

Metadata och dess inverkan på vår digitala integritet

En kvalitativ studie om metadata, kunskap och digitala fotspår

Av: Signe Svangren och Jenny Nilsson

Handledare: Kai-Mikael Jää-Aro

Södertörns högskola | Institutionen för naturvetenskap, miljö och teknik

Kandidatuppsats 15 hp

Medieteknik C | Höstterminen 2018

Programmet för IT, medier och design



Abstract	3
Keywords	3
Sammanfattning	4
Nyckelord	4
1. Inledning	5
1.1 Syfte och frågeställning	7
2. Bakgrund	8
3. Metod	10
3.1 Metodbeskrivning	11
3.2 Genomförande	11
3.2.1 Datainsamling	11
3.2.2 Informanter	13
3.2.3 Analysmetod	13
4. Teori	14
4.1 Avdesigning	14
4.2 Utilitarismen	16
4.3 Privatliv	18
5. Resultat och analys	21
5.1 Kunskap	21
5.2 Försiktighet	22
5.3 Tillit	24
5.4 Paradoxalt beteende	25
5.5 Positivitet	26
5.6 Okunskap	28
5.7 Behov	29
5.8 Säljande	29
5.9 Misstänksamhet	30
5.10 Avdesigning	31
5.11 Utilitarismen	34
5.12 Privatliv	36
7. Diskussion	39
7.1 Hur är användares attityd till metadata i relation till deras kunskap?	39

7.2 Hur påverkar kunskaperna och attityden värderingen av digital integritet?	41
7.3 Slutsats av diskussion	45
7.4 Vidare forskning	46
8. Slutsats	46
9. Referenser	47
10. Bilagor	49
10.1 Intervjufrågor	49
10.2 Samtyckesblankett	51

Abstract

The paper describes a qualitative study of users' attitudes to metadata in relation to their knowledge and how it affects their valuation of digital integrity. Method for data collection is semi-structured interviews and a critical event. The informants were two people who work with IT and two who do not. The theories of undesign, utilitarianism and privacy were chosen to discuss in relation to the result. A thematic analysis method is used to find relationships between attitudes and other interesting themes in the result. These themes, which we have named after the main attitudes of the informants, includes inter alia knowledge, trust, suspicion and positivity. In the discussion chapter, the results are linked with the analysis and answer the research question. The conclusion is that there is no clear correlation between the informants' knowledge and their attitude, knowledge of metadata has little significance for the attitude and the knowledge and attitudes have little effect on the evaluation of integrity among our four informants.

Keywords

Metadata, integrity, GDPR, Digital footprints, Knowledge, Attitude, Digital integrity, Privacy

Sammanfattning

Uppsatsen behandlar en kvalitativ studie av användares attityder till metadata i relation till deras kunskap samt hur det påverkar deras värdering av digital integritet. Metod för datainsamling är semistrukturerade intervjuer samt en kritisk händelse. Informanterna var två personer som är yrkesverksamma inom IT och två som inte är det. Teorierna avdesign, utilitarism samt privatliv valdes ut att diskuteras i relation till resultatet. En tematisk analysmetod används för att hitta samband mellan attityder och andra intressanta teman i resultatet. Dessa teman, som är döpta efter de huvudsakliga attityderna informanterna uppvisat, var bland annat kunskap, tillit, misstänksamhet och positivitet. I diskussionskapitlet sammankopplas resultatet med analysen och besvarar forskningsfrågan. Slutsatsen av denna studie är att vi inte funnit något samband mellan de fyra informanternas kunskap och deras attityd, kunskap om metadata har liten betydelse för attityden och att kunskaperna och attityderna i liten del påverkar värderingen av integritet.

Nyckelord

Metadata, Integritet, GDPR, Digitala fotspår, Kunskap, Attityd, Digital integritet, Privatliv

1. Inledning

Metadata är data om data och är strukturerad information som förklarar, beskriver och lokaliserar åtkomst och användning av dokument och resurser. Metadata används i olika sammanhang och baserat på sammanhang delas de in i olika kategorier: beskrivande, administrativa, strukturella och användargenererade. Beskrivande är den data som kan definiera, hitta och förstå en handling eller ett dokument. Administrativ data hanterar information om dokumentets skapandeprocess samt användningsområden för resursen. Strukturella metadata kartlägger olika resursers relation till varandra samt hur de tillsammans skapar ett digitalt dokument. Användargenererad metadata är den data som kan kopplas till en individ och ofta innehåller personlig information såsom internetsökningar och egna anteckningar (Björkhem 2017). Denna uppsats kommer att fokusera på användargenererad metadata och dess direkta samt indirekta inverkan på användarna. Den användargenererade datan skapas alltså av användarnas interaktion med artefakten och ligger till grund för de digitala fotspår som efterlämnas. Hur den insamlade metadata sedan används beror på vilken tjänst som används, det kan exempelvis resultera i riktad reklam eller direkt riktade politiska budskap. Användargenererad datainsamling beror på om den använda tjänsten är finansierad via exempelvis abonnemang (Netflix), via reklam (Facebook), finansieras av en affärstransaktion (Uber), alternativt via donationer (Wikipedia) (Haider och Sundin 2018).

År 2013 avslöjade Edward Snowden den omfattande insamlingen av privatpersoners data som NSA (National Security Agency) förde i USA. Snowden bevisade att det på 30 dagar samlades in information om ungefär 97 miljarder mail och 124 miljarder telefonsamtal, tillsammans med information om sms, kontoutdrag och Google-sökningar gjorda världen över medan detta förnekades av de ansvariga. Enligt NSA samlades denna data in med syftet att öka säkerheten för medborgarna då det förmodades att terrorism och liknande kunde hittas tidigare vid bättre övervakning (Sundström 2015). NSA ansåg inte att insamlingen var problematisk eftersom den endast samlade in metadata. Jeffrey Pomerantz beskriver metadata som en karta, där

komplexiteten i kartan utvecklas ju mer data du besitter. Därför är uttrycket *bara metadata* missvisande eftersom omfånget på NSA:s insamlade resurser är så omfattande att komplexiteten och förståelsen för användarna är stor (Pomerantz 2015, 00.01.57). Trots förhoppningen att minska brottsligheten med insamlingen har metadata hittills aldrig stoppat en kriminell handling. Detta beror enligt Snowden på att den enorma mängd data som samlas in omöjligt kan förstås och analyseras. Enligt NSA var insamlandet oproblematiskt eftersom metadata endast innehåller information om datan - exempelvis telefonnummer, längd på samtal samt GPS-koordinater till var ett samtal har gjorts, utan att samla information om vad som sades i samtalet (Sundström 2015). Liknande avlyssning genomförs även i Sverige sedan FRA-lagen trädde i kraft år 2009. Denna lag tillåter Försvarets Radioanstalt att lyssna på samtlig kabeltrafik för att kunna kartlägga hotbilder som terrorism och kriminalitet (Hernadi 2008).

År 2017 uttryckte Jarboh ett vidare intresse att undersöka attityder kring digitala fotspår efter att GDPR-lagen trätt i kraft (Jarboh 2017, 34). Med hänvisning till detta ansåg vi att fortsatt forskning kring attityderna borde genomföras. Då GDPR syftar till att verka integritetsstärkande (Datainspektionen 2018) fanns intresse att forska i huruvida användarna ansåg att känslan av integritet ökat med den nya reformen. Till följd av ökad digital användning är samhället ständigt uppkopplat. Den ökade uppkopplingen möjliggör en utveckling för både konsumenter, företag och samhällsstrukturen samtidigt som det ställer högre krav på samhällets anpassning samt stöd av den personliga integriteten. Ett exempel är ökad användning av sociala medier, där uppladdade bilder automatiskt får metadata i form av exempelvis GPS-koordinater, klockslag och söksträngar. Metadata indexeras sedan för att underlätta strukturering av sökresultat när metadata används av sökmotorer som exempelvis Google eller Yahoo (Pixell 2018). Den implementerade metadata tillhör då respektive sökmotor och kan anonymiseras vid behov, vilket leder till att en anonymt postad bild ändå kan informera om var och när den är tagen, något som kan anses icke-anonymt. I Googles integritetspolicy från år 2000 står det att kakor kan komma att sparas för användarinställningar vilka sedan kan analyseras för att avläsa användarens användarbeteende. Detta är en typ av anonymisering eftersom kakorna kan koppla samman samtliga Google-sökningar som gjorts med samma dator och på så sätt läsa av användares

beteendemönster (Hoback 2013, 00:10:48). 2001 hade denna integritetspolicy uppdaterats till att informera användare om att kakor samlas in för att förstå användares sökmönster. Fortsatt stod det att dessa kakor inte kommer att delas med en tredje part så länge datan inte riskerar att tillhöra ett brottsmål och därför kan vara av intresse för myndigheter. Utvecklingen mellan dessa två år betyder att integriteten har minskat och att kategoriseringen av specifika användare har ökat (Hoback 2013, 00:10:58). En paradox gällande integritet diskuterar Norberg, Horne och Horne då konsumenterna ofta uttrycker sitt motstånd till att företag samlar privata data och baserar sin försäljningsstrategi på detta. Samtidigt visar studier att konsumenterna idag i allt större utsträckning frivilligt väljer att dela sin privata information, detta benämns i artikeln som en integritetsparadox där akt och handling skiljer sig åt (Norberg, Horne och Horne 2007, 100).

Vi anser att den ökade aktualiteten av ämnet bidrar till att göra det intressant för efterforskning. Samhällets digitalisering leder till ökad mängd metadata vilket resulterar i högre krav på sekretessen i samhället och är därför ett fenomen som vi vill efterforska.

1.1 Syfte och frågeställning

Syftet med denna uppsats är att uppnå teoretisk generalisering av relationen mellan kunskap och attityd hos användare kring insamling av metadata i användning av digitala artefakter, samt hur detta påverkar deras värdering av digital integritet. Uppsatsen ska också skapa förståelse för ämnet metadata och digitala fotspår samt vad den konkret betyder för informanterna. Eftersom större studier har gjorts av liknande ämnen, vilka redogörs för i avsnitt 2. *Bakgrund*, ämnar vi att bidra med en del till ett större forskningsområde.

För att uppnå studiens syfte har följande frågeställningar använts,

- *Hur är användares attityd till metadata i relation till deras kunskap?*
- *Hur påverkar kunskaperna och attityden värderingen av digital integritet?*

Vad som menas med värdering av integritet beskrivs vidare under avsnittet 4.3. *Privatliv*.

2. Bakgrund

Det finns ett antal tidigare studier som berör ämnet metadata samt digitala fotspår och dess integritetspåverkan. Dessa studier redogör vi för nedan, vilka sedan ligger till grund för analys och diskussion.

En studie innehållande analys av användares åsikter är studien som nämnts ovan av Norberg, Horne och Horne (2007). Där diskuteras integritetsparadoxen som uppstår då användarna noteras misstycka till hur företagen samlar privata data i kommersiella syften, samtidigt som inget antyder att kunderna försöker undvika att efterlämna denna typ av data. En användarpolicy ska finnas för att skydda användarna och markera hur den insamlade datan kommer att användas, studien visar dock hur användarna sällan tar del av informationen och accepterar villkoren ändå. En komplikation uppstår då eftersom något som skapas för användarna bevisligen inte nyttjas och användarvillkoren då endast tillåter företagen att ha ryggen fri. Den uttryckta önskan om bredare grad av integritet är inget som användarna själva försöker skapa (Norberg, Horne och Horne 2007, 120). Likväl kan läsbarheten av användarvillkoren diskuteras. För bästa läsbarhet bör texten vara skriven i gemener - medan den istället oftast är skriven i versaler och i en hög typsnittstyngd vilken noteras minska läsbarheten. Cirka 61% av konsumenterna säger sig i en undersökning gjord 2012 inte läsa användarpolicyn innan de godkänner dessa. Detta kan leda till en problematik gällande icke-läst information angående exempelvis avgifter och detta uppskattas kosta ett genomsnittligt amerikanskt hushåll ungefär 20.000 kronor om året (Sullivan 2012).

Tidigare studier visar även att metadata finns tillhörande det mesta, trots att data kan krypteras. Det finns svårigheter att dölja samtlig information om exempelvis privat kommunikation som sker online eftersom metadata om vem som pratat, när och hur nästan alltid medföljer ändå (Tyagi et al. 2017, 423). Intresset för att samla denna metadata kan antingen vara statlig, vilket betyder att staten vill samla denna data för att kunna kategorisera innehållet i samtalen och då kunna avläsa om något kriminellt planeras och möjliggöra ett gripande av personen innan den kriminella akten utförts (Cole 2014, 2). Intresset kan också vara kommersiellt vilket innebär att

företag samlar personliga data för att sedan kunna rikta direktreklam eller politisk propaganda till användaren (Haider och Sundin 2018). Tidigare studier framhåller både positiva och negativa aspekter av användandet av metadata. Dock är det främst negativa perspektiv som lyfts fram och då generellt rörande inskränkning av integriteten. Både David Cole (2014) och Nirvan Tyagi et al. (2017) lyfter fram att samtliga metadata kan hävdas vara integritetskränkande, dels eftersom, som ovan nämnt, dessa typer av data kan samlas trots att användaren tror sig vara anonym (Tyagi et al. 2017, 423). Men även eftersom en tillräckligt stor mängd metadata kan kartlägga en persons liv utan att egentligen presentera innehållet i konversationen (Cole 2014, 1).

Tidigare studier har även genomförts på användares attityder till olika aspekter av digital användning och privatliv. Exempel på detta är en studie av användares attityder till privatliv angående närhetssensorer i smarta telefoner (Jonsson och Olsson 2018, 1). Forskarna såg en ökad medvetenhet och omsorg för aspekter som berör privatlivet hos användarna jämfört med sina tidigare studier. De konstaterade även att användarna väljer att lita på olika företags tjänster beroende på vilka tillstånd de kräver av användarna, snarare än att läsa användarvillkoren. Detta samtidigt som respondenterna i studien läser användarvillkoren i större utsträckning än i forskarnas tidigare studier. Studien resulterade också i en insikt att användarna är villiga att dela data om plats, närhet och identitet så länge de kan kontrollera vem som har åtkomst till datan. Sist menar forskarna att användarna inte värderar någon viss typ av data som känsligare än någon annan. Vid en läcka av privata data är det bristen på kontroll över informationen som användarna fruktar, inte informationen i sig (Jonsson och Olsson 2018, 5).

Ett annat exempel är studien av användares attityder till insamling av webbläsardata (Chow et al. 2017). Forskarna studerade vilken typ av data insamlat från webbläsare användarna anser som känsligast (Chow et al. 2017, 1817). Deltagarna i studien fick ange vilken grad av känslighet typerna hade, typer som domäner, fullständiga URL:er, kategorier av webbplatser och beteendeprofiler. Resultatet var att användarna bedömer URL:er som känsligast, framför kategorisering av vilka webbplatser användaren besöker (Chow et al. 2017, 1821). De kategorier

av webbplatser användarna ser som känslig information var generellt medicin, finans, sociala medier och avsett för vuxna (Chow et al. 2017, 1820).

Ytterligare exempel är en undersökning av vilka faktorer som påverkar användares acceptans för mobil massavläsning, vilket innebär en kollektiv sammanlänkning mellan mobila digitala enheter i närområdet via sensorer. Detta görs av olika syften, exempelvis att kartlägga trafik i städer. Forskarna har utrett användarnas inställning till anonymitet gällande mobil massavläsning (Dey et al. 2016, 65). Resultatet var att användarna inte litar på platsanonymisering vid mobil massavläsning. Även om användare kan anonymiseras från platsen upplever de ändå en kompromiss av sitt privatliv (Dey et al. 2016, 80). Användarna litar mer på att anonymisera en aktivitet än platsen. Vidare litar de mer på att förbli anonyma under ljudupptagning än via platsen, liksom via video och bild. Forskarnas hypotes baserat på resultaten är att användarna saknar både kunskap och tillit till verktyg för anonymisering av data vid mobil massavlyssning (Dey et al. 2016, 81).

3. Metod

Här följer en beskrivning av de metoder som använts i uppsatsen, analysmetoden redogörs även för att tydliggöra den kommande analysen. Därefter följer en redogörelse för genomförandet av metoderna. Metodernas tillförlitlighet problematiseras nedan för att redovisa överväganden som gjorts under projektet. Då studien är kvalitativ ska den inte generalisera en hel population utan skapa förståelse för två grupper av populationen användare av digitala artefakter:

yrkesverksamma inom IT och icke yrkesverksamma inom IT. Specifikt hur urvalet gjorts anges i avsnitt 3.2.2 *Informanter*. Resultatet syftar till att kunna användas som en modell som kan appliceras på liknande fall ur samma grupper (Alvehus 2013, 127–128). Av denna anledning valdes nedan följande metoder ut.

3.1 Metodbeskrivning

Urvalet är strategiskt med syftet att jämföra attityder och värdering av integritet hos människor med olika kunskap om ämnet (Alvehus 2013, 82). Metod för datainsamling är semistrukturerade intervjuer (Alvehus 2013, 82) samt studie av kritisk händelse (Bell 2005, 179) som används för att undersöka deltagarnas egna uppfattning om de händelser i vardagen som samlar in metadata. Den ursprungliga definitionen av kritisk händelse är en uppgift som avgör skillnaden mellan framgång och misslyckande (Bell 2005, 179). Semistrukturerad intervju bedöms relevant eftersom den tillåter utrymme för informanternas spontana reaktioner (Alvehus 2013, 82) vilket kan vara fördelaktigt vid undersökning av attityder. Intervju som metod valdes för att ge informanten möjlighet att uttrycka känslor och gå djupare in i resonemang, vilket är svårt vid exempelvis en enkätundersökning (Bell 2005, 157). Efter intervjuerna antecknades och analyserades intressant information (Alvehus 2013, 85). En tematisk analysmetod i sex steg används för att strukturera datan. Metoden görs genom att datan genomgås systematiskt för att hitta eventuella samband och teman. Den intressanta informationen som hittades i intervjuerna antecknades i form av nyckelord. Datan bearbetades ett flertal gånger för att identifiera alla tänkbara teman och namnge dem (Braun och Clarke 2006, 16).

3.2 Genomförande

3.2.1 Datainsamling

Metoden kritisk händelse i form av dagboksanteckning valdes ut som en effektiv samt koncentrerad insamling där vi låtit informanten anteckna detaljerna av en utvald kritisk händelse där metadata samlas in (Bell 2005, 179). Den utvalda kritiska händelsen var; när informanterna använder en reseplaneringsapplikation för att söka en resa med kollektivtrafik. Händelsen valdes ut då den klassades som en allmängiltig situation som sannolikt alla fyra informanter befinner sig i under vardagen. Händelsen kan även klassas som avgörande för framgång eller misslyckande med att hitta den snabbaste resan med kollektivtrafik från en punkt till en annan. Informanterna antecknar alla digitala spår de tror att reseapplikationen sparar från sökningen. Detta användes

sedan som underlag till intervjuerna för att undersöka till vilken grad informanterna är medvetna om vad som sker, och jämföra med hur de agerar utifrån den kunskapen. Under intervjun ombads informanterna utveckla sina anteckningar och förklara varför de tror som de tror.

Intervjuerna utformades för att kartlägga användarnas vardagliga bruk av digitala artefakter som sparar metadata och jämföra det med användares egna uppfattning om när det sker. De ämnar även undersöka hur användarnas attityd till metadata är och hur detta relaterar till deras värdering av integritet. Informanterna meddelades i förväg vad syftet med intervjun var, hur den skulle genomföras och hur informationen skulle komma att användas (Bell 2005, 156). Likaså tillfrågades informanterna om de godkände att intervjun spelades in och informerades om vilka som ges tillgång till inspelningen (Bell 2005, 164). Dessutom garanterades informanterna konfidentialitet för deras egen trygghet vilket definierades i texten (Bell 2005, 48).

Samtyckesblanketter utformades gällande hantering av informanternas personliga information för att följa GDPR (Datainspektionen 2018). Pilotstudier utfördes för att säkerställa att frågorna var relevanta och rätt formulerade (Bell 2005, 158).

Inspelning av intervjun valdes för att minimera risken för feltolkning av det informanterna sade. Risken finns alltid vid inspelning att informanten påverkas negativt och agerar på ett onaturligt sätt (Alvehus 2013, 85). Risken vägdes mot de fördelar som fanns, vilka vägde mer. Det strategiska urvalet problematiserades och bedömdes relevant med tanke på forskningsfrågans karaktär, och eftersom studien är kvalitativ krävs inte ett representativt urval (Alvehus 2013, 127). Reliabilitet och validitet har i viss mån tagits hänsyn till, emellertid prioriteras dessa faktorer högre vid en kvantitativ studie (Alvehus 2013, 122). För att säkerställa god kvalitet i denna studie har tre specifika begrepp används som måttstockar, vilka Alvehus (2013, 123) förespråkar som relevanta i kvalitativ forskning. Hantverkskvalitet eftersträvas genom en systematisk datainsamling, analys och diskussion. Kommunikativ validitet uppnås genom dialog med dels informanterna - varav några är yrkesverksamma inom det utforskade området - och dels en handledare som representant av forskningssamhället. Pragmatisk validitet ämnar att uppnås i den utsträckning som är möjlig för en kvalitativ studie på denna forskningsnivå. Att påverka

samhället ses som ett realistiskt mål i detta fall, emellertid finns förhoppningar att studien kan komma till nytta för någon i samhället (Alvehus 2013, 123–124).

3.2.2 Informanter

Det strategiska urvalet gjordes genom att kontakta olika informanter via LinkedIn som enligt sina egna profilinställningar är yrkesverksamma inom metadata. För informanterna som icke är yrkesverksamma inom IT genomfördes ett slumpmässigt urval (Alvehus 2013, 66) efter att vi säkerställt att de har andra yrken.

Studien bestod av fyra deltagare, två personer som arbetar med IT och två som inte gör det. Deltagarna benämns i studien som informant 1, informant 2, informant 3 och informant 4. Detta för att uppfylla löftet om konfidentialitet som givits (Bell 2005, 48). Vi har valt att fokusera på den privata användningen av artefakter, framför den professionella för att möjliggöra en likvärdig analys mellan de två personkategorierna. Vi anser att skevhet kan uppstå om privat användning jämförs med arbetsrelaterad användning eftersom denna förmodas skilja sig något åt.

Informant 1 är en 32-årig kvinna som är egenföretagare. Informant 2 är en 32-årig man som arbetar som kock. Informant 3 är en 30-årig man som jobbar som IT-säkerhetskonsult. Informant 4 är en 30-årig man som jobbar som metadataspecialist inom Video OnDemand. Åldersspannet mellan informanterna kan anses som snävt, emellertid finns fördelen att alla fyra informanter ingår i samma generation och kan jämföras som likvärdiga ur det perspektivet. Med en homogen grupp som denna kan direkta jämförelser göras. Kön fördelningen hade önskvärt varit jämnare för att ur denna aspekt generera en heterogen grupp (Alvehus 2013, 69). Likaså hade studien fördelaktigt bestått av fler informanter för ökad representation, men inom tidsramen för projektet fanns endast dessa informanter tillgängliga.

3.2.3 Analysmetod

Analysmetoden genomfördes enligt en tematisk analysmodell (Braun och Clarke 2006, 16) för att hitta samband mellan attityder och andra intressanta teman i resultatet. Eftersom syftet var att

hitta attityder sökte vi efter återkommande uttalanden som tydde på attityder, och listade dessa. Därefter undersökte vi samband mellan attityderna och samlade ihop attityder som liknade varandra. Detta bildade teman av attityder som vi namngav enligt egna tolkningar, bland annat kunskap, tillit, misstänksamhet och positivitet.

4. Teori

I detta avsnitt beskrivs de teorier som ligger till grund för analysen av resultat. Teorierna är avdesign (eng. undesigning), utilitarism samt privatliv. Dessa har valts ut då de anses relevanta att diskutera i relation till resultatet och svaret på frågeställningen. Teorierna kommer användas för analys av resultatet ur ett samhällsligt perspektiv. Nedan följer en kortfattad redogörelse för respektive teoris huvudsakliga kännetecken och hur de är passande samt kommer att användas för analys i denna rapport.

4.1 Avdesigning

Teorin om avdesign anses relevant eftersom den ifrågasätter nödvändigheten av design av ny teknologi. Teorin syftar till att fatta beslut om ny design baserat på de långsiktiga konsekvenser den har potential att få (Pierce 2012, 957). Vi har valt Pierces beskrivning av teorin, som härstammar från Frys teori om eliminerande design (eng. elimination design), vilken bygger på att ifrågasätta en design och eliminera den om den inte bidrar till en hållbar utveckling (Pierce 2012, 958). Teorin har uppstått till grund av de negativa följder som uppstått inom fältet för människa-dator-interaktion i form av exempelvis sociala, miljömässiga och moraliska problem (Pierce 2012, 957). Teorin betonar makten designers har för att påverka användares liv och hur den makten inte bör missbrukas (Pierce 2014, 34). Idhes teori om mikroperception används av Pierce som argument för avdesign. Idhe menar att all teknologi har förstärkande och förminsande egenskaper, men att användarna ofta förbiser de förminsande i ljuset av de förstärkande. Som exempel används teleskopet, vilket ses som en framgång eftersom det

förlänger människans blick. Begränsningarna i synfältet som uppstår ignoreras lätt (Pierce 2012, 959).

Det finns olika grader av avdesigning som föreslås av Pierce. Den första nivån är *hämmande design* som innebär att hämma viss typ av användning av en annan design, exempelvis farthinder på vägarna som hämmar bilkörning (Pierce 2012, 960). Därefter kommer *förflyttande design*, vilket innebär att flytta en design från sin ursprungliga plats för att främja en annan typ av beteende, som att flytta TV:n från vardagsrummet för att minska TV-tittande. *Raderande design* är att bokstavligen förinta existensen av en design, vilket är svårt att i ett fritt samhälle genomföra men intressant i teorin. *Utestängande design* är att hindra en design från att fullföljas till färdigt stadium. Inom detta ramverk finns underkategorier som förtydligar ändamålet med respektive design (Pierce 2012, 961). Pierce beskriver *självhämmande design* och *självhämmande alternativ*, vilket är två varianter av design som hämmar sin egen användning. Det kan göras genom exempelvis strategiskt obekvämt placerade funktioner, som knappar, eller valmöjligheter till begränsad användning, för att användaren själv ska kunna minska sin användning (Pierce 2012, 961–962). Pierce skriver även om *ersättande* och *återställande design*. Att ersätta design med en modernare version och på så sätt avdesigna den gamla modellen är standard inom design. Att återställa design till ett äldre stadium av utvecklingen kan däremot ses som en annorlunda metod för design, men som görs exempelvis när människor väljer att odla egna råvaror hemma istället för att köpa producerad mat. *Exkluderande design* är att förflytta design ur vissa kontexter för att förändra beteendet hos omgivningen just där, vilket liknar *förflyttande design* (Pierce 2012, 962). *Skyddande design* är en aktivitet för att väcka uppmärksamhet för människor som inte drar nytta av en ny design, eller rentav riskerar att skadas av den, och på så sätt försöka hindra den, och görs exempelvis genom kampanjer eller demonstration (Pierce 2012, 963).

Pierce skriver om tre frågor som forskare har uppfunnit för att överväga nödvändigheten av ny design (Pierce 2012, 964, vår översättning):

”Kan teknologin ersättas av en likvärdigt genomförbar low-tech eller otekniskt tillvägagångssätt för situationen?”, ”Resulterar en teknologisk uppfinning i mer problem eller skada än situationen den är menad att vända sig till?” och ”Löser en teknologi en beräkningsmässigt lätthanterlig transformation av ett problem snarare än problemet själv?”.

I rapporten kommer teorin användas för att analysera huruvida metadata bör eller kan avdesignas, baserat på de attityder användare har, eftersom attityder kan ses som en konsekvens av designen. Vi försöker bedöma om metadata bidrar till en hållbar utveckling i relation till de sociala aspekter som kan komma att diskuteras under intervjuerna. Ides teori om mikroperception kan även användas som för att analysera vilka aspekter metadata är förstärkande och ur vilka det är förminskande. Vi analyserar om de förstärkande egenskaperna hos metadata framhävs framför de motsatta.

4.2 Utilitarismen

Teorin grundades av Jeremy Bentham, som även var hedonistisk utilitarist. Bentham ansåg att värdet av ett liv, eller en handling, bestäms av den grad njutning det tillför, enligt hedonismens fokus på njutning. Bentham definierade utilitarismens kärna, nyttan (eng. utility), som en egenskap hos objekt som kan producera lycka, framgång, njutning eller fördelar samtidigt som det motverkar de negativa motsvarigheterna (Dimmock och Fisher 2017, 13). Alltså är den rätta handlingen det som bringar bäst konsekvenser för störst antal människor. Detta gör teorin konsekventalistisk, det vill säga att moralen bestäms av handlingens följd. Ett liknande begrepp som beskriver teorin är teleologi, vilket betyder att den kännetecknas av någontings slut eller syfte. Relativismen ingår även här, som betyder att kontext och återigen konsekvenser har stor betydelse i att döma det rätta i en situation. Motsatsen är absolutism, som menar att en viss handling alltid är rätt eller fel, oavsett omständigheter (Dimmock och Fisher 2017, 14). Dimmock och Fisher (2017, 15) illustrerar detta med ett exempel om tortyr. En absolutist kan hävda att tortyr alltid är moraliskt fel, oberoende av hur eller varför den utförs. En utilitarist skulle däremot argumentera att tortyr i vissa fall leder till mer lycka och välmående för

majoriteten av människor, exempelvis om tortyr används på en terrorist för att provocera honom att avslöja sin plan och en terroristattack kan förhindras. Teorin är dessutom maximerande då den inte godtar agerande som bara skapar njutning, utan agerande som resulterar i maximal njutning för en maximal population. Utilitarismen kan även kallas opartisk då den strävar efter lycka för det största antalet människor och inte tar hänsyn till klass, kultur eller liknande sociala grupper. Alla människors njutning och brist på lidande värderas likvärdigt (Dimmock och Fisher 2017, 15).

För att kunna använda teorin i praktiken uppfann Bentham den så kallade *njutningskalkylen* som ett verktyg för att räkna ut vilken handling som resulterar i mest njutning för flest människor. Kalkylen beräknar en mängd faktorer som intensitet, varaktighet, säkerhet och avstånd till njutning (Dimmock och Fisher 2017, 16). Denna kalkyl är dock problematisk i flera fall. Det kan vara svårt att jämföra olika typer av njutning från fall till fall med en fast modell som kalkylen. Dessutom tar kalkylen bara människors njutning och lidande i beräkning, trots att utilitarismen ska vara likvärdig för alla och trots att djur bevisligen kan uppleva både njutning och smärta (Dimmock och Fisher 2017, 17).

Utilitarismen som en maximerande teori kan anses krävande att följa. Eftersom den kräver maximal njutning för den totala populationen människor tillåter den inga handlingar som enbart tillfredsställer individen (Dimmock och Fisher 2017, 17–18). Dessutom kan den relativistiska aspekten ifrågasättas då den inte främjar någonting absolut, därav varken demokrati eller mänskliga rättigheter. Inom teorin ryms heller ingen hänsyn till en människas avsikter med en handling, utan enbart konsekvenser. Om personen i fråga ämnade att göra gott för andra med sin handling men misslyckades, har denne agerat omoraliskt (Dimmock och Fisher 2017, 18). John Stuart Mill adderade sin egen tolkning av utilitarismen som kom att dela teorin i två läger. Detta med anledning av de problem han funnit med teorin, varav några beskrivs ovan (Dimmock och Fisher 2017, 20). Benthams teori klassas som en handlingsutilitarism och Mills som regelutilitarism. Mills nya version av teorin fokuserar mer på regler som är satta för att generera mest glädje för majoriteten om de följs (Dimmock och Fisher 2017, 22). Dessa ämnar att skapa

mer allmännyttan i det långa loppet, snarare än handlingsutilitarismens metodik att moralisera en handling i taget (Dimmock och Fisher 2017, 23). En annan skillnad Mill utgjorde var att värdera njutningens kvalitet lika högt som Bentham värderade kvantiteten. Förut betraktades enbart mängden lycka hos människor, Mill ansåg att det finns bättre typer av glädje än andra. Att njuta av intellektuell kultur ansåg han bättre än att njuta av uppfyllandet av djuriska lustar (Dimmock och Fisher 2017, 21). Mill ansåg också att individuell njutning är moraliskt godtagbart eftersom det bidrar till den totala mängden lycka hos samhället (Dimmock och Fisher 2017, 20).

Utilitarismens princip testas i denna rapport på fallet metadata och undersöka om det innebär bäst utfall för majoriteten av människor. Detta genom att diskutera på vilket sätt metadata producerar njutning respektive lidande för våra informanter, samt i så fall vilka av dem, med målet att bestämma vilket som är övervägande. Detta görs utefter informanternas uttryckta attityd till metadata. Utilitarismens grundstenar, som relativism och maximalism kommer att användas som jämförelse mot metadata.

4.3 Privatliv

För att analysera informanternas upplevelse och behov av integritet används Westins teori om privatliv (Westin 1966). Under intervjuerna i detta projekt undersöktes informanternas upplevelse av integritet i förhållande till sitt privatliv med anledning av metadata. Informanterna ställdes frågor om vilka typer av data de anser är personlig och/eller känslig, som de inte vill dela med sig av till andra. Westins teori om privatliv anser vi relevant för att analysera informanternas upplevda integritet då den berör hur individer påverkas av övervakning via insamling av data (Westin 1966). Vi finner den dessutom relevant då informanternas definition av integritet många gånger handlade om att kunna agera utan att bli övervakad, och att behålla privatlivet för sig själva.

Westin en artikel som reaktion på samtidens övervakningssamhälle i USA (Westin 1966, 1003). I artikeln beskriver Westin olika former av övervakning som USA använder, som fysisk och psykisk. Intressant för denna rapport är hans beskrivning av dataövervakning (Westin 1966,

1004). Westin beskriver ett antal trender som revolutionen av datorer innebär. Först och främst företagens övergång till datorer som lett till en omfattande dokumentering av människors liv. Individens data, exempelvis passinformation, födelseattest, körkortsinformation, bankuppgifter, personuppgifter och telefonloggar, som tidigare inte registrerades, finns numera lagrat i olika databaser. Teknikens utveckling tillåter nu massiv lagring i små format, som mikrofilm. Tack vare datorernas kapacitet kan företag lagra information om sina kunder, anställda och medlemmar, vilket i sin tur möjliggör att företagen ifrågasätter och ställer högre krav på dessa (Westin 1966, 1010–1011). Dessutom har tekniken möjliggjort kommunikation mellan datorer och därmed lättare utbyte av data mellan företag och organisationer. Vissa företag delar även personliga data utan att stämpla den som konfidentiell. Sist förutspår Westin en ökad användning av kreditkort och utfasning av kontanter (Westin 1966, 1011–1012). För att sammanfatta dessa trender skildrar Westin ett framtida scenario där alla detaljer och aspekter av individens liv finns tillgängliga i olika databaser. Individens varje rörelse i vardagen skulle registreras för statens övervakning och få handlingar skulle förbli privata (Westin 1966, 1013–1014).

Westin kategoriserar begreppet privatliv i fyra stadier. Det första är isolering, där individen är avskild från andra, ensam med egna intryck och tankar. Detta är den yttersta formen av privatliv (Westin 1966, 1020–1021). Intimitet är nästa stadie, vilket innebär umgänge med individens närmaste, en liten grupp som familjen, vänner eller kollegor. Intimitet uppfyller det grundläggande behovet av mänsklig kontakt. Anonymitet är det tredje stadiet, när individen rör sig i samhället som en i mängden utan att bli ifrågasatt eller behöver ta ansvar för sina handlingar. Individen har större frihet att uttrycka sig eftersom människorna i omgivningen sällan fortsätter att delta i dennes liv (Westin 1966, 1021). Reservation är det fjärde, ytligaste stadiet av privatliv. Individen hämmar olika delar av sin personlighet, anpassat till olika sociala relationer och normer. Detta för att skydda sig själv från full utelämning och bevara detaljer som är för värdefulla, pinsamma eller personliga (Westin 1966, 1021–1022).

Westin argumenterar vidare för de fyra funktionerna av privatliv. Den första är personlig autonomitet, en tro på unikheter och individens mänskliga värde som finns i demokratiska stater

(Westin 1966, 1022). Westin beskriver människans behov av autonomitet som ett upprätthållande av mänskliga relationer i form av cirklar. I den innersta cirkeln ingår enbart individen själv, med sina djupaste hemligheter. Därefter fördelas individens relationer mellan cirklarna ut till de ytligaste bekanta där få personliga detaljer delas. Den innersta cirkeln är den mest sårbara, som kan riskeras av utomstående som inte respekterar gränsen eller anser att de gör intrång för att hjälpa till och att det kompenserar skadan. Westin menar att privatliv är avgörande för individens utveckling, utan ensamtid att tänka och experimentera försvinner individualiteten, som är en viktig byggsten för demokratin (Westin 1966, 1023–1024). Den andra funktionen är emotionell frigörelse. Människan antar ett flertal roller i vardagen baserat på vad de olika sociala situationerna kräver, något som är tröttsamt i längden och skapar ett behov av en fristad från detta då individen kan vara sig själv. På samma sätt behöver individen vila från det höga tempot och överraskningar livet innebär. Utöver detta behövs frigörelsen som tillåter att regler bryts emellanåt. Alla människor bryter regler eller normer av något slag och i ett fritt samhälle måste detta få ske utan straff, liksom de behöver utrymme att klaga på auktoriteter utan att stå till svars för det (Westin 1966, 1024–1025). Människor behöver även privatlivet för självutvärdering. De behöver tid i lugn och ro för att bearbeta lärdomar, moraliska tvivel och sitt egna beteende. Detta kan ses som en religiös upplevelse, men även de icke troende kan använda stunden till förlåtelse eller kontemplation. Kreativitet utvecklas bäst i ensamhet (Westin 1966, 1026–1027). Sist utmålar Westin begränsad och skyddad kommunikation som en funktion för privatliv. Det tillåter människan att dela vad den vill med vem den vill, utefter sina sociala relationer. Den kan dela privata saker med närstående, eller med professionella personer som garanterar att informationen inte kommer att användas mot individen. Begränsad kommunikation tillåter även gränser mellan exempelvis arbetsgivare och arbetstagare, vilket upprätthåller en hållbar arbetsplats. Begränsningarna tillåter oss att följa sociala etiketter i olika sammanhang (Westin 1966, 1028–1029).

I analysen använder vi de fyra stadierna av privatliv för att analysera vilka av dem som påverkas av metadata och hur. Vi försöker bedöma detta utifrån informanternas beskrivning av sin integritet och när de upplevt att den har riskerats. Med den kritiska händelsen som underlag ser

vi vilka stadier som ingår och analyserar hur informanterna uppfattar detta. Vidare undersöker vi hur väl Westins prognos stämmer med nutiden. De fyra funktionerna av privatliv appliceras på metadata för att analysera bland annat vilka sociala cirklar som påverkas av individens agerande med digitala artefakter och dess insamling av metadata. Vi analyserar om och hur metadata främjar eller hämmar emotionell frigörelse, självutvärdering och begränsad och skyddad kommunikation.

5. Resultat och analys

I detta avsnitt analyserar vi resultatet av intervjuerna inklusive de kritiska händelserna. En tematisk analys har använts för att strukturera innehållet i relevanta teman som vi funnit vid analys av studiens data och döpt efter de huvudsakliga attityderna som informanterna, å vår utsago, har uppvisat. I varje tema är informanternas resultat blandade, i diskussionskapitlet kommer de sedan delas upp enligt kategorierna yrkesverksamma inom IT (informant 3 och 4) och icke yrkesverksamma inom IT (informant 1 och 2).

5.1 Kunskap

Informanternas kunskap om metadata klassades enligt tre kategorier som vi skapat med hjälp av den tematiska analysen. Den kategori där flest svar från de två informanterna som inte är yrkesverksamma inom IT hamnade i kallar vi *grundläggande uppfattning*. De två yrkesverksamma informanterna inom IT redogjorde för metadata genom svar som vi klassar som *djupgående medvetenhet*. Informant 4, som arbetar med metadata för optimering av tjänster inom Video OnDemand, uttryckte en begränsad kunskap om ämnet till sitt fält. Därför kategoriserar vi hans kunskap som *djupgående nischad kunskap*. Emellertid uppvisade han också kunskap om metadata som vi klassade som *djupgående medvetenhet*. Gällande GDPR-lagen uttryckte samtliga fyra informanter en osäkerhet angående vad den innebär. Samtliga var medvetna om dess existens och kunde redogöra för dess användning på ett ytligt plan, men hävdade att de var dåligt insatta i vad den innebär i praktiken. De som var yrkesverksamma inom IT hade dock förmågan att uttrycka mer detaljer om lagen, trots att de ansåg sig själva som dåligt insatta. Detta

märktes inte minst vid diskussionen om den kritiska händelsen, då informanterna angav hur de tror att SL:s reseapplikation sparar metadata om deras sökningar. Informant 2 uttryckte följande ”*Dom samlar kanske in min position, tid, om jag köper biljett i appen, om jag kollar i förväg eller för att åka direkt*”. Informant 4 svarade på samma fråga med att SL sparar metadata för att analysera vilka sträckor som är populära, informera rätt personer om vilka sträckor som ska tas ur drift, användarens plats (om hen godkänt detta) och därmed hur lång tid en viss resa tog jämfört med beräknad tid. Vidare sparas användarens populära transportmedel och hållplatser, samt generella data för att kunna samla statistik över SL och optimera både applikationen och verksamheten, enligt informant 4. Informanterna var vana användare av digitala artefakter på fritiden, samtliga använde smartphone och dator. Informant 3 hade även en smartklocka, smart-TV, Google Home och Alexa. Informant 4 använde bland annat chromecast, Android-TV och TV-hub.

5.2 Försiktighet

Negativa och försiktighetstagande attityder till teknologin och metadata fanns bland informanterna. Dessa attityder handlade främst om att på ett medvetet sätt *undvika risker* de ansåg fanns med att metadata loggas.

Till exempel gällde detta hur informanterna uttryckte sig *ogilla övervakning*. Informant 3 uttryckte detta genom att väga de positiva aspekterna, minskande av kriminalitet - emot de negativa aspekterna, som ofta var integritetskränkande. Han ansåg att insamling av metadata är för minimerande av invånarnas integritet för att det positiva ska kunna vägas mot det negativa. Informant 3 uttrycker det enligt följande på frågan om vilka för- och nackdelar han anser att det finns med metadata ”*Mest nackdelar, men fördelar för polisen, och för den nationella säkerheten. Men den inskränker så mycket i den personliga integriteten så det är inte värt det*”. Flera av informanterna poängterade även att de inte kände möjlighet att själva styra över hur deras data loggas och att detta resulterade i en känsla av *maktlöshet*. Bland annat informant 4, som ansåg att det aldrig kommer gå att vara helt osynlig i användandet av digitala artefakter och

sa ”Du kommer aldrig vara helt osynlig när du använder olika tjänster, så är det”. Enligt honom är detta en negativ aspekt för integriteten som påverkar användarna.

Temat försiktighet baseras även på den *medvetenhet om risker* som framkommit under intervjuerna. Informant 3 uttryckte följande ”*det som är oroväckande är att datan säljs vidare till dataaggrigeringsföretag, som i den här artikeln jag läste om ett experiment där miljoner av exempeldata kunde identifiera specifika personer(...)*Jag vet att risken finns därute, jag bryr mig inte om att vara i en anonym mängd, jag vill undvika att identifieras”. Även informant 4 berörde detta ämne när han uttryckte att han i vissa fall undviker specifika företag och deras tjänster med hänvisning till hans medvetenhet om att de säljer informationen vidare till en tredje part, ”*det har hänt att jag undviker vissa tjänster för att jag vet hur de använder sig av eller säljer vidare datan, men det är väldigt sällan*”. Informant 4 påpekade även risken med att metadata hamnar i fel händer. Han exemplifierade detta med den kritiska händelsen som handlade om SL:s insamling av metadata, om vad som kan hända ifall fel person får ta del av statistiken och kan se vid vilken tid flest människor är samlade på specifik plats. Informant 4 belyste även de personliga problem som kan uppstå vid oförsiktiga uttalanden på sociala medier, vilket kan spåras enkelt med hjälp av metadata långt bak i tiden. Han exemplifierade detta som ”*(...)säg att jag hade skrivit ett negativt anonymt inlägg om mitt företag för fem år sedan för att jag var missnöjd med en tjänst, hade det kunnat knytas till mig hade jag inte kanske fått jobb här.*”. Denna medvetenhet resulterar enligt informanterna i olika åtgärder, bland annat uttrycker informant 3 det som att han *medvetet agerar* för att undvika sin läggning av metadata, ”*jag gör vad jag kan, när jag kan det. Jag använder brandvägg, försöker använda tjänster som inte är min operatör, använder en VPN-tunnel, använder en annan tjänst som jag har högre förtroende för*”. Medvetenheten resulterar även i *hämmande användning på grund av säkerhetstänk* och informant 2 anger att han undviker att lägga upp bilder på sina barn i sociala medier för att undvika exponeringen av dem. Informant 4 anser att även han hämmas i viss användning och exemplifierar detta med företag som har användarvillkor vilka är komplicerade eller svåra att tyda. Han anser att detta tyder på något misstänkt och försöker då att använda en annan, likvärdig tjänst. Komplicerade användarvillkor kan enligt informant 4 exempelvis betyda att datan säljs

vidare alternativt att företaget tillåts addera kakor som samlar in hans användarmönster vilket enligt honom äventyrar hans känsliga information.

5.3 Tillit

En annan återkommande attityd under intervjuerna var *tillit till företag* och *tillit till myndigheter eller auktoriteter*, vilket var avgörande för hur informanterna valde att använda digitala artefakter som sparar metadata. Informant 3 uttryckte en tillit till banken som gjorde att han inte hade några problem att dela känslig information som betaluppgifter med dem via digitala artefakter. Tilliten grundade sig i att informanten alltid tvingats lita på att banken hanterar hans pengar på ett säkert sätt, och att de digitala funktionerna endast är en förlängning av det. Samtidigt är han medveten om risker med att lita på banken eftersom han inte har någon aning om vad som faktiskt försiggår bakom en tjänst som Mobil bankID, ur sitt perspektiv som IT-säkerhetskonsult. Informant 4, ur sitt professionella perspektiv, hade en tillit till företag som baserades på det egna företaget och hoppades att andra företag använder metadata i samma syfte - att optimera tjänster för användarna. Han berättade att det egna företaget enbart samlar metadata länkat till användare som är sparade som ID-nummer i en databas, alltså kan företaget inte se den specifika individens identitet. Följaktligen innebär det att när en användare avslutar sin tjänst hos företaget kan de ej sälja datan vidare till tredje part och koppla den till individen. Företaget kan enbart se att ID-numret representerar en typ av användare som varit kund där. Dessa faktum beskrev informanten som motiv för att känna tillit till företag som hanterar metadata på detta sätt. Gällande medicindata hade informant 4 också en tilltro till myndigheter som tillhandahåller dessa sorters data om honom. Informant 4 visade även tilltro till företag som Facebook då han trodde att dem, liksom andra företag, samlar metadata för optimering av tjänsten. Han visade dessutom förtroende för GDPR-lagen och de myndigheter som reglerar denna. Informant 2 angav också tillit till banken av anledningen att hans bank utlovat säkerhet för hans känsliga information. Informant 1 nämnde tillit till Vårdguiden 1177, samtidigt som hon inte var helt säker på att tilltron var befogad. Hon kunde heller inte motivera tilltron för myndigheten mer än att hon får en känsla.

Några informanter utgav sig för att göra ett *medvetet urval av företag* baserat på den tillit de hade eller saknade i olika fall. Informant 2 sade sig föredra att betala med de företag han bedömer som säkra, exempelvis PayPal, istället för att betala direkt med internetbanken. Han berättade att han ibland väljer bort vissa tjänster i sin digitala användning för att undvika intrång på integriteten. Informant 3 påpekade att vissa företag går att undvika, som Amazon och Google, då deras högsta syfte är att tjäna pengar, men att andra inte kan undvikas. Informanten var av uppfattningen att företag som NSA, som gjort sig skyldiga till massavlyssning av människor, kommer att kunna fortsätta med det om de vill och att medvetna val av företag inte alltid hjälper. Ett tema som liknande det medvetna urvalet av företag baserat på tillit syntes i form av hur informanterna agerar med tjänsterna, vilket exemplifieras vidare ovan under rubriken *Försiktighet 5.2*.

5.4 Paradoxalt beteende

Ett tema som uttrycktes i olika former bland informanterna kallar vi *paradoxalt beteende*. Det kännetecknas av att informanten har en uppfattning om att hans digitala användande efterlämnar metadata, samt känner någon nivå av tillit till företag eller myndigheter, men väljer att agera mot sin kunskap och tillit. Den renaste formen är händelser informanter beskriver som vi benämner som *paradoxer*. Informant 1 berättar, som ovan nämnt, att hon litar på Vårdguiden 1177, men att hon inte kan veta säkert. Hon beskriver även att hon sällan ifrågasätter situationer när hon riskerar att utlämna känslig data, och om hon gör det kan hon ofta lämna ut datan - exempelvis betalinformation - trots att en webbsida känns opålitlig. Informant 2 delger att han undviker att dela bilder på sina barn på sociala medier, samtidigt som han inte har något emot att hans flickvän gör det. Informant 3 yttrade att han använder Google som sökmotor, trots att han vet om att de samlar in data om hans sökningar. Detta beror på att han ser Google som den bästa sökmotorn. Nästa form av paradoxalt beteende kallar vi *halvhjärtade försök att agera medvetet*. Informant 2 svarade att han påverkas väldigt lite av vetskapen om metadata och att han försöker att ibland undvika att använda sitt kreditkort, men inte alltid. Informant 4 menar att han ibland undviker vissa tjänster då han vet hur de använder och säljer vidare datan, men att det är väldigt

sällan. Oftast använder han tjänsten ändå, om han vill det. Informanten yttrar även i sitt resonemang om företagets användning av metadata för användaroptimering att han väljer att inte vara orolig för vad de gör med datan. Detta kategoriseras som att agera *medvetet naivt*. Informant 3 uttrycker ordagrant att han hoppas naivt att företag på webben sparar så lite data som möjligt om användarens agerande, under en diskussion om kakor.

En annan aspekt av det paradoxala beteendet är att flertalet informanter ser *sig själv som ointressant, anonym* för att profilera i en större insamling av metadata, och därför inte har någon anledning att oroa sig till skillnad från andra. Informant 1 sa, vid frågan om hur hon tänker om din integritet vid användning av digitala artefakter, att ”*Jag är inte en offentlig person och jag syslar inte med något fuffens så det rör mig inte*”. Hon uppger att hon lämnat ut sitt telefonnummer och mejladress till alla möjliga företag, som ringer och vill sälja saker, vilket är jobbigt. Emellertid är det inte värre än att hon står ut, och eftersom det är den värsta konsekvensen hon mött så ser hon ingen anledning att förändra sitt beteende. Eftersom hon dessutom får gåvor av företagen emellanåt kan hon dessutom utnyttja systemet för *egen vinning*, en annan aspekt som återkom bland informanterna. Informant 1 delgav att hon vid ett tillfälle avsiktligt sökte på Google efter företag som erbjuder städhjälp i hemmet, för att försöka få riktade erbjudanden om det. Alltså har hon inget problem att dela sina metadata om det innebär egen vinst. Även informant 2 uppskattade riktad reklam, då han enbart vill se det han är intresserad av och kan få det genom de metadata han efterlämnar. Informant 2 ser också att han kan vinna på att dela metadata genom fördelarna som exempelvis GPS-funktioner, och därför är det värt att dela sin platsinformation. Han uppskattar även att han blir rekommenderad, förutom reklam, tjänster han föredrar, som PayPal vid köp online. Informant 4 ser sig själv också som ointressant för profilering. Han resonerar att det hade varit annorlunda om han haft en målbild, en stalker eller liknande hot som gjort honom intressant att spåra via metadata. Informant 3 var också av åsikten att han inte är intressant för att profileras, med undantag för att kunna sälja saker till honom.

5.5 Positivitet

Positiva attityder framkom främst då det ansågs att *metadata hjälper* informanterna i olika aspekter och detta kallar vi *positivitet*. Informant 1 uttryckte en positiv attityd gällande metadata i samspel med kriminalitet online, där hon ansåg att metadata underlättar spårningen av kriminella. Informanten sa att poliser behövs online i samma utsträckning som poliser på gatan och att arbetet underlättas av förenklade metoder att följa och spåra specifika personer. Hon exemplifierade detta med uttalande från NSA och FRA där dessa organisationer poängterat hur de använder metadata för att spåra specifika, misstänkta gärningsmän. Informant 2 uttryckte även att metadata inger en känsla av att hjälpa honom, exempelvis uttrycktes *bekvämligheten* med personaliserad reklam där informanten ansågs sig blir serverad med köpförslag som passar honom och hans rörelsemönster. Detta knyter an till attityden *egen vinning*, liksom att informant 2 ansåg att det hjälper honom att endast se vad han kommersiellt *är intresserad av*. Informant 4 uttrycker liknande synpunkt då teknologin hjälper honom att optimera sin användning av tjänster vilket ger möjlighet att utnyttja en tjänst på bästa sätt, vilket är en annan aspekt av den *säljande* attityden. Informant 4 exemplifierar med Video OnDemand-tjänster, som även nämns under *5.1 Säljande*, där rekommendationer kan ges från de mest aktiva tittarna, till de mindre aktiva kunderna för att på så sätt motivera de inte så aktiva tittarna att se på mer och då utnyttja tjänsten till fullo. Optimeringen är då enligt informant 4 att hjälpa kunder hitta rätt och till detta kan metadata användas som hjälpmedel.

Att teknologi och i detta fall *metadata hjälper användarna* understryks av de informanter som *principiellt var för digital utveckling* av samhället. Informant 1 anser att det alltid finns bakåtsträvare i samhället och att detta hämmar samhällets utveckling. För att detta skall undvikas bör invånarna acceptera utvecklingen och metadatan som enligt henne är en del av utvecklingen. Informant 1 fortsätter resonemanget med synpunkten att det finns värre saker i samhället än samlad information om oss - och detta exempelvis den kriminalitet som informanten talat om ovan. Samhällets digitala utveckling kan minska denna kriminalitet och stoppa olagligheter som

sker online med hjälp av förenklad spårning och detta leder till den positivism av utvecklingen som leder till teknologins möjlighet att hjälpa.

Övergripande för denna positivitet var att samtliga fyra informanter, i olika utsträckning, kände sig *orädda för metadata*. Detta är dels beskrivet i avsnittet ovan, *5.4 Paradoxalt beteende* där informanterna *ser sig själva som ointressanta och anonyma* för att profilera. Vidare exemplifieras även denna oräddhet av informant 1 som berättar att hon har samma lösenord till många olika sidor och trots vetskapen om att ifall ett lösenord läcks, läcks alla lösenord är hon inte speciellt brydd av att förskaffa sig säkrare inloggningsuppgifter. Även informant 2 uttrycker denna oräddhet i diskussion gällande kryptering av privata konversationer och i frågan om han väljer specifika applikationer för att kryptera sina konversationer, *”det är väl ett plus att det krypteras, men jag väljer inte applikation efter det nej”*.

5.6 Okunskap

I de genomförda intervjuerna uppkom ett flertal insikter som tyder på *okunskap* hos informanterna. Informant 3 berättade att han aldrig tänkt på digitala betallösningar som känslig information eftersom han är uppvuxen i ett kontantlöst samhälle. Det utbredda användandet av tjänsterna är enligt informanten en del av normaliseringen vilket har lett honom till att inte betrakta digitala bankuppgifter som känsliga, samtidigt som han vid frågan svarar att det i allra högsta grad är känsliga uppgifter. Samtidigt kommenterar han, precis som ovan nämnt i temat *5.3 Tillit*, att han litar på företag och att de gör det de ska för att skydda honom. Denna okunskap baseras även på de informanter som kommenterar sig inte ha vetskap om den Snowden presenterade om NSA i 2013. Informant 4 uttrycker det enligt följande, *”jag vet inte exakt allt kring det han gjorde, jag vet bara att han delade ett gäng dokument som den amerikanska staten inte ville skulle delas. Exakt vad som rymdes i dem filerna har jag inte koll på. Jag kanske låter lite pessimistisk, men det finns nog en hel del sånt som folk inte vill ska komma fram av olika anledningar”*. Samtidigt som informanten inte säger sig ha full koll på vad Snowden gjorde kommenterar han att Snowdens arbete var viktigt och av stor betydelse. I och med ovan citat kan det även antas att okunskapen bottnar i *ett ointresse för nyheter*. Även informant 1 innehar

liknande inställning till Snowdens uttalanden, och hon uttrycker det enligt följande, ”*jag har inte sett filmen (om Snowden), så tror det inte påverkat mig direkt. Men man har ju hört saker som gör att man blir lite mer negativt inställd. Men direkt påverkad skulle jag inte säga nej*”.

5.7 Behov

Informanterna uttryckte även flera behov som ledde fram till olika inställningar gällande metadata. Främst uttrycktes behovet av privatliv som oftast benämndes i samband med kritisk inställning till metadata. Informant 2 anger att integritet för honom är att själv få välja vad en vill dela med sig av och med vem - det som för honom är personligt är av stor vikt att behålla privat för att upprätthålla känsla av integritet. Han delger även att hans *behov av privatliv* gäller barnen, och precis som ovan nämnt i 5.2 *Försiktighet*, är det av stor vikt för informanten att inte exponera sina barn. Informant 3 anser liknande att hans behov av privatliv berör rättigheten att göra det man vill utan att riskera att bli bevakad. Han anser även att metadata riskerar privatlivets integritet eftersom det kan kartlägga hans beteendemönster och därmed exponera honom som person. I paritet uttrycker även informant 4 att han har ett behov av privatliv och att denna tar sig uttryck då han vill skydda sin egen person. Han anser att det idag inte finns en problematik med metadata, då den enligt honom inte riskeras att spridas. Detta på grund av att företagen, enligt honom, inte samlar information om specifika personer utan att det som samlas istället sparas som ID-nummer där det inte finns möjlighet att spåra vilken person som gjort vad. Han anser dock att det skulle vara kritiskt om denna typ av anonymisering inte fanns och att detta skulle leda honom till att dölja sin person online. Informant 1 uttrycker även vissa behov av privatliv, som att hon inte vill att vem som helst ska få ta del av känslig information som medicindata, eller att ingen ska få reda på vem hon är baserat på hennes inlägg på sociala medier.

5.8 Säljande

Informant 4, som arbetar med metadata för optimering av tjänster inom Video OnDemand, uttryckte en attityd mot metadata som kan beskrivas som *säljande*, samtidigt som han kunde resonera om andra aspekter av metadata under intervjun. Han påpekade många funktioner

metadata har som kan användas för att optimera olika tjänster, exempelvis genom att personalisera dem. Informanten argumenterade för att metadata kan hjälpa användare att utnyttja tjänstens fulla potential. Detta exemplifierar han med sina egna arbetserfarenheter. Han har upplevt att användare går miste om innehåll som passar deras intressen på grund av att de inte exponeras lika mycket som de populära filmerna och serierna, som säljer sig själva. Detta kan motverkas genom att användarnas metadata utnyttjas för att systematiskt profilera användare och rekommendera innehåll som är lämpat för deras intressen. Alternativet är att manuellt testa vilka grupper som kan uppskatta ett specifikt innehåll, och då gynnas inte individen. Alltså betonar informant 4 både *effektiva* och *för användaren gynnande* aspekter. Han påpekade själv att han förmodligen har en positiv bild av metadata för att han arbetar med det för optimering av tjänster och sällan ser negativa konsekvenser av det i arbetet.

5.9 Misstänksamhet

Attityden misstänksamhet återfanns i flera intervjuer, gällande att metadata informanterna lämnar används till något särskilt syfte som de själva inte informeras om. Temat uttrycktes generellt sätt i två varianter: *misstanke om övervakning* och *misstanke om något bakomliggande*. Informant 1 beskrev sin kunskap om vad metadata är som att ”*Jag tror att det är saker som kanske sker bakom det jag gör*”. Därefter angav hon att hon tror att metadata är exempelvis information som GPS-koordinater, filstorlek på en bild och vilka som är med på bilden. Informant 2 svarade på samma fråga med ”*Jag tror att det är typ datan som inkluderas i det jag gör, den datan som jag inte ser*”, vilket också antyder att han ser metadata som något som sker bakom kulisserna, osynligt för gemene man. Informant 2 gissade även att metadata kanske säljs vidare till tredje part, men visste inte säkert. Informanten angav som nackdel med metadata att någon kan använda den för att se rörelsemönster hos honom. Informant 3 tog upp problematiken om de anklagelser som riktats mot Facebook om att de har använt röstsamtal som gjorts via tjänsten för att kunna fortsätta avlyssna användarna efter samtalet, för att sedan kunna rikta reklam mot dem. Informanten gav detta som ett exempel på anledningar han har att misstänka att något outtalat sker som ger hon känslan av att hans integritet riskeras. Informanten har även förstått att reklamen riktas efter sammankopplingar som görs mellan användarens aktiviteter på

olika webbplatser, och att det tyder på bakomliggande aktiviteter. Informant 3 sa, vid diskussionen om Edward Snowdens upptäckt av NSA:s massavlyssning genom metadata att han redan innan nyheten misstänkte att något sådant kunde pågå. Nyheten bekräftade mest vad han trodde.

I följande avsnitt utvecklas analysen av resultatet utifrån de tre teorier som presenterades i 4. *Teori*. Syftet är att tolka resultatet ur tre teoretiska perspektiv, vilka sedan hjälper till att besvara forskningsfrågorna. För analysens skull diskuterar vi informanternas uttalade attityder, i diskussionen sammanfattar vi informanternas attityder utifrån ett större perspektiv där deras agerande inkluderas.

5.10 Avdesigning

Vi analyserar om teorin avdesign är relevant för metadata genom att evaluera informanternas attityder och på så sätt tolka teknologins långsiktiga konsekvenser. Dessa långsiktiga konsekvenser kan enligt teorin avgöra om funktionen av teknologin bör om-/avdesignas.

Enligt teorin avdesign har designern möjlighet att påverka användarens liv och det är av stor vikt att denna makt inte missbrukas (Pierce 2014, 34). Ett exempel på potentiellt maktmissbruk är användningen av användarvillkor som bland annat upplyser användarna om hur företaget hanterar lagrade personuppgifter (Norberg, Horne och Horne 2007, 120). Genomförda intervjuer visar att läsförståelsen i dessa kan vara svår och att användare måste besitta förståelse för språkbruket för att förstå dessa, informant 4 som arbetar med metadata säger följande, *”Det har hänt att jag undviker vissa tjänster för att jag vet hur de använder sig av eller säljer vidare datan(...)jag inser när jag är inne och läser kriterierna om hur de använder datan, då vet jag vad det betyder och känner att jag kanske inte vill och då kanske jag väljer ett alternativ om det finns(...)jag har jobbat med IT i ett antal år så förstår jag ju lingon”*. När GDPR lagstodgades 2018 var en målsättning att verka integritetsstärkande och exemplifiera användarvillkoren och användningen av dessa (Datainspektionen 2018). Resultatet från våra intervjuer visar att denna målsättning ännu inte har uppnåtts fullt ut. Informant 2 delger följande, *”Med tanke på alla mejl*

jag fått borde jag veta mycket (om GDPR), men jag kan faktiskt inte så mycket. Mer än att om ett företag har uppgifter om dig så ska de enligt GDPR göra så att du kan höra av dig till dem och be de ta bort alla uppgifter de har om dig. Det är väl typ kontentan av det hela. Men jag har ganska dålig koll faktiskt". Även informant 4 uttrycker viss skepsis till funktionen av GDPR då han anser att det bara lett till att användarna idag måste godkänna att data om dem lagras, vilket förut

genomfördes i det dolda. Studien av Jonsson och Olsson bekräftar även att användare inte läser användarvillkoren för att avgöra om ett företag är tillförlitligt, utan bedömer det utifrån de tillstånd tjänsten kräver av användaren (Jonsson och Olsson 2018, 1). Användningen av användarvillkor skulle därmed kunna anses ineffektiv och i förlängningen kan det också tolkas som ett maktmissbruk vilket uppstår när designerna kan påverka andras liv. Enligt teorin om *Avdesign* är detta inte en hållbar utveckling i relation till sociala aspekter och kan vara anledning nog att avdesigna teknologin.

Vidare är metadata både förstärkande och förminskande vilket informanterna uttryckt i respektive intervjuer. Det främsta problemet är att de förminskande funktionerna ofta förbises bakom de förstärkande (Pierce 2012, 959) och det kan därför vara svårt att förskaffa sig en rättvis bild av den fullständiga funktionen. Förstärkande funktioner som poängterades var bland annat att teknologi hjälper användarna, det utvecklar samhället, gynnar användare och kan inge tillit till företag. Förminskande funktioner var istället att metadata kan vara integritetskränkande, skapa maktlöshet, inge en känsla av övervakning och behov av att verka medvetet för att undvika att bli bevakad. Hur de olika funktionerna ter sig diskuteras i avsnitt 5. *Resultat*. Hur funktionerna inger njutning och lidande till användarna diskuteras även nedan, med utgångspunkten utilitarism. Kombinationen av de båda betyder att metadata både hjälper och stjälper, beroende på kontexten där den används. Denna kontext kan även baseras på vem som är intressant, de genomförda intervjuerna visar tydligt att företag och privatpersoner har olika vinning av metadata och att detta bestämmer vilka egenskaper som är förstärkande och förminskande. Exempelvis informant 4 som talar som både privatperson, samt ur vinkeln av ett företag (som yrkesverksam inom VOD) säger följande *"(...)de mest aktiva tittar på den här*

versionen av olika serier, då kan vi boosta de som inte tittar lika mycket, men som kan verka intressant. Så att de kan utnyttja tjänsten de betalar för”. Detta uttrycker främst företagets åsikt, vilket är att sälja fler produkter. Till skillnad uttrycker informant 3 att integritet för honom är *”...rättighet att göra det man vill utan att bli snokad på(...)att kunna kolla och dela saker utan att någon hänger över axeln och samlar in. Det kan vara vardagliga saker, som att jag vill kunna söka resor på SL utan att de kartlägger mina rörelser”*. Det visar en stor differens mellan vem som är intressenten och vad som är produkten, de förminskade och förstärkande egenskaperna är varierande beroende på vem som frågas.

Vi anser därför att det är problematiskt att avgöra om uppfinningen metadata resulterar i störst andel problem eller om den främst hjälper. Detta eftersom de förstärkande och förminskande funktionerna är i mångt likvärdiga. Dock visar intervjuerna att våra informanter känner mer lidande än nytta i användandet av metadata och därmed kan det diskuteras att metadata stjälper mer än det hjälper. Främst belyses detta då teknologin används i annat syfte än vad som från början var dess syfte. NSA poängterade att metadata används i syfte att motverka terrorism och informanterna diskuterade även dem att metadata är bra ur en säkerhetssynpunkt, exempelvis informant 1 som uttryckte det enligt följande, *”det kanske skrämmer någon att typ inte hålla på barnporr och andra kriminella saker. Internet har ju varit ett stort hål där man inte kan komma åt folk som håller på med kriminella saker. Och förhoppningsvis kanske metadata och digitala fotspår kan underlätta att komma åt dessa och på så sätt underlätta brottsutredningar”*.

Samtidigt har NSA inte belägg för att någon kriminell handling faktiskt har stoppats med hjälp av metadata (Sundström 2015) och informanterna diskuterade vidare om det är av vikt att bevaka samtliga användare för att finna några kriminella. Informant 3 i distinktion till informant 1 tyckte att det trots möjligheten att stoppa kriminalitet är för integritetskränkande att lagra så mycket information om användare. *”Jag ser mest nackdelar (med metadata), men fördelar för polisen, och för den nationella säkerheten. Men den inskränker så mycket i den personliga integriteten så det är inte värt det”*.

5.11 Utilitarismen

För att avgöra om metadata är moraliskt försvarbart enligt utilitarismen undersöker vi om informanternas attityd till det kännetecknas mest av lidande eller njutning. Vi resonerar att attityden är den tydligaste konsekvensen av metadata i detta fall, med tanke på frågeställningens karaktär.

De attityder som kan klassas som lidande är de som hamnar i kategorierna *försiktighet*, *okunskap* och *misstänksamhet*. Detta kan motiveras av informanterna som uttrycker sitt *ogillande* av den *övervakning* metadata används till, exempelvis informant 3 som menar att det inkräktar på integriteten. *Maktlösheten* som flera informanter upplever gällande sina digitala fotspår kan tolkas som ett lidande. De informanter som är *medvetna* om att det finns *risker* med sin användning av digitala artefakter och *agerar medvetet* därefter för att skydda sig mot dem indikerar att de försöker undvika ett lidande som de annars utsätts för. Även varianten av attityden, *hämmad användning*, antyder ett lidande eftersom informanterna i fråga inte vågar utöva sin fulla användning av sina digitala artefakter. *Misstänksamhet* tolkar vi som lidande eftersom berörda informanter tror sig utnyttjas av kända eller okända parter som analyserar deras beteende utan deras vetskap. Misstänksamheten uttrycktes olika av informanterna men gemensamt skildras känslor av att metadata är något som pågår i det dolda och styrs av makter med kommersiella mål. *Okunskap* kan orsaka lidande eftersom det rimligen kan leda till maktlöshet.

Attityder som kan tolkas präglade av njutning är *tillit*, *positivitet*, *säljande* och till viss del *paradoxt beteende*. Tillit tolkas som njutning eftersom informanterna beskriver tilliten till olika företag eller myndigheter som en trygghet, en befrielse från oro. De positiva attityderna som att *metadata hjälper*, exempelvis för att spåra kriminella, och att vissa informanter är *orädda* inför metadata, ser vi som tecken på njutning. Informant 1 som är *principiellt för metadata* resonerar att metadata är en naturlig del av samhällets utveckling och att det leder till fler för- än nackdelar. Likaså informant 4 som hade en *säljande* attityd skildrar metadata som något som kan

skapa många fördelar för människor, och i förlängningen kan fördelarna tolkas som njutning. Attityden att metadata kan användas för *egen vinning* är av samma karaktär och vinningen innebär följaktligen njutning för användaren.

De attityder som kan tolkas som lidande uttrycktes något fler gånger under intervjuerna än de motsvarande som klassas som njutning. Enligt utilitarismen skulle metadata inte vara moraliskt försvarbart eftersom det leder till mer lidande än njutning för informanterna (Dimmock och Fisher 2017, 14). Bland informanterna uttrycktes åsikter som överensstämmer med utilitarismen, exempelvis informant 3 som sa att metadata innebär *”Mest nackdelar, men fördelar för polisen, och för den nationella säkerheten. Men den inskränker så mycket i den personliga integriteten så det är inte värt det”*. Detta påstående tyder på att informanten gjort ett moraliskt övervägande av konsekvenserna och funnit att metadata orsakar för mycket lidande. Informant 1 använder samma resonemang men är av motsatt åsikt. Informant 1 menar att om metadata kan stoppa kriminalitet som pågår online så är det värt den potentiella risk mot integriteten som finns. Alltså har hon övervägt att metadata kan resultera i mer njutning, tack vare den minskade kriminaliteten, i relation till det lilla lidande insamling av data om människor orsakar.

För att undersöka om metadata är relativistiskt bör en ställa sig frågan om metadata enbart används i de fall det kan skapa njutning och minska lidande för största möjliga antal människor (Dimmock och Fisher 2017, 14). Informant 3 exemplifierar hur metadata kan förhöja användarens upplevelse och interaktion med olika digitala tjänster tack vare dess möjlighet till personalisering. Han menar att om hanteringen av datan sköts på alla företag som den sköts på hans arbetsplats, genom anonyma ID-nummer som inte kan spåras till individen, finns små eller inga risker för individen. Denna situation skulle kunna ses som moraliskt korrekt enligt utilitarismen utifrån sin kontext. Emellertid förekommer metadata i sammanhang då syftet är att profilera ett företags kunder, enligt informanterna 3 och 4. Metadata och även profilerna kan även säljas vidare till andra företag, vilket i så fall anges i stundtals otydliga användaravtal, något som informant 4 anger kan resultera i att användares känsliga data delas med fler parter än vad användaren känner till. I detta fall är det svårt att se hur hanteringen av metadata skapar njutning

för majoriteten av människor. Snarare kan hävdas att användandet gynnar företagen och deras vinst, på bekostnad av användarna som bör utgöra en majoritet. Enligt det resonemanget kan vi inte heller påstå att metadata är maximerande, då majoriteten av människor inte gynnas (Dimmock och Fisher 2017, 15). Däremot enligt informant 3, finns fördelar för gruppen tack vare att individen profileras, vilket tyder på maximalism i någon grad.

5.12 Privatliv

Genom att undersöka informanternas skildringar av metadatans roll i deras liv kan vi se vilka av Westins fyra stadier av privatliv påverkas av metadata och hur. Informant 4 är bevisligen av uppfattningen att all användning av digitala tjänster lämnar någon typ av spår efter sig: *”Du kommer aldrig vara helt osynlig när du använder olika tjänster, så är det”*. Detta antyder att samtliga stadier påverkas av metadata under förutsättningen att digitala artefakter används i situationen, något som exemplifieras av informant 4:s beskrivning av hur SL samlar metadata, som beskrivs i 5.Resultat. SL:s applikation kan naturligtvis användas när individen befinner sig i både det isolerade stadiet för att planera en framtida resa eller det intima stadiet för att resa i grupp. Informant 3 delgav att han ibland undviker att använda vissa tjänster via digitala artefakter på tunnelbanan av rädsla för att någon ska kolla över hans axel och se känslig information. Alltså påverkas informanten i det anonyma stadiet. Likaså kan applikationen användas i stadiet av reservation, vilket i detta fall är svårt att skilja från det anonyma stadiet, och därmed påverkas av metadata. Utöver diskussionen om SL:s reseapplikation framkom yttranden från informanterna som tydliggör en önskan om att få reservera sig som de vill. Informant 2 definierade sin tolkning av integritet som *”Det handlar väl om hur mycket man vill dela med sig om - vem man är och vad man gör. Det som är personligt som man kanske vill hålla hemligt”*. Uttalandet anser vi stämmer väl in på Westins beskrivning av reservationsstadiet, att individen väljer vilka delar av sin personliga information omgivningen får ta del av (Westin 1966, 1021–1022). Vår tolkning av reservationsstadiet är att det inte nödvändigtvis är särskilt från de andra stadierna, utan är ett förhållningssätt till människor i både den intima och anonyma omgivningen. Reservation kan beskriva informanternas vanligaste definition av integritet. Alla

fyra informanter uttrycker i olika grad ett behov av privatliv. Informant 1 beskrev integritet som *”Att man får behålla saker för sig själv”* och informant 3 som *”Jag tänker att det betyder rättighet att göra det man vill utan att bli snokad på”*. Båda dessa uttalanden, samt det ovan nämnda av informant 2, kan tolkas som att informanterna vill ha möjligheten att reservera sig själva. Informant 3 upplever uppenbart att metadata inkräktar på integriteten på ett sätt som antyder att samtliga stadier av privatliv är drabbade. Informanten angav också att han inte har problem med att vara en i en anonym mängd, men undviker helst att bli identifierad. Även informant 4 påstår att metadata är relativt riskfritt för övervakning så länge kartläggningen inte kan knytas till en specifik individ, utan en anonym ID-siffra i en databas. Informant 3 förtydligar sin åsikt med att han ogillar kartläggningen av hans beteendemönster. Informant 2 yttrar också ett ogillande och en oro gällande den frågan, liksom informant 4. En parallell kan dras till studien gjord av Dey med flera, om användares attityd till mobil massavläsning. Tekniken som används till synkronisering av digitala enheter i närområdet för olika funktioner (Dey et al. 2016, 65) kan anses som kartläggande av rörelsemönster. För att dra en slutsats av detta kan sägas att informanterna föredrar att reservera sig själva i alla situationer, och ser helst att insamling av metadata görs på en anonym nivå. Däremot finns både misstankar och vetskap om att metadata tränger in på samtliga stadier av privatliv. Detta stämmer överens med studien av Dey et al. (2016), som resulterade i att användarna saknar kunskap om anonymisering vid mobil massavläsning och därför inte litar på det (Dey et al. 2016, 65).

Westins prognos om framtidens övervakningssamhälle (Westin 1966, 1013–1014) kan analyseras utifrån informanternas upplevda övervakning i denna studie samt utifrån tidigare studier. Eftersom informanterna uppger att intrång på deras privatliv förekommer och att övervakning och kartläggande av rörelsemönster nämndes upprepade gånger kan vi konstatera att de åtminstone upplever sig vara övervakade en stor del av deras liv. Westins prognos bygger på statens övervakning såväl som företagens (Westin 1966, 1003). Informanterna yttrade i flera fall tillit till företag och myndigheter utifrån perspektivet att de troligen inte skulle orsaka någon skada med den insamlade datan om användarna. Misstron som uttrycktes riktades främst mot

företag som upplevdes opålitliga, eller som informant 3 sade, uppenbart försöker tjäna mer pengar på sina kunder. Insamlingen av metadata sker, som tidigare nämnt, både i privat (Haider och Sundin 2018) och offentlig sektor (Cole 2014, 2). Anledningen till att informanterna upplever den ständiga övervakningen skulle kunna bero på den ökade digitala användningen i samhället, som de naturligt påverkas av (Pixell 2018). Informanterna angav att de använder flera digitala artefakter i vardagen, informanterna 3 och 4 något fler artefakter än informanterna 1 och 2. Av den anledningen kan vi anta att informanternas digitala vanor resulterar i stora mängder användargenererade data, som sammanlagt bildar användarnas digitala fotspår (Haider och Sundin 2018). Vidare kan vi diskutera Edward Snowdens upptäckt av NSA:s massinsamling av metadata från USA:s befolkning med syftet att förebygga terrorism (Sundström 2015) som bekräftelse på Westins prognos om övervakningssamhället (Westin 1966, 1013–1014). Kritiker till metoden hävdar att insamlingen resulterat i tillräckligt stora mängder metadata för att NSA skulle kunnat generera en mycket komplex kartläggning av individens rörelsemönster (Pomerantz 2015, 00:1:57). Slutligen kan sammanfattas att en kan argumentera för att Westins prognos från 1966 om framtidens övervakningssamhälle var relativt korrekt (Westin 1966, 1013–1014).

De fyra funktionerna av privatliv kan diskuteras i relation till metadata. Den första funktionen, autonomitet, har människan ett behov av som Westin beskriver i cirklar (Westin 1966, 1022) vilka vi anser påminner om de fyra stadierna av privatliv som redan nämnts (Westin 1966, 1020–1022). Den innersta cirkeln kan tolkas som det isolerade stadiet, den yttersta cirkeln som det reserverade stadiet och så vidare. Därför resonerar vi att metadata berör alla cirklar, liksom det berör alla fyra stadier. I så fall, enligt Westins teori, är individens autonomitet under hot vilket i sin tur riskerar hela demokratin som bygger på individualiteten hos deltagarna (Westin 1966, 1022). För att undersöka om informanterna upplever emotionell frigörelse, nästa funktion, måste närliggande ämnen diskuteras då det inte framkom specifikt under intervjuerna. Attityder som att vissa informanter ser sig *själv som ointressant, anonym*, kan tolkas som att de upplever en frihet av att vara i en anonym mängd. *Tillit* kan även ses som en trygghet, vilket kan likna emotionell frigörelse. En aspekt av emotionell frigörelse Westin beskriver är frigörelsen från

straff för brott mot normer och regler, som människan behöver. Westin hävdar att människan behöver utrymme att begå småbrott och klaga på auktoriteter utan att straffas varje gång (Westin 1966, 1024-1025). Informant 4 nämner ett fall där detta utrymme har minskat på grund av sociala medier: "(...)säg att jag hade skrivit ett negativt anonymt inlägg om mitt företag för fem år sedan för att jag var missnöjd med en tjänst, hade det kunnat knytas till mig hade jag inte kanske fått jobb här". Sammantaget kan tyckas att metadata försvårar emotionell frigörelse, emellertid diskuterades frågan för lite för att vi ska kunna dra en slutsats om det. Likaså framkom inte av intervjuerna huruvida deras personliga egentid påverkas av metadata, och om de finner att tiden för självutvärdering har påverkats av deras digitala användning. Den sista funktionen av privatliv, begränsad och skyddad kommunikation, kan vi konstatera påverkas av metadata i högsta grad, med tanke på tidigare diskussion om övervakning.

7. Diskussion

I detta avsnitt sammankopplas resultat med analys för att besvara frågeställningarna. Därefter diskuterar vi vilka forskningsfrågor inom området som kan vara relevanta för framtida forskning. Diskussionen leder sedan till 8. *Slutsats*.

7.1 Hur är användares attityd till metadata i relation till deras kunskap?

Informant 1 och 2, vilka tillhör kategorin *icke verksamma inom IT*, uppvisade en grundläggande uppfattning om metadata. Informant 1 yttrade attityder som tillit till myndigheter, paradoxalt beteende och utnyttjande av metadata för egen vinning. Hon ser att det finns fördelar med metadata, exempelvis förebyggande av kriminalitet, som uppväger nackdelarna. Hon är av princip för teknisk utveckling och anser att metadata är en nödvändig del av den. Överlag har informanten en positiv attityd till metadata. Informant 2 angav attityder som kännetecknas av hämmad användning, tillit till myndigheter, medvetet urval av företag, paradoxalt beteende, egen vinning och oräddhet. Hans beteende präglas till stor del av instinkter och känslor. Sammantaget

sett verkar informant 2 inte ha en tydlig inställning till metadata, utan pendlar mellan sina negativa attityder och sitt positiva agerande.

Informanterna 3 och 4, vilka tillhör kategorin *yrkesverksamma inom IT*, besatt båda två en djupgående kunskap om metadata men ur olika synvinklar. Informant 3, som arbetar med IT-säkerhet, uttryckte attityder som försiktighet och riskmedvetenhet, och uttalade att han anser att metadata har fler nackdelar än fördelar. Emellertid uppvisade han attityder som tillit till myndigheter som använder metadata och att han tror att de största riskerna han utsätts för är kommersiella. Han tar försiktighetsåtgärder i de fall han kan under sitt digitala användande men inte på bekostnad av tjänster han anser bättre än andra, som Google. Därmed kan konstateras att informant 3 använder sin kunskap och agerar medvetet för att minska riskerna för negativa konsekvenser av metadatainsamling, men till en viss gräns. Generellt ser vi att informant 3 har en negativ attityd till metadata.

Informant 4, som jobbar med metadata för optimering av digitala tjänster, upplevde sig ha mestadels kunskaper om metadata inom sin nisch av arbete men även kunskaper tack vare sin tidigare karriär inom andra delar av IT-branschen. Informant 4 uttryckte attityder som maktlöshet, riskmedvetenhet och medvetet agerande, men även att han är ointressant för värre konsekvenser än profilering för kommersiella syften. Dock uttryckte han fler attityder av positiv karaktär, som grundades i hans egen hantering av metadata i sin yrkesroll. Han angav flera vinster metadata kan resultera i när det används för att personalisera och optimera digitala tjänster, som dessutom innebär få risker för individen. Vi bedömer att informant 4 utnyttjar sin kunskap för att minimera de risker med metadata han anser finns och kan påverka, samtidigt som han har en generellt positiv attityd till metadata.

Gällande informanterna 1 och 2 anser vi att deras grundläggande kunskap inte direkt påverkar deras attityder. Informant 1 valde att se fördelarna med metadata som övervägande då det överensstämde med hennes starka åsikter om samhällets utveckling och var därför av en medvetet positiv attityd som baseras på den vaga kunskap hon tyckte sig ha. Informant 2, som

hade en attityd av blandad karaktär, gav intryck av att inte kunna bestämma sig för om nackdelarna eller fördelarna vägde mest eftersom han saknade kunskap om det. Informant 3 var övervägande negativt inställd till metadata vilket sannolikt berodde på hans kunskaper som IT-säkerhetskonsult. Informant 4 som var av generellt positiv attityd baserade den på sina kunskaper som metadataspecialist inom Video OnDemand.

För att sammanfatta kan det konstateras att informanternas kunskap påverkar inte alltid deras attityd. Informanterna som saknade yrkeskunskap inom IT valde att antingen fatta ett beslut utefter den kunskap de har eller att inte kunna bestämma sig alls. Informanterna med yrkeskunskap inom IT var uppenbart påverkade av den yrkesroll de hade och attityden speglade att den ena använder metadata för optimering och den andra arbetar med skydd mot det.

Denna insikt kan jämföras med analysen enligt utilitarismen, som konstaterade att informanternas uttalade attityder kännetecknas mer av lidande än njutning. Vid ett större perspektiv, där informanternas uttalade attityder jämförs med deras agerande, kan vi se tydligare vilka informanter som verkar lida respektive njuta av metadata. Eftersom attityderna vi klassar som lidande är de samma som de negativa kan vi se att informant 1 och informant 4 upplever mer attityder av njutning medan informant 3 upplever mest lidande och informant 2 väger mitt emellan. Njutningen och lidandet har alltså, liksom attityderna i sig, ingen tydlig relation till informanternas kunskap. Metadata orsakar aningen mer lidande än njutning för studiens fyra informanter. Enligt utilitarismen skulle fortfarande metadata vara moraliskt oförsvarbart i detta fall eftersom det inte skapar njutning för ett maximalt antal människor. Våra informanternas uttalade attityder är främst negativa och de ser fler nackdelar än fördelar med metadata. Metadata anses alltså vara förminskande och med hänsyn till våra informanternas intervju svar, utifrån teorin avdesign, bör alltså metadata om/-avdesignas. Att avdesigna metadata till en mindre teknisk lösning skulle inte vara ett alternativ då funktionen baseras på att vara högteknologisk.

7.2 Hur påverkar kunskaperna och attityden värderingen av digital integritet?

Informant 1 och 2 uppvisade olika attityder till integritet vilka kan relateras till de skilda inställningar angående metadata som har diskuterats ovan, i 7.1 och 7.2. Båda informanterna ansåg att integritet var rättigheten att få behålla känslig information privat och själv bestämma vad som ska delas med andra. Informant 1 är generellt orädd för konsekvenserna av sin egen digitala användning och ser sig inte som en intressant måltavla för kartläggning. Informanten uppger samtidigt ett behov av privatliv och misstänker att metadata är något osynligt bakomliggande som hon ej kan påverka. Informant 2, som pendlade mellan negativa och positiva attityder angående metadata, vidtog däremot ett antal försiktighetsåtgärder för att skydda sin egen integritet. Han uttryckte även ett behov av privatliv och en misstanke att metadata används för kartläggning av individens rörelsemönster.

I likhet med varandra ansåg båda informanterna att medicindata och journaltjänster var känslig information och i behov av att skyddas för att bibehålla digital integritet, även bankuppgifter så som kontoinformation och koder ansågs av båda informanterna vara känsliga. Detta stämmer överens med studien av Chow med flera där användarna rankade bland annat kategorierna finans, medicin som de mest känsliga av deras sökhistorik i webbläsare (Chow et al. 2017). Båda informanterna litade också på myndigheterna och tjänsterna som förvaltar denna känsliga information, exempelvis 1177 och banken är enligt informant 1 och 2 säkra och den känsliga informationen som används där riskeras inte att utlämnas. Däremot skildes åtgärderna som de båda informanterna vidtog för att slutligen skydda den digitala integriteten, informant 1 ansåg att hon inte vidtog några åtgärder för att skydda sig själv till följd av att hon dels inte anser sig vara intressant nog för att vara en måltavla för kartläggning, samt då hon litade på de myndigheter och företag som tar hand om hennes känsliga data. Hon uttryckte även att hon ibland använder sig av betaltjänster online som hon inte litar på till grund av sin lathet. Informant 2 uttryckte till skillnad från detta att han väljer kända betaltjänster framför andra, till exempel Paypal framför mindre etablerade tjänster, för att detta inger honom en känsla av säkerhet. Informant 2 uttryckte

även att han undviker att publicera bilder på sina barn online för att upprätthålla en känsla av integritet. Känslan av integritet som han anser sig upprätthålla är då han undviker att dela privata saker med hela världen. Sammanfattningsvis kan det i och med detta anses att båda informanterna har en tydlig bild av vad integritet är och trots att de båda värderar integritet online i likhet med varandra utför de olika åtgärder för att undvika hur deras privata data delas. Informanternas snarlika kunskap om ämnet till trots har de två skilda åsikter om hur integritet upprätthålls i samspel med teknologin och det kan därför inte antas att kunskapen i detta fall påverkar värderingen av digital integritet. En tydlig likhet mellan informant 1 och 2 är dock tilliten till företag och myndigheter som de båda uttrycker, bådaskt agerande kan kopplas till en tilltro till de myndigheter som besitter de känsligaste delarna av sina metadata.

Informant 3 och 4 uppvisade olika attityder till metadata samt att båda även företog olika åtgärder för att skydda sin integritet online. Informant 3, som främst har en negativ inställning till metadata, vidtog flest försiktighetsåtgärder medan informant 4, vilken har främst positiva attityder till metadata, vidtog även han försiktighetsåtgärder, om än färre än informant 3. Informant 4 baserade även sina åtgärder baserat på hans kunskap. Informanterna ansåg båda att integritet var rättigheten att göra vad man vill utan att riskera att bli snokad på. Informant 3 definierade det som att exempelvis kunna söka en resa via SL utan att ens data lagrades medan informant 4 tyckte att det främst handlade om rättigheten att som konsument aktivt kunna välja vad som ska delas med andra. Informant 4 uttryckte det istället som att inget användaren gör kan göras utan att lämna spår, men integritet är att ha rättigheten att välja bort de tjänster som användaren inte vill dela dina uppgifter med. Informanterna hade vidare spridda åsikter gällande vad som anses vara känsliga uppgifter och därmed av vikt att skydda för att bibehålla integriteten. Informant 3 ansåg att en stor mängd data såsom journaltjänster, privata konversationer - mejl, sms och chattar, samtliga data tillhörande sociala medier - konversationer, vem som är kompis med vem och så vidare, sökningar i olika sökmotorer, bilder och dess tillhörande metainformation samt betaluppgifter, medan informant 4 parallellt endast ansåg att bankuppgifter och privata chattar tillhör integritetskänslig information. Informanternas agerande är också något varierande, informant 3 innehar en stor tillit till svenska företag och myndigheter

eftersom de historiskt sett har haft mindre läckor än exempelvis amerikanska företag. Samtidigt som han själv utför många åtgärder för att minska sin loggning av privata data, exempel på detta är VPN-skydd på allt han gör samt att han undviker att använda offentliga wifi-anslutningar på exempelvis hotell. Informant 4, till skillnad från tidigare informanter anser att en liten mängd data faktiskt är privat och det därför inte är av lika stor vikt att faktiskt skydda sig. Han anser sig även inte vara en tillräckligt intressant målbild, precis som informant 1, för att vara i risk att kartläggas. De åtgärder som informanten tar är exempelvis att läsa användarvillkoren för att avgöra företagets baktanke och på så sätt kunna undvika en integritetsproblematik. Han menar att användarvillkoren kan innehålla information om hur datan används och att ett medvetet användande kan minska integritetsproblematik, detta i samband med ovan nämnd problematik - att integritet är rättigheten är själv bestämma vilka data som skall delas med andra. Informanten uttrycker att det är kränkande av integriteten först när en applikation tar data från användaren utan att detta tydligt kommuniceras. Informant 4 uttrycker dock att detta inte är ett vanligt problem, utan något som med enkelhet kan undvikas av samtliga användare. Han påpekar att säkra företag, och exemplifierar med företaget som han själv arbetar för, inte sparar information som går att spåra till en specifik individ utan att ID-nummer används och att den känslig informationen därför inte går att spåra till specifika kunder. Informant 3 och 4 har skilda åsikter om deras integritet men i likhet med varandra innehar de stor kunskap och förstår hur datan kan komma att missbrukas. Även hur de arbetar för att upprätthålla känslan av integritet är skild, informant 4, i likhet med informant 1 och 2 väljer att aktivt lita på de myndigheter och företag som besitter möjligheten att se hans metadata. Informant 3 till skillnad från de andra informanterna innehar inte en direkt tillit till företag och anses därför inneha en skarpare värdering av sin integritet. Informant 3 anser att integritet är för känsligt för att vara värt att riskera och metadata innebär en stor risk i och med att teknologin kan läcka. Den likhet som kan länkas mellan informant 3 och 4 är att värderingen av integritet baseras på deras kunskap, vilken uppnås av deras yrke. Informant 4 som jobbar med att skydda användarna baserar även sin personliga användning på detta och informant 3 som verkar för att optimera användningen av metadata baserar även han sin syn på digital integritet på detta.

För att återkoppla till Westins teori om privatliv summerar vi den som att de fyra funktionerna av privatlivet påverkas i stor utsträckning av metadata, liksom de fyra stadierna av privatliv, eftersom de påminner om varandra enligt vår analys. Detta gäller studiens samtliga fyra informanter, oavsett kunskap och attityder till metadata. Vi konstaterar även att Westins prognos om övervakningssamhället kan påstås stämma och att informanterna ser många metoder att övervaka människor med hjälp av metadata.

7.3 Slutsats av diskussion

Ovan resultat kan i paritet tolkas som de förminskande och förstärkande egenskaper som presenteras av Idhe, i teorin om avdesign (Pierce 2012, 959). Samtliga fyra informanter noterar det positiva och negativa i användandet av metadata och väljer utifrån dessa aspekter att tolka sin digitala integritet. Informant 2 anser att det övergripande innefattar förminskande egenskaper och skulle därför kunna vara för en avdesigning, medan informant 1 anser att de förstärkande egenskaperna är fler och är enligt teorin inte benägen att avdesigna produkten. Tydligt visar informant 3 att han anser att de förminskande egenskaperna är fler medan informant 4 till skillnad från informant 3 och i likhet med informant 1 ser de förstärkande egenskaperna som fler.

Kopplat till Westins teori om privatliv kan konstateras att de tre informanter, 2, 3 och 4, som uppgav att de föredrar att kunna reservera sig själva, var som sagt av olika kunskap om och olika attityd till metadata. Dessa tre upplever att metadata riskerar intrång på privatlivets samtliga stadier. Enligt den analysen finns inte heller någon koppling mellan informanternas kunskap och attityder gentemot värderingen av integritet.

Det går även att i frågeställningarna se den integritetsparadox som först nämnts i *1. Inledning*, där Norberg, Horne och Horne diskuterar beteende och handling som två skilda event. Trots en uttryckt motvilja att som användare dela sin privata information med företag, visar studier att allt fler användare frivilligt delar sin data med företag (Norberg, Horne och Horne 2007, 100). Ett tydligt exempel på detta är informant 2 som trots sin dels negativa inställning till metadata inte genomförde direkta handlingar för att undvika att hans data lagras. Han sa exempelvis att han

undviker att lägga upp bilder på sina barn i sociala medier, samtidigt som han inte har något emot att hans flickvän gör det. Även informant 3 uttryckte att det finns, enligt honom, tydligt negativa aspekter av samlandet av metadata samtidigt som han anser att de positiva aspekterna vägs upp emot de negativa och därför inte behöver tas i beaktning.

7.4 Vidare forskning

Framtida studier som kan vara av intresse är hur olika yrkesgrupper förhåller sig till ämnet *attityder till metadata*, till skillnad från denna uppsats där yrkesgrupperna delats på två där den ena är verksam inom IT och den andra gruppen inte är det. Förmodat att fler yrkesgrupper inkluderas kan ett annat, nyanserat resultat avläsas där olika typer av yrkesverksamma inkluderas. Dessutom kan en liknande studie som denna men med fler informanter, ur flera olika yrkesgrupper, generera ett intressant resultat. En kvantitativ version av studien där en större populations attityder undersöks med hjälp av exempelvis enkätstudier anser vi relevant, särskilt med anledningen av att GDPR-lagen nu funnits i bruk under en tid. Studien kan undersöka om attityden hos människor påverkats efter att GDPR blivit en del av vardagen för många privatpersoner och företag.

8. Slutsats

Syftet med uppsatsen var, som nämnt i inledningen, att uppnå teoretisk generalisering av relationen mellan kunskap och attityd hos användare kring insamling av metadata i användning av digitala artefakter, samt hur detta påverkar värderingen av integritet. Vårt bidrag till forskningen är en kvalitativ studie inom ett forskningsområde som till viss del är utforskat, vilket exemplifieras i avsnitt 2. *Bakgrund*.

Följande frågeställningar har studien besvarat och kortfattas här nedan.

- *Hur är användares attityd till metadata i relation till deras kunskap?*

Det finns inget tydligt samband mellan de fyra informanternas kunskap och deras attityd. Hos informanterna ur kategorin icke-yrkesverksamma inom IT syns svagast samband då de båda har olika attityd men ungefär samma kunskap. Ur kategorin verksamma inom IT märktes att båda informanternas attityd baserades på deras kunskap, som kom från olika yrken i IT-branschen.

- *Hur påverkar kunskaperna och attityden värderingen av digital integritet?*

Kunskaperna och attityderna påverkar i liten del värderingen av integritet hos våra fyra informanter. Det kan tolkas att erfarenheten hos de fyra informanterna baserar deras syn på integritet samtidigt som det inte går att dra paralleller mellan faktisk tekniskt kunskap och hur de skyddar sin integritet på nätet.

9. Referenser

- Alvehus, J. (2013). *Skriva uppsats med kvalitativ metod: en handbok*, Upplaga 1. Liber, Stockholm.
- Bell, J. (2005). *Introduktion till forskningsmetodik*. Upplaga 4. Studentlitteratur.
- Björkhem, M. (2007). Metadata. Kungliga biblioteket - Sveriges nationalbibliotek.
<http://www.kb.se/bibliotek/Metadata/> [hämtad 2017-11-21]
- Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3:2, 77–101.
http://eprints.uwe.ac.uk/11735/2/thematic_analysis_revised_-_final.pdf [hämtad 2018-11-16]
- Chow, R., Naeun Lee, L. & Rashid, A.M. (2017). Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing systems, pages 1816–1823.
doi.org/10.1145/3027063.3053078 [hämtad 2019-01-09]
- Cole, D. (2014). We kill people based on metadata. *Cyber peace*.
<https://cyber-peace.org/wp-content/uploads/2014/05/We-Kill-People-Based-on-Metadata.pdf>
[hämtad 2018-11-28]
- Datainspektionen. (2018). Idag stärks skyddet av den personliga integriteten. Datainspektionen.
<https://www.datainspektionen.se/nyheter/idag-starks-skyddet-av-den-personliga-integriteten/>
[hämtad 2018-12-06].

- Dey, A.K., Gustarini, M. & Wac, K. (2016). Anonymous smartphone data collection: factors influencing the user's acceptance in mobile crowd sensing. I: *Personal and Ubiquitous Computing*, volym 20, nummer 1, februari 2016, s.65–82.
<https://link.springer.com/article/10.1007%2Fs00779-015-0898-0> [hämtad 2019-01-09]
- Dimmock, M. & Fisher, A. (2017). Utilitarianism. *Ethics for A-Level*, 1st ed., Open Book Publishers, Cambridge, UK, 2017, s. 11–29. *JSTOR*, www.jstor.org/stable/j.ctt1wc7r6j.5. [hämtad 2018-11-28]
- Haider, J. och Sundin, O. (2018). Algoritmer och data. Internetstiftelsen i Sverige.
<https://www.iis.se/lar-dig-mer/guider/algoritmer/algoritmer-och-data/> [hämtad 2018-11-21]
- Hernadi, A. (2008). Det här är FRA-lagen. *Svenska Dagbladet*.
<https://www.svd.se/det-har-ar-fra-lagen> [hämtad 2018-12-07]
- Hoback, C. (2013). Terms and conditions may apply. Nätjättarna och integriteten. [video].
<https://www.netflix.com/title/70279201> [hämtad 2018-11-16]
- Jarboh, M. (2017). Kunskap och attityder kring digitala fotspår och hur det påverkar användandet av internet. En studie om integritet, tillit och egenmakt. Södertörns Högskola, Institutionen för Naturvetenskap, miljö och teknik.
<http://sh.diva-portal.org/smash/get/diva2:1176614/ATTACHMENT01.pdf> [hämtad 2018-11-14]
- Jonsson, H. & Olsson, C.M. (2018). User privacy attitudes regarding proximity sensing. Proceedings of the 13th International Conference on Availability, Reliability and Security, Article No. 25. Hamburg, Germany - August 27–30, 2018.
<https://dl.acm.org/citation.cfm?doid=3230833.3233270> [hämtad 2019-01-09]
- Norberg, P., Horne, D. och Horne D. (2007). The privacy paradox, Personal information disclosure intentions versus behaviors. *The Journal Of Consumers Affairs*.
doi.org/10.1111/j.1745-6606.2006.00070.x [hämtad 2018-11-16]
- Pomerantz, J. (2015). *Metadata [Elektronisk resurs, ljudbok]*. Gildan Media.
<https://www.storytel.com/se/sv/books/628426-Metadata>.
- Pierce, J. (2012). Undesigning Technology: Considering the Negation of Design by Design. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, May 5–10, 2012. doi.org/10.1145/2207676.2208540 [hämtad 2018-10-23]

- Pierce, J. (2014). Undesigning Interaction. I: *Interactions*, volym 22, nummer 4, juli–augusti 2014, s.36–39 <https://dl.acm.org/citation.cfm?doid=2637406.2626373> [hämtad 2018-11-06]
- Pixell, R. (2018). Integriteten. Internetstiftelsen i Sverige.
<https://www.iis.se/lar-dig-mer/guider/uppkopplade-prylar/samhallet-gar-online/> [hämtad 2018-11-06]
- Sullivan, M. (2012). It's Not Your Eyes...the Fine Print Is Getting Really, Really Small. *Wall Street Journal*.
<https://www.wsj.com/articles/SB10001424052970204124204577154670004173532?ns=prod/accounts-wsj> [hämtad 2018-12-07]
- Sundström, L. (2015). Fem timmar med Edward Snowden. *Dagens Nyheter*.
<https://fokus.dn.se/intervju-edward-snowden/> [hämtad 2018-11-23]
- Tyagi, N., Gilad Y., Leung, D., Zaharia, M. & Zeldovich, N. (2017). Stadium, A distributed metadata-private messaging system. Proceedings of the 26th Symposium on Operating Systems Principles. s. 423–440. doi.org/10.1145/3132747.3132783. [hämtad 2018-11-28]
- Westin, A. (1966). Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy. *Columbia Law Review*, 66(6), 1003-1050. doi.org/10.2307/1120997 *JSTOR* [hämtad 2018-11-29]

10. Bilagor

10.1 Intervjufrågor

Hej! Tack för att du ställer upp på en intervju! Den här intervjun kommer ta ungefär en halvtimme. Resultatet kommer att finnas i vår c-uppsats som kommer att publiceras på webben. Enbart din yrkestitel och ålderskategori kommer att sparas, det kommer alltså inte kunna spåras att just du besvarade dessa frågor. Om du samtycker kommer intervjun att spelas in, vilket kommer att kunna höras av enbart oss, vår handledare och examinator. När projektet är helt avslutat kommer inspelningen kasseras. Är det något du undrar över innan vi börjar?

Kritisk händelse:

Sök en resa till jobbet via kollektivtrafiken med hjälp av SL:s reseplanerare. Anteckna alla spår du tror att applikationen sparar om dig och din sökning. Du kan anteckna på valfritt ställe. Under intervjun ber vi dig att visa anteckningarna så att vi kan samtala om dem.

Uppvärmning

1. Hur gammal är du?
2. Vad arbetar du med?
3. Vilka digitala artefakter använder du på fritiden (*tex. Smartphone, iPad, dator*)?

Kunskap

4. Vad vet du om metadata? (*I din vardagliga närhet*)

Om de kan ej kan något, hoppa till fråga nummer 8

5. När tror du att du efterlämnar metadata?
6. Hur skulle du säga att vetskapen om metadata påverkar ditt digitala användande?
7. Vad tror du är konsekvenserna av de digitala fotsår som du lämnar efter dig? Positiva och negativa.

Om nej,

8. Tror du att användningen av dina digitala artefakter efterlämnar spår? Hur?
9. Har du någon gång noterat ett samband mellan det du gör/googlar och vilka annonser som visas på dina digitala artefakter? Hur?
10. Känner du till GDPR-lagen?
11. Vad vet du om den?

Integritet

12. Vad är integritet för dig?
13. Vad tänker du om din integritet vid användning av digitala artefakter?
 - 13.1. Tycker du att integritet vid användning av digitala artefakter är viktigt och hur uttrycker sig i så fall detta?

14. Vad är känslig information enligt dig, som du inte vill dela med dig av till andra?
(Medicindata, bankuppgifter, betaluppgifter, GPS-koordinater osv).
15. När tror du att du utlämnar sådan känslig data?
16. Har du någon gång fått känslan av att din integritet riskeras vid användning av digitala artefakter? När och hur?
17. Finns det moment i den digitala användningen som du undviker för att inte lämna ut känslig information? *(Stängt av GPS, sparar ej kortinformation vid köp, använder ej kontokort, använder ej sociala medier osv.)*

Attityd

18. Vad har du för intryck/uppfattning om metadata?
19. Vad tycker/tror du att det finns för fördelar med metadata?
20. Vad tycker/tror du att det finns för nackdelar med metadata?
21. Hur tror du att metadata kan påverka din integritet på digitala artefakter?
22. Har din uppfattning om integritet och metadata påverkats av de avslöjanden som Edward Snowden gjorde 2013? *(förklara lite)*

Avslut

24. Nu när vi samtalat om ämnet en stund, har din uppfattning om metadata förändrats på något sätt?

Tack för att du ville medverka!

10.2 Samtyckesblankett

Samtycke till att delta i studien: Kunskap och attityd kring metadata.

Jag har skriftligen informerats om studien och samtycker till att delta. Jag är medveten om att mitt deltagande är helt frivilligt och att jag kan avbryta mitt deltagande i studien utan att ange något skäl. Min underskrift nedan betyder att jag väljer att delta i studien och godkänner att Södertörns högskola behandlar mina personuppgifter i enlighet med gällande dataskyddslagstiftning och lämnad information

.....

Underskrift

.....

Namnförtydligande

.....

Ort och datum

Kontaktuppgifter

Jenny Nilsson

jenny12.nilsson@student.sh.se