avslöja information om lokalisering av en person, flera personer eller frånvaro av en person.

I det teoretiska ramverket har vi valt att använda oss av fyra av C.I.A-triangelns aspekter, dessa fyra är de som passar bäst in med studiens syfte enligt. Under tematiseringen kom det fram att några av aspekterna var väldigt lika och kunde användas på liknande sätt för att mäta informationssäkerhet, gränsen drogs vid dessa för att kunna redovisa ett resultat på ett lättförståeligt sätt.

# 4. Empiri

*Inledningsvis presenterar vi informanterna som ställt upp på våra intervjuer med den bakgrundsinformationen som behövs för att man ska få en bild av dem. Sedan presenteras det informanterna har tagit upp under sina intervjuer under fyra olika kategorier som fångar in det som behövs för att göra en analys på det.*

---

## 4.1 Presentation av informanter

*Informant ett* använde sig av alla sociala medier som tas upp i denna studie. Denne ansåg sig mest aktiv på snapchat där den hade Snap-kartan igång jämt, dock hade denne ett litet antal vänner på mediet. Den använde sig av instagram och facebook men mer passivt, gjorde inga egna inlägg utan observerade bara andra. Man fick intrycket av att informanten hade bra koll på säkerhetsrisker och hade ett högt säkerhetstänk men ansåg inte att platsdelning var en risk för denne.

*Informant två* använde sig av alla sociala medier. Studenten var mest aktiv på snapchat där personen delade plats med väldigt många genom Snap-kartan. Studenten hade öppet konto på instagram, där bilder ofta taggades med plats. Personen ansåg sig ha mest koll på platsdelning angående dessa två medier, medan ansåg att hen hade mindre kunskap om vilka funktioner med platsdelning som Facebook erbjöd. Informanten reflekterade mycket under intervjuns gång om sitt kontaktnät på de olika medierna. Efter intervjun anpassade studenten sina sekretessinställningar på Snapchat för vilka som kunde se.

*Informant tre* använde sig av alla sociala medier. Studenten var mest aktiv på snapchat då den vid intervjun hade Snap-kartan igång och ansåg snapchat som dennes mest använda medie. Hen hade ett ganska stort antal vänner och hade inte några specifika säkerhetsinställningar utan alla kunde se all aktivitet som var allmän. Informanten var en aktiv användare av instagram då den ibland publicerade bilder med och då ofta taggade platsen. Personen hade ett stort socialt nätverk på instagram. Facebook användes mer passivt och inte alls i samma utsträckning som de andra två.

*Informant fyra* använde sig av alla sociala medier. Studenten ansåg Facebook vara opersonligt och föredrog därför Snapchat eller Instagram. Informanten hade bra koll på diverse funktioner i alla medier och hade bra koll på hur gps-tekniken fungerade. Denna medvetenhet uttryckte informanten genom att hen brukade ändra sin GPS-funktion, i syfte att det var underhållande. I övrigt ansåg studenten inte att platsdelning eller sitt användningssätt var en säkerhetsrisk. Däremot sa informanten att hen hade väldigt lite koll på hur mycket information applikationerna använde. Hen var medveten om att mycket data kunde användas i reklamsyfte och för applikations-ägarens egen vinning.

*Informant fem* använde alla sociala medier, men använde endast platsdelning aktivt på Snapchat. Studenten ansåg sig ha för stort kontaktnät på Facebook och att denna tillsammans med instagram användes i mer formellt syfte. Informanten såg ingen funktion i att utnyttja check-in funktion eller plats-taggar på varken Facebook eller Instagram. Hen var mycket medveten om sekretessinställningarna och uttryckte sig vara väldigt noggrann med att anpassa dessa efter applikation och kontakter.

*Informant sex* hade även denne alla sociala medier men var en mycket passiv användare. Denne publicerade mer eller mindre aldrig på medierna så alla kunde se utan bara i privata meddelanden till direkta personer. Personen använde sig inte av platsdelning i någon av medierna. Personen hade inte reflekterat så mycket över säkerhetsrisker med platsdelning men var avogt inställd till användandet av det.

## 4.2 Redogörelse av intervjuer

### 4.2.1 Informanternas syn på sociala medier och platsdelning

Majoriteten av informanterna uttryckte att de använde sociala medier i syfte att göra något annat för en kortare stund, när man inte har något annat för sig. Flera informanter var eniga i att mobilen oftast plockades upp vid mindre intressanta tillfällen; informant tre sa *"Jag använder det nog i korta stunder faktiskt, och ibland lite längre om jag är uttråkad"* och både informant fyra *"ja det är nog mest för att göra av med dötid"* och informant ett var av samma åsikt *"Mycket slösurfande"*.

I samband med användningsområden beskrev två av informanterna sin användning av medierna på följande sätt. Informant fyra använde sig av begreppen aktiv och passiv i samband med hur valde att använda platsdelning i olika medier; *" Det finns ju aktiv typ dela din plats på messenger där du aktivt går in och nu. här är jag just nu till en person. att man skickar sin platsdelning"*. Informant fem pratade pratade om det i termerna informell och formell användning; *"jag kan tänka mig att snapchat är mer informellt och då facebook och instagram är mer formell användning utav platsdelning"*.

I alla intervjuerna tog kommunikationssyfte upp som användningsområde. Både personerna som var negativt och positivt inställda till aktiverad platsdelning beskrev att de skaffat en applikation för att vänskapskretsen hade detta. Informant sex sa " *instagram skaffade jag för att mina kompisar tyckte att jag skulle skaffa det så jag skaffade det*", informant tre använder det också för att kompisarna gör det *"Man har ju så många kompisar som också använder det och det är ju därför jag använder det, för att se vad mina kompisar gör och andra som är så här bekanta "*. Informant fem sa att denne hade platsdelning igång för att hans kompisar ville det *"Jag hade inte förut men jag satte på det för mina vänner övertalade mig att det var kul. För att jag skulle kunna se vart dem va o de se vart jag va"*. Förutom detta kopplar informant tre och sex också begreppet sociala medier med skolan, något de måste gå in på för att se hålla sig uppdaterade om studierna.

För informant ett, fyra och fem var sociala medier ett sätt att hålla kontakt med vänner. På Facebook ansåg majoriteten att nätverket var som störst av de tre vi valt att undersöka i studien. Informant tre beskrev det som *”Känner kanske lite att jag borde rensa för jag känner ju inte alla 500..“*, liknande svar fann vi hos informant ett, fem och sex som menade på att Facebook är stort nätverk som man haft längre än de övriga två sociala medierna Snapchat och Instagram.

Det var olika resonemang hos informanterna om vilka man valt att dela sin platsinformation med. Informanterna nämnde att de kontrollerade sina profiler genom att ändra kontoinställningarna mellan öppet och privat samt slå på eller av aktivering av platsdelning. Informant tre var den enda som uttryckte att den hade valt att ha två konton, öppet och privat, där denne accepterade personer baserat på hur nära relation de hade. Kontroll över sina konton löste bland annat informant ett och fem som inte accepterade vem som helst, utan de närmaste vännerna. Informant ett hade utvecklat kontroll under sin tid som användare: *“ jag har ju många vem är det här på facebook men nu lägger jag inte till, nu är jag väldigt du vet så där selektiv”*. På Snapchat hade alla vi intervjuade privata inställningar men informant två började själv reflektera under intervjun vilka personer hen accepterar *“jag vet ju alla som ser mig… eller ah jag tänker nog inte alltid riktigt hur många som ser mig på snapchat för ibland lägger man ju bara till folk“*.

Alla informanter var medvetna om att sekretessinställningar för platsdelning fanns. De visste att villkor skulle godkännas för att aktivera platsdelning och att funktionen kunde stängas av. Informant fem och sex sa båda att de inte godkänner att platsdelning aktiveras direkt till skillnad från informant fyra som i samband med Snapchats Snap-karta beskrev förhållandet som *“jag tror jag bara inte stängde av den och sen ba varför stänga av den? Delar med alla jag har som vänner”*. Däremot fanns det informanter som uttryckte att de inte hade koll på att eller hur inställningar för applikationerna kunde anpassas för platsdelning. “*Det finns så många inställningar vem som kan se vad, det är vänner, vänners vänner, vem som kan se vad och så vidare.*“ - Informant tre.

Under intervjuerna tog informanterna upp check-in och taggnings funktionerna. Majoriteten av informanterna pratade om detta i syfte att visa upp att man var på restaurang eller utomlands. Informant tre och sex uttryckte följande om dessa funktioner:

> “Här är vi, inte för att skryta utan mer att nu gör vi något annat, jag tror bara att man vill visa sina kompisar att man gör något annat. Okej, ingen bryr sig, det är liksom så, jag bryr mig ju inte heller”

> “Det är ju aldrig när de bara är ute och gör något, det är så här att om någon har varit ute och ätit på en fin restaurang kommer taggen upp för att alla ska se att de har gjort det“ ….Det har blir lite så att man ska visa upp sig”

### 4.2.2 Vilka fördelar ser informanterna med platsdelning i sociala medier?

Alla informanter kunde komma på fördelar med platsdelning, trots deras inställning till att att använda det själva. Flera ansåg att man känner mer samhörighet med sitt nätverk när man visar vart man befinner sig, informant två: "*att känna samhörighet kanske om man lägger upp en bild på nått ställe"*. Fyra av informanterna nämnde att det var ett bra sätt för att kunna hitta närstående om man inte fick tag på dem. Informant tre tog upp att det blir allt vanligare bland yngre barn att använda sig av sociala medier och att det då kan vara väldigt fördelaktigt för föräldrarna att kunna lokalisera dem. Följande citat visar när två studenter pratar i positiv bemärkelse när de nämner dessa användningsområde. Informant två: *"Det kan ju vara lite lätt ibland när man inte får tag på nån och så kan man se att jaha, hon är på jobbet"*. Informant tre: "*ah kanske är framför allt den aktiva platsdelning som känns användbart. man ska t.ex. möta varandra i en stad och går från två olika håll"*.

Informant två, fem och sex nämnde alla att facebooks funktion för Katastrofsvar var en av de mest positiva funktionerna med platsdelning. Det är en trygghet att kunna se att ens vänner som befinner sig i utsatta områden är säkra. *"När det hänt någon naturkatastrof och du kan berätta för dina vänner att du är säker då är det ju bra"* sa informant fem och informant sex sa "*Jag kan säga att den här checka in vid en naturkatastrof eller skolskjutning, den kan jag tänka att den har det positiva"* som även det hyllade Katastrofsvars-funktionen.

En sak som togs upp som positivt av tre av våra informanter var möjligheten att kunna byta sin position med hjälp av gps:en utan att man faktiskt förflyttade sig. Informant fyra beskrev det som en kul grej, "*jag kan ändra min gps position. det är kul då kan man ändra tagsen. t.ex. nordkorea har en tagg. den kan jag använda"*, men påpekade även det faktum att man faktiskt inte behöver vara på den platsen man taggar sig på, *"ibland så lägger man upp en bild några dagar senare då är ju inte jag där nu. bilden behöver ju inte ens va tagen där"*. Även informant två och fem tog upp att man kan tagga sig på en annan plats och låtsas som att man befinner sig där, de sa *"på snapchat behöver du ju va där för att visas ...där. du kan ju lägga upp en bild från förra veckan och tagga vart du va då. ja man kan ju låtsas om man vill men"* och *"men så på instagram kan man ju tagga en plats där du inte är. du kan ju va i stockholm och tagga japan liksom"*.

En sak som diskuterades bland flera av informanterna som både en positiv och negativ sak var insamlandet av data från tjänsten när man använde sig av platsdelning. Informant ett förhöll sig positiv till det när man befann sig på en ny plats och ville ha information om vad som fanns i ens närhet, *"så kan det ju vara ganska enkelt att man kan söka någon speciell restaurang som finns i närheten och kan google få din location, det är ju praktiskt vid såna tillfällen"*. Även informant fyra tog upp insamling av data som en positiv sak då det kunde förbättra det sociala mediet för för en själv, till exempel att *"din reklam blir bättre, mer anpassad till dig"*. Informant fyra tog även upp att att *"om jag sitter på en resturang rätt länge antar den jag varit på den restaurangen och då vet den tillslut att jag*

*är en person som gillar att va på sån typ av restauranger"* som fördelar med att tjänsterna samlar in data när man använder sig av platstjänster. Informant fem var den enda som nämnde att insamling av data om ens platsdelning kan hjälpa myndighet att lösa brott om de misstänker att någon har haft något fuffens för sig, *"Det är väl för att catch the bad guys. Inom brott, se om nån försvunnit"*.

### 4.2.3 Vilka nackdelar ser informanterna med platsdelning i sociala medier?

Svaren bland våra informanter när det kom till negativa aspekter var mer uppdelade. Tre av informanterna nämnde att platsdelning kunde ha negativa konsekvenser i sociala sammanhang. Om man har platsdelning påslaget och inte befinner sig där man sagt till andra att man ska vara så kan det skapa osäkerhet bland ens bekanta. I vissa situationer kanske man inte vill berätta vart man är eller som informant nummer fyra sa, *"att jag t.ex. sagt till en person att jag inte kommer på dens fest och så då så ska ju den personen tror jag är där jag va"*. Även informant sex instämmer i det med kommentaren *"Det är ju alltid det här att om du skulle ljuga till nån och säga att man ligger hemma sjuk och så ser den en på Snap-kartan att man gör något annat för att man inte var modig nog att säga att man inte ville eller jag orkar inte umgås med dig idag"*. Informant ett pratade även denne om liknande saker då det kan skada relationer, *"jag har ju läst nånstans att det är jättemånga par som typ har blivit så här du vet att man måste ha på Snapchat-kartan för annars har du något fuffens för dig eller har du något att dölja, det föder mycket svartsjuka"* och att det kan göda ett osunt beteende.

Flera informanter påpekade att de tyckte att det var obehagligt att folk kunde se vart de befinner sig. Informant sex beskrev det som *"Jag tycker att det är lite creepy att folk ska veta var fan man är"*. Under samtalet började informant tre spekulera i sitt eget förhållningssätt till platsdelning då denne ansåg det obehagligt, *"att folk vet vad jag gör och var jag är och så. Så jag får lite obehagsvibbar, så egentligen borde jag kanske.."*. Informant två tyckte att det var obehagligt att folk kunde se vart denne bor, *"känner det är lite obehagligt nu att man har på sin karta. då vet ju alla vart man bor"*.

En oro som fanns bland tre av våra informanter som ändå förhöll sig positiva till platsdelning var en osäkerhet i vilka som kunde se deras aktivitet. Informant två uttryckte sin oro över att *"det är inte säkert att alla på ens snapchat är hederliga människor"*. Informant ett tog upp möjligheten till att ha en stalker och att om man då delade sin plats hela tiden så förenklar man väldigt mycket för denna, *"men skulle man ha någon sån här stalker så skulle det ju vara väldigt lätt, det är ju lätt att hitta nån såklart"*. Informant tre som tidigare tog upp att det var en positiv fördel för föräldrar att kunna ha koll på sina barn spann vidare på att det dock kunde vara ett problem om barnet inte var noga med vilka den la till på sociala medier, *"dock nackdel om eftersom det är de som styr sina egna sociala medier och de kanske inte har koll på sin egen säkerhet och så så de blir vän med folk de inte vet vem de är så kan de se vart de är"*.

Informant fyra, fem och sex tar alla upp att platsdelning kan leda till att många avslöjar mer om sitt privatliv än vad de egentligen tänkt. Informant fyra säger att *"man öppnar upp sitt privatliv mer och mer"* och informant fem tar upp att *"folk delar så korkade saker nu för tiden och delar så korkade inlägg, alltså folk som blivit av med jobbet för saker de delat på sociala medier och sånt måste man ju tänka på"*. Denne är medveten om att det är mer integritetsrelaterat men att även detta kan ses som en säkerhetsrisk om man inte kan säga med stor sannolikhet att man vet exakt vad som publiceras om en och vem som kan se det. Informant fem är medveten om att utan några privata inställningar så delar man sakerna med hela sitt nätverk, *"alla mina facebook vänner är inte mina närmaste så de är inga jag behöver dela med allihopa"* och att de flesta som delar sin plats med hela nätverket troligtvis bara gör det för att få uppmärksamhet, *"nej där tycker jag att folk som delar sin position vill mest visa för andra ja jag var nära, det är liksom nästan bekräftelse, uppmärksamhet"*.

Det som flera av informanterna såg som en kul grej med platsdelning var att man kunde modifiera den platsen man var på och att ens platsdelning inte alltid då var korrekt. Informant tre tog upp detta som en negativ aspekt, att man inte kan förlita sig på informationen man får av platsdelning; *"man förlitar sig ju inte på dem helt heller, just att man kan få en snapchat och den inte varit aktiv på flera timmar så kommer den personen fortfarande vara kvar på samma ställe"*.

En sak som delade informanterna var datainsamling till följd av platsedelning. Informant ett såg det endast som något positivt medan informant fyra kunde komma på både positiva och negativa saker med det. Informant fyra tog upp att tjänsten nog fick ut mer av insamlingen än vad denne fick, den sa att *"de får mer än jag får. även om jag får bra reklam får dem mer än jag. känns lite unfair"*. Ansåg att datainsamling av platsdelning endast var negativt, *"det ju också att de kanske inte använder det på ett etiskt sätt. Alla sociala medier jobbar ju med belöningar och så för att man ska bli beroende"*. Denne tog upp att följderna kan vara beroende och att data inte använts på ett respektabelt sätt.

### 4.2.4 Informanternas syn på säkerhetsrisker med platsdelning

Den första säkerhetsrisken som fem av informanterna nämnde var risken med att andra kunde se vart man befann sig och vilka konsekvenser det kunde få. Flera nämnde Snap-kartan och att de tyckte att det var obehagligt att man kunde se exakt vart man befann sig, den visar exakt i vilken del av byggnaden man är som informant tre sa; *"dock så vet jag att på snapchat så zoomar du in där jag är så ser du vilket hus jag är, och det är, det är så sjukt, verkligen"*. Informant två tog upp att det som var särskilt läskigt med det här var att man kunde se vart man bor; *"känner det är lite obehagligt nu att man har på sin karta, då vet ju alla vart man bor, det är ju lite läskigt"*. Informant fyra påpekade att snap-kartan nog var det största hotet och om man stänger av den så minskar risken ganska

mycket; *"hmm kanske snapmaps. typ den är så tydlig den visar hela tiden exakt vart man är. om man tar bort den minskar man mycket"*.

Flera av informanterna kände sig osäkra över vilka som kunde se ens aktivitet på de sociala medierna, vilket upplevdes vara en säkerhetsrisk. Informant fyra var medveten om att *"det är nog säkert fler som kan se mig än jag tror"* och att det sänkte nivån på hans egen säkerhet i de sociala medierna. Informant tre var inne på samma spår och pratade om att med ett väldigt stort nätverk så ökar risken då men troligtvis är vän med flera man inte känner så väl. Personen sa att denne troligtvis har vänner på sociala medier som den inte känner och att det då blir mer obehagligt att ha platsdelning igång, *"om jag hade lagt till någon som jag inte riktigt vet vem det är, vilket jag tror kan ha hänt någon gång, någon som jag egentligen inte känner hade jag inte velat ha på den eftersom man kan se exakt vart man är"*. Informant två funderade över sina egna inställningar och förhållningssätt till att lägga till nya vänner, *"nu känner jag att jag har noll kontroll och att jag behöver stänga av på snapchat eller ta bort en del. antingen ha kvar och ta bort de jag inte känner så bra längre eller stänga av den"*.

Informant fem sa tydligt att *"all sorts platsdelning blir som ett intrång på någons privatliv"* och flera av de andra informanterna var också inne på det spåret. Informant sex uttryckte det *"men integritetsperspektivet är högt, jag är mån om att dela så lite som möjligt för att det är ingens jävla bussiness om vad jag gör"*. De pratar båda om att man måste ha koll på sina sekretessinställningar som faktiskt kan öka ens internetsäkerhet väldigt mycket. De tycker att mycket av det man gör på sociala medier är väldigt privat och att fler borde tänka på vad de publicerar, *"jag tycker allmänt att platsdelning känns som ett hot. Som ett intrång på en själv"*.

Flera pratade även om att andra kan gå in och titta på vart man är och att man kanske inte alltid vill det om man reflekterar över situationen. Vänner kan få reda på saker om en som man kanske egentligen inte tänkt på om man vill dela, som informant tre sa; *"det kan ju vara så att det har hänt något personligt och de befinner sig på ett ställe där ja, där de inte borde vara. Vissa är nog inte ens medvetna om att de har det på. Typ hur vet man om man inte går in och kollar?"*. Informant ett berättade att det är så denne får reda på saker men också att den själv inte ser det som en säkerhetsrisk; *"alltså att de som alltid har uppe och plötsligt så försvinner de så tänker jag att ja, det är ju så man oftast får veta att nån kompis har gått hem med någon eller är på dejt eller så"*.

En potentiell säkerhetsrisk till följd av att man inte visste vem som kunde se och att de kan se exakt vart man befinner sig är att då förenklar man för brottslingar. Om man visar vart man befinner sig så visar man även vart man inte befinner sig och det kan vara ett lika stort problem. Informant tre nämnde att om man visar vart man är så kan ju en stalker eller liknande se vart man befinner sig och då kan de leta upp en, *"tänk om man faktiskt har en stalker, eller om det finns någon som är ett psykfall som man bara, jag vill inte ha kontakt med den här personen men man inte tänker på att man har plats påslagen och de kan se*

*vart man är, ja men ja, det är ju så lätt att den står utanför din port sen"*. Informant sex tankar gick i samm spår om att man inte kan veta helt säkert att man inte har någon kontakt som skulle kunna tänkas skada en, *"kan väl säkert tänka mig att folk har blivit mördade på det sättet. Det sägs väl att typ 99% av fallen sker av någon i dess närhet så det måste väl vara enkelt typ att kolla på Snap-kartan och se att den är där och då gå och göra det"*.

Informant två och fyra spann vidare på det att när man använder sig av platsdelning så visar man även vart man inte befinner sig och att man då kan ha lämnat ett tomt hus stående i flera dagar. Informant två pratade om just det och hur det kunde vara en säkerhetsrisk om man inte hade väldigt privata inställningar på det sociala mediet, *"om man lägger upp en bild att man är på mallorca och har öppet konto och att hela ens hus står helt tomt"*. Även informant fyra tog upp risken för inbrott men ansåg att ingen skulle göra inbrott hos denne och såg inte det som en säkerhetsrisk då, *"hmm a de kan se om man är hemma osv. tror ingen skulle göra inbrott hos mig"*.

Det fanns många spekulationer om hur insamling av data kan vara en säkerhetsrisk. En säkerhetsrisk kan bli till följd av det på grund av okunskapen som finns om vad de olika tjänsterna samlar in. Våra informanter var själva väldigt osäkra på vad de olika medierna samlade in, informant fem och sex uttryckte det *"nej ingen aning, ingen aning om vad de tar"* och *"vad som samlas in om mig tycker jag inte att jag har koll på"*. När vi frågade informant fyra vilka av medierna samlade in data svarade han *"inte snapchat men säkert facebook kan använda för att sälja vidare"* och även informant fem instämde i att snapchat kändes säkrare då man enligt denne bara delar med sitt egna nätverk, personen ifrågasatte sedan dock om i fall tjänsten också samlade in data; *"jag tänkte att jag bara delade min platsinformation med mina kompisar på snapchat [....]. Men snapchat får ju ändå min info…Men på nått sätt känns snapchat som ett mindre hot"*. Informant sex försöker ha kontroll över den datan som samlas in men förhåller sig ändå tveksam till tjänsterna; *"man orkar ju inte läsa igenom allt om vad de samlar in men jag har varit inne på allt och typ klickat bort det som går men de samlar nog fortfarande in en jävla massa data om mig"*. Både informant fem och sex ifrågasatte flertalet gånger varför tjänsterna skulle behöva samla in data om dem; *"det behöver inte de ha, vafan ska de behöva ha det för?"* och *"de behöver inte veta, jag ser ingen anledning till varför de ska veta"*.

Flera av informanterna ansåg att det inte fanns några risker med sitt användande av platsdelning eller ansåg att deras medvetenhet om riskerna är alldeles för låg. Informant fem tyckte inte att platsdelning var en stor del av sitt liv och hade därför inte reflekterat vilken negativ inverkan det kan ha på dennes säkerhet på internet; *det är inte ens stor grej i mitt liv så har inte tänkt på det så mycket"*. Informant fyra tyckte inte att denne är i riskzonen för några faror när det kommer till platsdelning så denne såg det inte som en säkerhetsrisk; *"jag ser det inte som en stor risk"*. Informant ett pratade om att det är så enkelt att hitta information om en ändå även fast man inte använder platsdelning *"idag är ju det mesta ganska öppet och man kan hitta allt med några musklick. Det är liksom så enkelt att hitta varandra så det känns inte som en säkerhetsfråga längre"*. Informanten

pratade även om hur det skiljer sig mellan olika personer, att vanliga människor som inte är berömda av någon anledning riskerar troligtvis inte lika mycket när det väljer att visa sin plats som om en kändis skulle det. Den tyckte inte att det fanns någon anledning till varför någon skulle vilja utsätta denne för en risk; *"jag har inte så mycket av värde"*.

# 5. Analys

*I detta kapitel analyseras det materialet som framkommit i Empirin med hjälp av det teoretiska ramverket från kapitel två. Analysen kommer presenteras utifrån två huvudkategorier av informationssäkerhet inom platsdelning som presenterats i den teoretiska bakgrunden. Texten delas upp utifrån olika ämnesområden informanterna har diskuterat.*

---

## 5.1 Avslöjandet av känslig information

Denna kategori är en säkerhetsrisk för användare som inte är anonyma men inte vill att all platsdelningsinformation om en ska spridas. Vi fann att applikationerna skiljde sig sinsemellan eftersom användare har olika stora nätverk på dessa. För denna säkerhetsrisk blir användarens kontaktnät och inställningar väsentligt.

***Varför använder sig personer av sociala medier med platsdelningsfunktioner?***

Informanternas svar visar på att vänskapskretsen influerar till användning av sociala medier. Flera av informanterna sa att anledningen till att de hade sociala medier var för att deras vänner hade det *"mina kompisar tyckte..."*, *"för att se vad mina kompisar gör och andra som är så här bekanta"* eller "*mina vänner övertalade mig att det var kul, för att jag skulle kunna se vart den va och de se vart jag va"*. Detta kan tyda på det Alt (2017) beskrev angående FoMO - Fear of Missing Out, det finns en rädsla för att missa något i det sociala umgänget. Citaten visar hur stor påverkan umgängeskretsen har på våra informanternas användning av en applikation. När man använder sociala medier för att andra har fått en till det så finns det troligtvis en stor risk att man inte har tänkt igenom vilka följder det har, man ser bara fördelarna och får känna att man är en del av gruppen.

***Hur ser användarnas nätverk ut?***

Under intervjuerna reflekterade många över vilka de accepterade till olika medier. Informanterna var överens om att på Facebook hade man det största nätverket och där var inte många säkra på att de verkligen visste vilka alla är, "*Känner kanske lite att jag borde rensa för jag känner ju inte alla 500..".* Tankarna om platsdelning skiljde sig beroende på vilket förhållningssätt informanten hade för vilka den var vän med på det sociala medier. Informanterna var överlag mer villiga att dela sin position på nätverk där de hade ett mindre kontaktnät eller där man kunde ställa in att bara vissa vänner kunde se den och där man samtidigt hade ett större förtroende för det sociala mediet i sig. Dessa resultat bekräftar inte tidigare forskning av Fox och Royne (2018), här visar inte användarna sig sårbara att dela personlig information till sociala medier. Svaren kan antyda att användarna är mindre sårbara med sociala medier som är mindre och har mer tillit till vilken data som samlas in. Kanske finns det ett samband mellan mediets omfång och tillit till datainsamling och upplevd säkerhetsrisk? Alla de som hade aktiverat platsdelning nämnde att de

accepterat personer de egentligen inte var villiga att dela all information med. Detta innebar personer som de inte hade daglig kontakt med skulle kunna se deras position: *"jag har ju många vem är det här"* och "*ibland lägger man bara till folk"*.

***Hur hanteras data?***

Som tidigare nämnt i avsnittet har informanterna större nätverk på Facebook samt instagram, medan de nogrannare valt ut kontakter till Snapchat. Vilket kan bero på att Facebook använts under längre tid av många. Vi kan finna skillnader i oro kring utbyte mellan dessa sociala medier. Snapchat kändes som betydligt säkrare när det kom till ägande av insamlad data, informanterna hade större tillit att utbytet av platsinformation inte kom att användas för applikations-ägarnas egen vinning: *"inte snapchat men säkert facebook kan använda för att sälja vidare"*. Att fler har tillit till utbytet av platsdelning i Snapchat kan bero på att applikationen upplevs mer intim, att informanterna anser sig ha färre kontakter som är avsedd för att skicka bilder. Facebook skiljer sig på så vis att det funnits längre och har fler funktioner för att ta kontakt med okända, genom publika sidor, inlägg eller chattfunktioner.

***Att okända kan se ens plats***

Diskussionen som kom av huruvida informanterna bara hade vänner eller flera okända i sina nätverk handlade om att flera av informanterna tyckte att det kändes obehagligt att okända då kunde se vart man befann sig. Flera av informanterna tyckte att det kändes obehagligt både att folk kunde se en *"Jag tycker att det är lite creepy att folk ska veta var fan man är"* och att det var osäkra på vilka som kunde se *"det är nog säkert fler som kan se mig än jag tror"*. Sociala medier och platsdelning framför allt leder till att *"man öppnar upp sitt privatliv mer och mer"*. Detta leder då till säkerhetsrisker som faller under integritet och konfidentialitet i C.I.A-triangeln.

Informanterna var ganska överens om att *"all sorts platsdelning blir som ett intrång på någons privatliv"* och *"jag tycker allmänt att platsdelning känns som ett hot. Som ett intrång på en själv"*. Resultaten visar på att när man känner sig osäker på vem det är som ser ens platsdelning så blir det ett hot mot ens konfidentialitet, information avslöjas som man egentligen inte vill dela. Det här problemet bottnar i att personer har människor i sitt sociala nätverk som de egentligen inte vill ha och att de inte har ändrat de sekretessinställningar som finns. Det blir även ett hot mot den personliga integriteten att människor vet saker om en som man inte vill dela. Platsinformation kanske inte upplevs som konfidentiellt när det kommer till ens närmsta vänner, vanemönster eller vart man befinner sig. Informanter som hade platsdelning aktiverat såg ingen risk med att dela detta med sitt nätverk.

Några av informanterna började spekulera om hur det kan bli när man har kontakter som man inte har så bra koll på *"det är inte säkert att alla på ens snapchat är hederliga människor"*. En annan drog det till att om man har en stalker så underlättar

platsdelningsfunktioner för den personen, stalkern kan då lokalisera platsen där man befinner sig *"men skulle man ha någon sån här stalker så skulle det ju vara väldigt lätt, det är ju lätt att hitta nån såklart"*. Det är ett säkerhetshot enligt Vicente et. al. (2011) och faller inom integritetshotet lokalisering av en person.

## 5.2 Identifiering genom platsdelning

Andra kategorin utgår från anonyma användare som utsätts för säkerhetsrisk när identiteten kan avslöjas genom information från platsdelning. Vanligast var att informanterna hade öppna konton, men vid tillfällen som kunde ge negativ påverkan på privatliv och vänskap ville användarna hålla sig anonyma. Det framkom också att vissa platser upplevs mer intima än andra, gemensamt var att hemmet ansågs känsligt och något informanterna inte ville skulle avslöjas.

***Sociala komplikationer***

När vi frågade informanterna om nackdelar med platsdelning nämnde några av dem att platsdelning kunde leda till sociala komplikationer. *"Det är ju alltid det här att om du skulle ljuga till nån och säga att man ligger hemma sjuk och så ser den en på Snap-kartan att man gör något annat[...]"* sa en av informanterna om hur det kunde bli ett problem med att man inte är där man sagt att man skulle befinna sig. Detta faller in i Vicentes et. al. (2011) första integritetshot, lokalisering av en person, att man har sagt att man ska vara på ett ställe där man inte är. detta kanske inte ses som en allvarlig säkerhetsrisk men kan ändå vara ett hot mot vänskap och ens sociala umgänge utanför tekniken. En annan informant spekulerade i hur platsdelning kunde bidra till svartsjuka och osäkerhet mellan partners om man såg att den andra befann sig på ett oväntat ställe; *"jag har ju läst nånstans att det är jättemånga par som typ har blivit så här du vet att man måste ha på Snapchat-kartan för annars har du något fuffens för dig eller har du något att dölja, det föder mycket svartsjuka"*. Även fast många kan se det här endast som sociala problem kan det falla inom konfidentialitet- och integritetsrisker inom C.I.A-triangeln.

Ett viktigt krav till följd av detta är att det sociala mediet måste upprätthålla riktighet på användarens position. Riktighet gäller för både användare som ställt in korrekt GPS-position i realtid, för användare vars platsdelning omedvetet visar felaktig plats samt för de som visar en annan position med flit. Alla dessa platsinställningar kan utgöra en säkerhetsrisk för användaren, riktigheten för applikationerna är därför låg eftersom användarna inte kan vara säkra.

***Mediet visar var du är, eller inte är***

En av följderna av att visa vart man befinner sig är att man även visar vart man inte befinner sig, något som Vicente et. al. (2011) tog upp avsaknad av person, som integritetshot. *"Om man lägger upp en bild att man är på mallorca och har öppet konto och att hela ens hus står helt tomt"* sa en av informanterna samtidigt som den reflekterade

över att inbrott skulle kunna ske på så sätt. Att om man visar att man befinner sig utomlands och utan att veta om det har ohederliga människor i sitt nätverk så kan ju de se att ens hus kommer stå tomt ett tag. Detta var en av de fysiska säkerhetsriskerna som våra informanter tog upp under intervjun som visar på att det är inte bara information om en själv som sprids, det kan även ha större följder såsom inbrott.

***Vad har tjänsten rätt till för data?***

Gemensamt för informanterna var deras osäkerhet kring vad mediet hade tillgång till för platsinformation kopplat till deras identitet. Studenternas osäkerheten grundar sig troligen i okunskap kring vad de faktiskt delar med mediernas ägare och vilken information som kan kontrolleras av en annan part (Mendel et al., 2012; Whitman & Mattord, 2016). Enligt teoretiska ramverket och C.I.A-triangeln skulle det innebära låg upplevelsen av ägande, omedvetenhet om vilken platsinformation som kan förknippas med användaridentitet för platsdelning inom de granskade sociala medierna. För att upplevelsen av säkerhet och minimera risken att dela privat information om sig själv behöver applikationerna höja medvetenhet hos användarna om utbyte och kontroll av information.

Vad som framgår av informanternas svar är att de upplevde större säkerhetsrisk med att information kunde användas i ett ekonomiskt syfte. Det var bara en informant som nämnde reklamutbyte, det var i positiv bemärkelse, att få personliga fördelar. Inom upplevelse av ägande är det svårt att se sammankoppling till kategorierna av säkerhetsrisker från Vicente et al. (2011). Informanterna tycks inte uppleva lika stor oro över att känslig information avslöjas till ägarna av applikationen, de ansåg att en större säkerhetsrisk var att oärliga kontakter i deras sociala nätverk kunde utnyttja eller få platsinformation. Det kan tyda på en större tillit till ägarna än kontaktnätet. Flera uttryckte också att dem inte hade tillräckligt viktig information eller att dem inte var en användare som besatt information av intresse för andra parter: Utdrag från intervju med informant ett, två och fem: *"det är inte ens stor grej i mitt liv", "men jag känner mig inte riktig som en sån person jag är ganska öppen.*" och*"jag har inte så mycket av värde"*.

# 6. Slutsats och reflektion

*Här kommer vi att sammanfatta det arbete som gjorts. För att besvara studiens syfte och forskningsfråga kommer vi basera slutsatser om studieresultatet på vår analys. Vidare kommer vi att diskutera vårt metodval, presentera vårt kunskapsbidrag i jämförelse med tidigare studier och ge förslag till framtida forskning.*

---

## 6.1 Slutsats

Syftet med den här studien var att undersöka vilka säkerhetsrisker det finns med platsdelning och hur medvetna användare är om dessa. Vi ville ta reda på hur medvetna personerna i målgruppen var om möjliga risker med platsdelning och hur de förhöll sig till dessa. Den frågeställningen vi ville ha svar på var:

*Vilka säkerhetsrisker är användare medvetna om när det kommer till platsdelning?*

Under intervjuerna med studiens informanter kom det fram att alla var medvetna om att det kunde finnas konsekvenser med platsdelning men flertalet såg det inte som en säkerhetsrisk. När informanterna blev tillfrågade om följderna med platsdelning så nämnde flera risken med att fel person kunde se var man befann sig. Det rörde sig både om att vänner kunde se att man befann sig på ett ställe där man inte förväntades vara, eller att det kändes obehagligt att personer de egentligen inte kände kunde se var de bodde. Flertalet pratade om att det var obehagligt men att de samtidigt hade svårt att se det som den säkerhetsrisken det faktiskt är. Ett fåtal drog kopplingen till att platsdelning kunde göra att man kunde bli förföljd eller att det kunde leda till inbrott när det syntes att personen inte var hemma. De som hade platsdelning igång tyckte att det var viktigt att den visade det man hade ställt in, vare sig om det var ens exakta position eller om man förflyttat sig till Japan med flit. De som var negativt inställda till platsdelning var inte det på grund av risken för att vänner kunde se var de befann sig, utan vilken platsdata mediet samlar in om användaren. De värderade sin integritet högt och ville inte riskera att deras personliga data användes i ett syfte de inte godkände. Det var oroliga över hur deras data användes och såg det som den största säkerhetsrisken.

Det beteende som märktes mest var att majoriteten av informanterna verkade sakna kunskap om hur platsdelning kunde bli en säkerhetsrisk. Detta beror troligtvis på anledningen till att använda sig av sociala medier kom av en gruppeffekt. Om ens närstående har det så skaffar man själv också utan att tänka på konsekvenserna. Det framkom att informanterna inte hade någon större koll på användningsavtal och sekretessinställningar om hur deras konton kunde hanteras. De som valde att inte ha platsdelning påslagen valde det då de ville dela så lite information som möjligt i alla aspekter. De som hade platsdelning aktiverat som ett mer genomtänkt beslut ansåg sig själva som inte tillräckligt betydelsefulla för att platsdelning skulle kunna bli en

säkerhetsrisk för just dem. Informanterna som hade aktiverat platsdelning men som inte tänkt igenom beslutet berättade under intervjuerna när de reflekterade över funktionen, att de ansåg det obehagligt att andra kunde se exakt var de var och att de skulle fundera över sina inställningar.

## 6.2 Metoddiskussion

Vi har i största mån försökt ha ett kritiskt förhållningssätt under vårt arbete, det var viktigt eftersom vi inte kunde generalisera resultaten för att urvalet baseras på ett bekvämlighetsurval. En begränsning för studiens resultat har varit urvalet, ett större antal intervjuer hade varit önskvärt för ökad reliabilitet. Vi ansåg ändå att intervjuerna uppmuntrade till mycket reflektion, att vårt resultat visade på en ökad medvetenhet hos många informanter och att vi har uppnått studiens syfte. Ett alternativ till en intervjustudie kunde ha varit en enkät. Då hade vi nått fler användare men troligtvis fått mindre utvecklade svar.

Eftersom vårt urval gjort på en avgränsad målgrupp kan det ha kommit att påverka studiens validitet och reliabilitet. Vi har valt en smal åldersgrupp vilket kan komma att skilja sig mycket från andra individer, vi anser att vi lyckats bidra med kunskap om användarnas medvetenhet men att reliabilitet kan ifrågasättas eftersom vi har ett smalt urval, i och med det att informantgruppen endast bestod av studenter som läser systemvetenskap vid universitetet. Förhoppningarna låg i att de skulle ha som minst en grundläggande kunskap om vad informationssäkerhet var och hur sociala medier fungerar i allmänhet. I fråga om studiens reliabilitet, att samma resultat ges vid upprepad studie tror vi kan vara lägre. Vi märkte stora skillnader mellan dessa personers åsikter trots samma utbildningsområde och nära ålder, därför skulle ett större urval och fler insamlingsmetoder vara att föredra för vidare studier för att höja reliabiliteten för att uttala sig om användares medvetenhet.

Vi har reflekterat över vår roll i samband med denna studie. För att minska risker för feltolkningar av material har vi i största mån båda varit delaktiga i exempelvis transkribering eller genomarbetat analys. Däremot har vi, författarna, båda samma utbildning, denna förkunskap hos oss som forskare kan påverka hur vi analyserar resultatet. Denna förkunskap, inom studiens ämnesområde kan också vara negativ i samband med våra semistrukturerade intervjuer. Eftersom vi utvecklade följdfrågor under intervjuernas gång kan vi ha väglett informanterna och fiskat efter svar som vi omedvetet ville komma åt. Vi är införstådda med att våra egna kunskaper och tankar om önskat resultat kan ha påverkat vår analys av informanternas svar med detta är något som alltid är svårt att undvika i forskningssammanhang, man kan inte stänga av sin föreliggande kunskap.

För framtida studier hade vi rekommenderat att intervjuerna kompletterats med fokusgrupp. Vi ansåg att många informanter behövde tid att tänka och kom på saker under tidens gång, där vår roll som intervjuperson var viktig. Det hade därför varit intressant att

minska att vår förkunskap kan komma att spela roll för deras reflektion och låta fler användare uppmuntra varandra att resonera om säkerhetsrisker.

## 6.3 Vidare forskning

Om det hade funnits möjlighet att vidareutveckla den här studien så hade det varit intressant att intervjua fler personer och kanske då ställa olika grupper mot varandra. Det hade varit intressant att undersöka olika åldersgrupper eller personer inom olika branscher och se hur deras svar hade skiljt sig mot de vi fick fram i denna studie. En annan aspekt hade varit att kolla djupare på just ett specifikt medie och hur användare förhåller sig till det då vi fick fram att de hade olika förhållningssätt till olika sociala medier.

En tanke vi hade under arbetets gång var att göra en litteraturstudie där vi kollade på hur de olika funktionerna uppmärksammades i media. Vi hittade flertalet tidningsartiklar och blogginlägg om olika funktioner på de sociala medierna som uppmärksammade riskerna med platsdelning. Det hade varit intressant att ta in detta i studien och undersöka om användare tog hänsyn till sådana artiklar som blivit virala.

Det finns även ett teori som heter TAM, Technology acceptance model, som undersöker hur användare tar emot och använder sig av ny teknik (Venkatesh & Davis 2000). Vilket förhållningssätt de har till det och varför de vill börja använda den nya tekniken. Det hade varit intressant att koppla in den teorin i analysen om vad användare ser för säkerhetsrisker med platsdelning i förhållande till vilken inställning de har till platsdelning och de sociala medierna.

# 7. Källförteckning


Alt, D. (2017) Students' social media engagement and fear of missing out (FoMO) in a diverse classroom. Journal of Computing in Higher Education, 29(2). Tillgänglig: https://search-proquest-com.ezproxy.its.uu.se/docview/1917822695?pq-origsite=summon [Hämtad 2018-12-16]

Andersson, A., Hedström, K. & Karlsson, F. (2016) *Terminologi och begrepp inom informationssäkerhet - Hur man skapar en språkgemenskap.* Myndigheten för samhällsskydd och beredskap. Karlstad. Tillgänglig: https://www.msb.se/RibData/Filer/pdf/28002.pdf?fbclid=IwAR1GSx-rjzOTTnyugmUJG2NWyWNtLnbABRAJ_KFoeVDapUVh85uOmeGLpqs [Hämtad 2018-11-27]

Bryman, A. (2012) *Social research methods*. (4. ed.) Oxford: Oxford University Press.

Bernazzani, Sophia.(2017, 28 juli). A Brief History of Snapchat [Blogginlägg]. Tillgänglig: https://blog.hubspot.com/marketing/history-of-snapchat [Hämtad 2018-01-05]

Davidsson, P & Thoresson, A. (2017) *Svenskarna och internet 2017. Undersökning om svenskarnas internetvanor*. IIS (Internetstiftelsen i Sverige). Tillgänglig: https://www.iis.se/docs/Svenskarna_och_internet_2017.pdf [Hämtad 2018-09-28]

Europol (2018) GEOSOCIAL NETWORKING – WHAT YOU NEED TO KNOW: Public awareness and prevention, European Union Agency for Law Enforcement Cooperation. Tillgänglig: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/geosocial-networking-%E2%80%93-what-you-need-to-know [Hämtad 2018-12-08]

Facebook hjälpcenter (2018a) *Facebook och plats*. Tillgänglig: https://www.facebook.com/help/337244676357509?helpref=faq_content [Hämtad 2018-12-04]

Facebook hjälpcenter (2018b) *Hur använder jag Vänner i närheten?* Tillgänglig: https://www.facebook.com/help/iphone-app/291236034364603 [Tillgänglig 2018-12-04]

Facebook hjälpcenter (2018c) *Katastrofsvar*. Tillgänglig: https://www.facebook.com/help/141874516227713/?helpref=hc_fnav [Hämtad 2018-12-04]

Falch M., Tadayoni R., Henten A., & Windekilde I. (2009) *Business Models in Social Networking*. Aalborg University Copenhagen, Center for Communication, Media and Information Technologies. Tillgänglig: https://www.researchgate.net/publication/242178725_Business_Models_in_Social_Networking [Hämtad 2018-12-10]

Fox, A. K., & Royne, M. B. (2018) Private information in a social world: Assessing consumers' fear and understanding of social media privacy. Journal of Marketing Theory and Practice, 26(1-2), 72-89. doi:10.1080/10696679.2017.1389242 Tillgänglig:

https://web-a-ebscohost-com.ezproxy.its.uu.se/ehost/pdfviewer/pdfviewer?vid=1&sid=ac4b511f-37c5-4d29-82f9-a7775215b8b3%40sessionmgr4008 [Hämtad 2018-12-16]

Furini, M. & Tamanini, V. (2014). *Location privacy and public metadata in social media platforms: attitudes, behaviors and opinions.* Multimedia tools and applications, vol. 74, ss 9795-9825.

Gan, D., & Jenkins, L. (2015) *Social Networking Privacy-Who's Stalking You?* Future Internet, 03/2015, Volym 7, Nummer 4. First presented at CFET 2014—7th International Conference on Cybercrime, Forensics, Education and Training, Christ Church Canterbury, UK, 10–11 July. Tillgänglig: https://www.mdpi.com/1999-5903/7/1/67 [Hämtad 2018-11-21]

Hallikainen, P. (2015) *Why People Use Social Media Platforms: Exploring the Motivations and Consequences of Use.* , From Information to Smart Society, Switzerland. Tillgänglig: https://link.springer.com/chapter/10.1007/978-3-319-09450-2_2 [Hämtad 2018-11-21]

Haynes, D., & Robinson, L. (2015) *Defining user risk in social networking services*. Aslib Journal of Information Management, Vol. 67 Issue: 1, pp.94-115. Tillgänglig: https://doi-org.ezproxy.its.uu.se/10.1108/AJIM-07-2014-0087 [Hämtad 2018-12-22]

He, W. (2013) *A survey of security risks of mobile social media through blog mining and an extensive literature search.* Information Management & Computer Security, Vol. 21 Issue: 5, pp.381-400. Tillgänglig: https://doi-org.ezproxy.its.uu.se/10.1108/IMCS-12-2012-0068 [Hämtad 2018-12-22]

Hill, K. (2015) *Michelle Obama, Reese Witherspoon and other celebs are leaking location information on Instagram,* Splinternews.com. Tillgänglig: https://splinternews.com/michelle-obama-reese-witherspoon-and-other-celebs-are-1793845668 [Hämtad 2018-12-04]

Hinchliffe E. (2016) *Instagram is killing photo maps*, Mashable.com. Tillgänglig: https://mashable.com/2016/09/06/instagram-kills-photo-maps/?europe=true#wVduE5MWMSq6 [Hämtad 2018-11-28]

Hjerm, M., Lindgren, S., & Nilsson, M., (2014) Introduktion till samhällsvetenskaplig analys (2., [utök. och uppdaterade] uppl. ed.). Malmö: Gleerup.

Instagram Support (2018) *Instagram, Hashtag and Location Stories on Explore*. Tillgänglig: https://help.instagram.com/392382044488940 [Hämtad 2018-11-28]

Internetstiftelsen i Sverige (2017), *Svenskarna och internet 2017 - En årlig studie av svenska folkets internetvanor*. Tillgänglig: https://2017.svenskarnaochinternet.se/sammanfattning/ [Hämtad 2018-12-22]

Informationssäkerhet.se (2015) *Om informationssäkerhet.* Myndigheten för samhällsskydd och beredskap. https://www.informationssakerhet.se/Om-informationssakerhet-kon/vad_ar_informationssakerhet/ [Hämtad 2018-11-26]

Ionescu, D. (2010) *Geolocation 101: How It Works, the Apps, and Your Privacy*. PCWorld From IDG. Tillgänglig: https://www.pcworld.com/article/192803/geolo.html [Hämtad 2018-11-27]

Karlsson M. (2017) *Facebook Messenger får live-platsdelning*, Omni. Tillgänglig: https://omni.se/facebook-messenger-far-live-platsdelning/a/OK5ek [Hämtad 2018-12-04]

Karlsson M. (2016) *Facebooks "Vänner i närheten" får högre integritet.* SvD Näringsliv. Tillgänglig: https://www.svd.se/facebooks-vanner-i-narhetenfar-hogre-integritet [Hämtad 2018-12-04]

McNeff, J G., (2002) *The Global Positioning System*, IEEE Transactions on Microwave Theory and Techniques, Vol. 50, No. 3. Tillgänlig: https://ieeexplore-ieee-org.ezproxy.its.uu.se/stamp/stamp.jsp?tp=&arnumber=989949 [Hämtad 2018-12-08]

Mendel, T., Puddephatt, A., Wagner, B., Hawtin, D. & Torres, N. (2012), *Global Survey on Internet Privacy and Freedom of Expression.* Unesco Series on Internet Freedom, UNESCO Publishing, Paris. Tillgänglig: http://unesdoc.unesco.org/images/0021/002182/218273e.pdf [Hämtad 2018-11-27]

Nationalencyklopedin (2018a) Sökord: *Förhållningssätt*. Tillgänglig: https://www-ne-se.ezproxy.its.uu.se/uppslagsverk/ordbok/svensk/förhållningssätt [Hämtad 2018-12-12]

Nationalencyklopedin (2018b) Sökord: *Medveten*. Tillgänglig: https://www-ne-se.ezproxy.its.uu.se/uppslagsverk/ordbok/svensk/medvetenhet [Hämtad 2018-12-12]

Oates, B. J. (2006) *Researching information systems and computing.* London: SAGE Publications. Tillgänglig: https://web-b-ebscohost-com.ezproxy.its.uu.se/ehost/ebookviewer/ebook/bmxlYmtfXzEwOTk0MzFfX0FO0?sid=3f6325cf-4395-4b71-a2b5-efd13b413077@sessionmgr103&vid=0&format=EB&rid=1 [Hämtad 2018-09-27]

Pötzsch, S. (2009) *Privacy Awareness: A Means to Solve the Privacy Paradox?*. IFIP Advances in Information and Communication Technology, vol 298. Springer, Berlin, Heidelberg. Tillgänglig: https://link.springer.com/chapter/10.1007/978-3-642-03315-5_17 [Hämtad 2018-12-11]

Snapchat Support (2018a) *Om Snap-kartan.* Tillgänglig: https://support.snapchat.com/sv-SE/a/snap-map-about [Hämtad 2018-11-28]

Snapchat Support (2018b) *Vanliga frågor om Snap-kartan*. Tillgänglig: https://support.snapchat.com/sv-SE/article/snap-map-faq [Hämtad 2018-11-28]

Svenskarna och Internet 2017 (2017) *Kommunikation och sociala plattformar. Tillgänglig:* https://2017.svenskarnaochinternet.se/kommunikation-och-sociala-plattformar/anvandning-av-sociala-plattformar/ [Hämtad 2018-12-04]

Topping, A. (2012) *Social networking sites fuelling stalking, report warns*. The Guardian. 1 februari. Tillgänglig: https://www.theguardian.com/technology/2012/feb/01/social-media-smartphones-stalking [Hämtad 2018-11-21]

Venkatesh, V. & Davis, F. D. (2000), *"A theoretical extension of the technology acceptance model: Four longitudinal field studies"*, Management Science, 46 (2): 186–204

Vetenskapsrådet. (2017). *God forskningssed.* (2. rev. uppl.). Tillgänglig: https://www.vr.se/download/18.2412c5311624176023d25b05/1529480532631/God-forskningssed_VR_2017.pdf [Hämtad 2018-12-13]

Vicente, C R., Freni, D., Bettini, C., & Jensen C S. (2011) *Location-Related Privacy in Geo-Social Networks.* IEEE Internet Computing, Vol. 15, Issue. 3. Tillgänglig: https://ieeexplore-ieee-org.ezproxy.its.uu.se/stamp/stamp.jsp?tp=&arnumber=5719583 [Hämtad 2018-11-27]

Whitman, M.E. & Mattord, H.J. (red.) (2016[2012]) Principles of information security. (Fifth edition.) Boston, MA: Cengage Learning.

# 8. Bilagor

## Bilaga 1 Intervjumall

Numrerade frågor med siffror: huvudfrågor
Numrerade frågor med bokstäver: eventuella följdfrågor

**Bakgrundsinfo**

1. Ålder
2. Kön
3. Har du en smartphone?
4. Hur ofta använder du dig av sociala medier på mobilen per dag?
5. Har du/ Använder du
    a. facebook
    b. snapchat
    c. instagram

**Allmänt**

1. Varför använder du dig av sociala medier, i vilket syfte?

2. Använder du dig av platsdelning?
3. Om ja, varför använder du dig av platsdelning i sociala medier, i vilket syfte?
        a) Vad använder du för typ av platsdelning, i:
            i) facebook
            ii) snapchat
            iii) instagram

    Om nej, varför använder du dig inte av platsdelning i sociala medier, i vilket syfte?
        a) Har du använt dig av det förut?
        b) Har du aktivt stängt av platsdelning?
            i) I sådant fall, hur?

4. Vad har du för kunskap om hur platsdelning fungerar på olika sociala medier?
        a) Hur skaffade du dig den kunskapen?

5. Hur ser du på att använda platsdelning i sociala medier, används de på olika sätt i olika medier?
    a. Använder du dem olika i olika situationer?
    b. Tillsammans med olika personer?

.

Hur ser du på att använda platsdelning i sociala medier, används de på olika sätt i olika medier?
    a. Hur är din uppfattning om hur andra använder dem?
    b. Varför tror du att de använder dem?

6. Finns det sammanhang du stänger av platsdelning?
    a. I sådant fall, varför och vilka?

7. Känner du att du har kontroll över den informationen som som du delar med dig av?

**Säkerhetsrisker**

1. Om man ser till platsdelning inom ett säkerhetsperspektiv:,
    a. i vilka sammanhang är det positivt, ser du fördelar?
        i. har du/eller någon du känner varit med om en situation?

    b. i vilka sammanhang är det negativt, ser du nackdelar?
        i. har du/eller någon du känner varit med om en situation?

2. På vilket sätt tror du att din användning av/kontroll över platsdelning är en säkerhetsrisk för dig?
    a. Vilka risker tror du att det finns?

3. Reflekterar du över hur andra använder sig utav platsdelning i sociala medier?
    a. Om ja, vad reflekterar du över?
    b. Känner du att det utgör en säkerhetsrisk för dig när andra använder platsedelning i sammanhang där du är med?

4. Vad skulle få dig att reflektera mer över ditt beteende i sociala medier för att minska säkerhetsrisker genom ditt användande?

5. Har din syn på säkerhetsrisker förändrats efter denna intervju eller är den detsamma som innan?
    a) På vilket sätt?
    b) Tänker du göra några förändringar kring ditt användande?
        i) vilka?